规划通过 NSX 实现运维转型

实际最佳实践

指南

vmware

目录

简介

本白皮书主要适用于云计算、网络连接和安全性领域的高管和经理。另外也适用于参与组织中 NSX 实施工作的体系结构、工程和运维领域的经理和相关工作人员。

网络虚拟化是一项重大进步，能够帮助组织在速度、敏捷性和安全性方面获得优势。它的优势不亚于甚至超过近十年来计算虚拟化所提供的优势。要实现网络虚拟化的优势，组织需要评估和执行一项涵盖**人员**、**流程**和**技术**的实施计划。

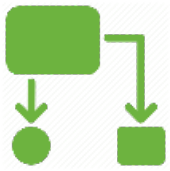
VMware 通过与现有 NSX 客户的密切合作，了解到将网络虚拟化投入运行所面临的现实问题。这些实际知识将帮助您完成对 NSX 的评估、部署和实施。您和您的组织可以查看并使用最适合您的具体情况的最佳实践。

虽然本白皮书介绍了大量的最佳实践，但要实施 NSX，只需做出最少的更改即可，完全不受现状的影响。实施 NSX 并不复杂，且具有明确的成功途径。

本指南分为三个主要部分，分别讨论针对以下各方面的关键知识和最佳实践：

人员

网络虚拟化提供了发挥组织力量的机会，还提供了让技术部门实现工作方式转变的重要优势。它也意味着组织要在慎重考虑后做出变革，以确保整个组织目标明确、行动一致。确保拥有灵活的组织结构，组建角色和职责明确的融合团队，让您能够获得最大的成效并实现组织和员工的最大价值。我们将围绕组织结构、内部接洽和沟通策略以及角色和职责提供相关信息和指导。



流程

实施网络虚拟化之后，应用生命周期中的手动流程都能实现自动化，因此可以提供大量提高工作效率的机会。针对如何调配、管理和监控应用与服务定义一个理想的未来状态，让您能够摆脱不必要的现有流程和实践。我们将围绕如何思考自动化、流程管理、使用工具等提供指导，还会提供一些有趣的用例。

技术

网络虚拟化的一个主要优势是将网络和安全功能从底层物理网络基础架构中剥离，将其转移至虚拟化层。这让您能够更好地设计和管理您的基础架构以便不断发展。我们将围绕体系结构最佳实践、基础架构的逐步实施以及定期发布的新功能等提供指导。

这些最佳实践并不是强制性的规范或“放之四海而皆准”的规则。您需要根据自己组织的独有特征、目标和优先事项来选择您认为合适的最佳实践。而且不要尝试一劳永逸的做法，可以先从两个或几个最佳实践开始，然后再逐步尝试其他最佳实践。

有一些组织在追求最佳性能的过程中会骄傲自满，很快便止步不前。这会限制组织可能取得的成功。请始终牢记最终状态，并不断努力来获得改进和提升以实现该状态。

人员

我们要讨论的第一个主题是人员：也就是负责应用和服务的端到端交付和管理的技术部门中的组织、团队和个人，他们最终也是成功实施网络虚拟化和安全性的决定力量。

有关组织结构的初步想法

网络虚拟化和 NSX 无需专门的组织结构类型。最佳结构取决于您的组织特有的因素。从传统的各自为政的组织，到完全融合的云计算团队，都有成功实施 NSX 的范例，即使是介于这两者之间的组织在实施上也没问题。

理想的组织结构由大量因素决定。设计结构时，应该考虑以下几点：

- 各领域和学科之间的一致性
- 价值流的成熟度
- 技术领导力的级别
- 员工的经验和专业知识
- 运维体验和复杂性
- 外包的使用
- 基础架构和应用的数量
- 升级或全新部署

我们的建议：设计融合的团队结构

根据实践经验，工作效率最高的团队是那些紧密交织、高度协作且自给自足的团队。事实证明，由于工作周期短，反馈流程精简而有力，知识共享和持续学习多，这类融合团队的工作效率更高。理想的情况下，这个团队的工作人员应该在一处办公。

我们已经看到一些成功的组织结构，既有根据领域（例如，计算、存储、网络连接和安全）组成团队的，也有根据学科（例如，体系结构、开发和集成、运维以及支持）组成团队的。无论是哪种情况，相应团队都要负责物理和虚拟基础架构。

随着您将更多的基础架构和应用从现有企业网络转移到云中，人员分配也会发生转变。随着时间推移，将会有越来越多的员工从事云计算方面的工作，越来越少的员工从事现有企业网络方面的工作。为帮助组织了解这种转变以及由此产生的新职业机会并做好准备，需要制定沟通和培训计划，这一点非常重要。同样重要的是您需要传达这样的理念，即无论员工是从事现有企业网络方面的工作，还是从事云计算方面的工作，每个人的贡献对于组织的整体成功都至关重要。

采用共同的成功衡量指标

组织方面的另一个重要注意事项是遵照一个拥有明确的目标、目的、措施和激励的共同战略。从业务要求到运维和管理受 SLA 支持的高质量生产工作负载，您的团队应该采用以服务为导向的方法，共同对整个服务交付生命周期承担责任。

每个团队还应该具有共同的成功衡量指标，这些指标根据对您组织最重要的因素来制定。具体示例包括：销售就绪时间、对收入的影响、市场响应能力、创新速度，和/或为客户带来的优势以及客户满意度。目标应该向外专注于业务以及服务使用者。

允许团队制定和跟踪自己的成功衡量指标。确保衡量指标与共同的目标、目的相关且一致。除了与组织的目标保持一致之外，关键绩效指标应该具体、明确、可量化且可衡量。无论团队选择哪些关键绩效指标，都应该让指标简单易懂，并从少数几个易于理解且有意义的基本指标开始入手。

选择关键绩效指标后，记录下您今天的进度来作为基准。定期（例如每月或每季度）跟踪和评估您朝着期望的最终目标前进的进度。要让团队明白，这样做不是为了评判他人或既往绩效，而是为了证明团队的成功以及他们为业务带来的新价值。有了这些衡量指标，绩效审查和评估对个人来说会更有效、更切实际且更有意义。

打造具有责任感和参与感的文化

对于网络虚拟化和安全性来说，文化是成功的重要支柱。拥有支持软件定义的数据中心原则的文化至关重要。文化应该通过团队的共同体验、技能和价值观从团队内部有机地形成，而非从管理层强制进行文化变革，后者从根本上说非常困难。

通过建立共同的成功衡量指标，新的文化将会形成并自然而然地深入人心。新文化的根基在于清晰的以业务和使用者为中心的目标、共同承担的责任和风险、更紧密的协作与合作以及相互的信任与尊重。

团队：安全性和网络专家协同工作

网络虚拟化的一个主要优势是将网络和安全功能从底层物理网络基础架构中剥离，将其转移至虚拟化层。这种转移催生了一些问题，例如：“哪个团队负责在 hypervisor 中运行的虚拟网络连接和安全性工作？”以及“网络虚拟化会如何改变我的职责？”在这一部分，我们将回答上述问题。

您现有的网络和安全性员工将继续负责网络虚拟化和安全性工作。NSX 所依据的网络连接概念和技术需要员工具备网络连接专业知识。只有您的网络团队具备所需的专业知识。设计、部署和运维虚拟网络需要网络和安全专家，就像对待物理网络一样。

物理网络并未消失，而是变得更加简单且易于管理。我们建议不要随便地根据物理和逻辑网络来划分团队职责。要尽量提高速度和敏捷性，由网络架构师、工程师和操作员组成的团队应该负责物理底层和虚拟覆盖层。

当然，您也可以选择由一些网络工程师主要负责安装、安置和配置物理设备，其他人员主要负责虚拟覆盖层。但是，所有这些人员应该隶属于同一个团队。

网络连接这一学科中的职能（例如，架构师、工程师和操作员）已经发展为包括网络虚拟化和安全性。网络连接和安全性领域的大部分人员需要学习新的知识以增强他们的专业知识和技能。借助 NSX，网络服务可在 hypervisor 层中运行。网络专业人员必须对服务器虚拟化及其对逻辑网络服务的意义有一定的了解。

有关人员的最佳实践：培训

在评估流程的早期，最重要的当务之急是确保每个人都了解网络虚拟化的原则并接受有关 NSX 和相关的运维与管理工具（这些是云计算生态体系的组成部分）的培训。为此，VMware 提供了很多种方法，包括动手练习、研讨会和课程。这些资源主要面向那些没有服务器虚拟化背景的网络专业人员，同时也适合希望学习网络虚拟化的服务器虚拟化专业人员。您也可以制定团队间和团队内的知识分享和培训计划，为个人提供担任领导的机会，非正式地向其他团队和群组讲授最佳实践。

加快学习速度的最佳方法之一是确定并启动小型试点项目和评估。让所有必要的学科职能（体系结构、工程和操作员）参与到计算、存储、网络连接和安全等领域之中。

从小规模的跨职能团队开始

另一个可降低风险的建议就是在向网络虚拟化迈进的过程中，先从小规模的跨职能团队开始。如果您能够从孤立团队过渡到融合团队，请分阶段逐步进行。我们最常见的跨职能团队有两种。请选择最适合您的模式：

孵化团队	攻坚团队
如果您能够过渡到一个长期存在的融合团队，请使用孵化团队。孵化团队最终会成为组织结构/图表中的永久组成部分。另外，这个团队的成员应该是专为该团队服务的全职员工。	如果您不能过渡到一个长期存在的融合团队，请使用攻坚团队。可根据需要组建和解散攻坚团队。其成员多为兼职人员，其正式身份是其他团队的成员。我们已经发现政府机构往往都使用攻坚团队。

通常情况下，这样的跨职能团队会从头到尾对特定的应用体系或一组应用体系负责。团队中应该有计算、存储、网络连接和安全方面的专家。学科技能应该涵盖体系结构、工程和运维。团队必须能够处理一切事情，从设计、开发、测试到部署和日常运维。（请参阅附录，了解有关网络连接和安全性角色和职责的说明。）

为最初的团队选择变革推动者

为最初的团队选择变革推动者、领域专家、推广人员以及德高望重的领导。您物色的人选应该是：受到团队所有其他成员欢迎；知道如何建立人际关系、开创沟通渠道，能够发现并尽量减少冲突；鼓励他人做出改变，以身作则，身先士卒。如果团队成员不在同一处办公，请在项目启动前两周将他们召集在一起。

团队成员应该有与团队目标相一致的个人 MBO。举个例子来说，如果一位团队成员花费 50% 时间在孵化团队上，那么该工作应该占其 MBO 的大约 50%。这似乎是显而易见的事，但我们了解到这样的案例：某位员工花费时间在跨职能团队中工作，而这被视为一种兴趣爱好而不是其核心工作。如果出现这种情况，则不太可能取得成功。

有关人员的最佳实践：避免临时通知

切勿在您要执行部署之前临时通知相关人员。我们了解到这样的案例：网络或安全运维领域的人员太晚参与到流程中，结果导致项目进度被大大延迟。运维人员需要知道网络虚拟化和安全性是如何改变监控、警报和故障排除流程的。此外，还要了解他们的流程以及所用工具会如何改变，关于这一点，本白皮书稍后会讨论。

宣传成功和发展机会

在完成项目的网络连接和安全性工作时，说明可能的个人和专业发展。实现基础架构的虚拟化和自动化后，从事网络连接和安全性的员工将会有更多时间开展有趣的新项目。他们可以专注于能够向企业交付更高价值的战略计划。例如，他们不必再执行配置 VLAN、负载平衡器或防火墙规则等日常工作，而是可以设计能够为企业增加价值的新服务：自动的跨域流程、恢复能力设计、容量规划或其他有趣的项目和计划。

此外，还应说明组织中的创新者和远见者有机会为网络连接和安全性转型贡献一己之力。结果将对那些推动转型的人员有益，就像对在 IP 网络和最近的计算虚拟化领域中构建和发展了职业生涯的人员有益一样。在这两种情况下，企业都获得了具备新技能和知识的新型管理人员。参与转型将会丰富员工的专业技能，增加他们在就业市场中的机会和价值。

推动与服务用户的主动接触

提升团队能力的另一种积极方法是让服务的使用者（例如，应用、业务或基础架构的所有者）参与进来，向他们讲授新功能。请他们积极参与并获取他们的要求和反馈。他们会希望了解功能和用户体验将会如何变化。一些成功的接触活动包括：

定期接触：定期召开研讨会以提供最新动态、收集要求和征集反馈。

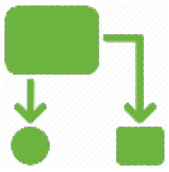
“行动胜过语言”：建立并传达团队会定期开发和发布新功能，这将提高客户的参与度。

在组织中传达成功信息是好的做法

除了向选定的团队成员和服务使用者推广项目之外，在业务线或整个组织中推广项目也不失为明智之举。这么做的目标是为项目争取广泛的群众支持，并建立起做实事的平台。分享有关项目带来的业务和 IT 成效的趣事。您可以综合运用演示文稿、对话、文章、博客文章、社交媒体、电子邮件或演示等方式来进行推广。团队里的每位成员都应该将自己视为项目的推广人员。宣传成功（无论大小）是高绩效组织的标志，并且应该被视为技术变革管理方面重要的最佳实践。

做出改变很难：寻求共识

众所周知，做出改变很难。在改变速度很慢的领域和学科，或者是改变被视为对职业或生活构成潜在威胁的地方，这一过程尤其艰难。这些因素可能会阻碍前进的步伐。有些人可能会积极反对转型。最佳方法是通过真诚的沟通和倡导以及宣传对组织的成功意义来寻求对网络虚拟化的潜在共识。您需要保持公开和透明，并愿意阐明和回答“对我有什么好处？对我们而言意味着什么？”等问题。



流程

在此部分中，我们将说明网络虚拟化对运维流程的影响，介绍您应采取哪些步骤来剖析和了解您的现有流程，并针对如何改进您的流程和工具以充分利用网络虚拟化和安全性提出建议。

清查和分析现有流程

网络虚拟化的一个关键价值主张是让与应用生命周期相关的典型手动流程实现自动化。这让您有机会全方位评估现有的流程，确定它们将如何与网络虚拟化共同发展。

重要提示：切勿在实施 NSX 网络虚拟化和安全性时简单地保留所有现有流程。如果这样做，您获得的好处和节约的成本将会减少。确定和了解您所有的现有网络和安全流程。了解网络虚拟化对以下流程的影响：

- 应用调配
- 配置管理
- 变更管理
- 容量管理
- 突发事件和问题管理

您将需要了解这些流程目前的运行状况，以及如何通过自动化和编排对它们进行简化。您会发现，现有的流程或步骤可以大大简化，甚至在一些情况下弃用。

在您全面了解流程之后，确定对这些网络和安全性流程实施自动化的优先考虑事项。为了迅速取得成效，您需要重点处理兼具高价值和低付出的领域。不要试图一次性简化过多流程；请从选择一个或两个开始。

流程最佳实践：基准分析

在开始之前，必须进行基准分析。在做任何更改之前，记录目前的流程时间作为衡量基准。计算每个流程的工作量和周期。在实施流程自动化之后，执行相同的衡量工作。现在，您可以就得出的结果进行比较和交流。了解性能有助于团队实现其目标（例如，缩短调配时间或者缩短检测并隔离问题的用时），还能帮助他们为用户制定合适的 SLA。

实施调配和管理自动化

对当前流程进行清查和评估之后，下一步是考虑实施应用或服务的调配和管理自动化。组织利用网络虚拟化和 NSX 固有的自动化功能，实现高速度、标准化、一致性和可审核性。自动化还可减少与手动配置错误相关的停机和安全性风险。自动化有助于提升开发和测试工作效率、缩短新应用的销售就绪时间、提供一致的标准化配置、减少错误发生率以及加快问题解决速度。

虽然 NSX 不需要自动化工具，但大多数客户会将各种工具和 NSX API 组合应用于云计算自动化。这些工具和 API 用于实施 NSX 功能性服务（即 L2 逻辑交换、L3 路由、负载均衡、防火墙和边缘服务）在虚拟网络中的调配和管理自动化。大多数使用 NSX 的组织会实施多个服务的自动化。

当前的一般情形是：仍然使用键盘和 CLI 在专用硬件上手动调配物理网络和 VLAN。结果是，网络变更成为阻碍应用部署的关键因素。如您所知，实施此类部署可能拖上几天、几周甚至更长时间，直到网络连接、性能、可用性和安全性全部就绪为止。

利用 NSX 向前迈进：组织利用 NSX 自动执行网络虚拟化和安全性的调配、配置、管理和停用任务。借助 NSX，网络团队不再需要配置大量具有流量引导功能和各种网络配置（如 VLAN、VRF、VDC、QoS、ACL 等）的物理交换机。

一旦作为底层网络的物理网络完成初始配置，就无需根据新的应用部署或不断变化的应用要求频繁地进行重新配置。现在，所有这些更改全部使用自动化工具在逻辑网络空间中执行。

流程最佳实践：专注 IT 自动化

建议您首先构建 IT 自动化，以加快其处理服务请求的速度。完成 IT 自动化后，可以添加一个自服务门户和服务目录，这样应用开发人员和 QA 工程师只需单击一下按钮即可访问整个环境。现在让我们来了解一些供 NSX 客户使用的自动化工具。

工具使用注意事项

如前所述，您必须首先确定、了解和记录要实施自动化的任务和流程。这是重要的一步，因为不同的 IT 自动化工具（如云计算管理平台和编排工具）提供不同的功能特性。所有这些工具都需要部分前期投资来学习和设置，而这些投入相比它们带来的好处都是值得的。

我们来看看 vRealize Suite 和 OpenStack 在网络基础架构的调配、管理和编排工作中的应用。首先从实施离散任务自动化开始，以熟悉工具。熟悉工具之后，您可以开始对在一个完整的堆栈中调配和管理应用及其网络连接和安全性的工作流实施自动化。网络操作员或云计算网络操作员应参与推动网络自动化的所有工具的评估和操作。

配置的标准化和自定义

组织可以利用模板和策略对完整应用体系的计算、存储、网络和安全性配置实施标准化。如果需要更改，只需修改模板，然后将新模板应用到生产环境中。所有使用该模板的工作负载将自动执行此更改。保留所有更改记录，以供审核和确保合规性。

工程人员可以发布静态和/或可自定义的配置。静态环境通常用于经过生产认证的堆栈。而可自定义的环境则用于开发和测试沙箱。可自定义环境能够解决 80% 或更多的用户要求，而开发人员或 QA 工程师可以按需更改环境配置。工作负载可以在新网络上运行，或连接到现有网络。

蓝图流程自动化示例

让我们来看看在一个标准化的三层应用蓝图中，有哪些任务可以实施自动化：

蓝图经过测试和验证之后，即发布到服务目录中以供用户使用。用户只需单击服务项，整个应用体系（包括所有连接、可用性和安全性）即可在数秒内完成部署。

此自动化服务比没有应用 NSX 的传统物理网络（一般需要几天或数周）快数倍。组织可以避免复杂的问题请求工作流、变更审核和批准、冗余需求调查和验证以及手动配置带来的较长周期和延迟。

流程最佳实践：基于角色的访问

基于业务角色对自服务门户实施基于角色的访问控制。此外，您还应根据业务组定义资源预留和分配策略、跟踪退单成本并致力于满足服务级别协议 (SLA) 的要求。

实施组安全策略自动化

NSX 自身能够自动执行许多任务，而这些任务在物理网络和安全基础架构中需要手动执行。例如，它提供了全新的方法来定义安全策略并将其应用于虚拟化层中的虚拟机。

旧方法：过去，安全团队基于 IP 地址、端口和协议手动创建规则。“5 元组”造成可怕的管理噩梦。

新方法：现在则基于安全组部署安全策略。您可以定义一个包含一组虚拟机的安全组，然后针对这些工作负载创建安全策略。这样，在向该安全组添加虚拟机时，安全策略会自动应用于新的工作负载，而无需任何手动干预。可以通过安全标记和/或上下文动态应用组成员资格。NSX 安全策略包括防火墙、防病毒和 IPS 等。

安全组可以是静态的或动态的 - 可经过编程，以便仅触发与工作负载相关的任意元数据。例如，用户组身份、操作系统特征、虚拟机名称和标记、病毒等。NSX 基于虚拟化相关上下文（而非物理拓扑）自动分配适当的安全组和策略。

对预先批准的安全策略进行集中编排和管理，这不仅可以减少规则剧增的情况，还能确保准确、一致地应用安全机制。此全新级别的自动化可以大幅降低跨工作负载管理安全策略的操作复杂性和费用支出。

每个安全团队都使用多种网络安全设备的独特组合来满足其环境需求。除了 NSX 的分布式防火墙功能，组织还应利用这一平台实现 VMware 技术合作伙伴提供的高级网络安全功能的自动化。

网络安全团队经常面临协调多个供应商提供的完全不相关的网络安全服务之间的关系的挑战。NSX 可以实现这一点。NSX 将网络服务分发到虚拟网卡环境中，以形成一个应用于虚拟网络流量的逻辑服务管道。可以将第三方网络服务插入此逻辑管道中，以允许使用物理或虚拟服务。企业使用 NSX 构建策略，这些策略利用 NSX 服务的插入、串联和流量引导功能推动服务在逻辑管道中的执行。

此外，集成的安全工具也将受益于 NSX 平台提供的运维模式。此类集成可以大幅提高调配速度、管理效率和服务质量，同时将服务器、网络和安全团队的职责分离。

高级安全功能可以通过与 Palo Alto Networks、Intel Security、Trend Micro、Symantec、Checkpoint 以及其他一些 VMware NSX 合作伙伴的产品集成来获得。

使用新式工具创建应用级可见性

Hypervisor 完美而独特地位于物理环境和虚拟环境的交界处。由于 NSX 虚拟交换机可以看到每个进出虚拟机的数据包，因此，它能提供最高级别的可见性和上下文。它还能将应用、虚拟网络、物理网络等内容之间不断变化的关系关联起来。

以下示例场景为您展示 NSX 独特的监控和故障排除功能：

实时摘要	监控和故障排除	调试
操作员可以选择任意虚拟机的网络接口，查看所有流量及其状态的实时摘要。寻找虚拟机时，无需为远程工具配置完整的数据包捕获以及筛选 IP 地址。	虚拟网络的方方面面均通过 NSX 的中央 CLI 和中央 API 获得。由于无需再判断进行问题排除的网络位置，这极大地简化了监控和故障排除活动。此外，执行故障排除时也无需在不同的控制台之间来回跳转。	每个数据包均在软件中由虚拟交换机处理，这为您提供优于传统网络的可见性。无需访问客户虚拟机，即可创建综合事务。可在转发管道中注入 Traceflow 数据包，以便在数据路径中执行精细的问题调试（例如，过度限制性 ACL 策略）。

操作员现已使用许多工具来管理和支持数据中心基础架构。他们使用不同的工具执行监控、故障排除和变更管理活动。借助网络虚拟化，使用现有的工具集也可以获取逻辑网络可见性。

实时监控工具对不断变化的虚拟化环境非常重要，在这些环境中，基础架构和应用在服务器之间动态迁移，并且网络自动重新配置。

流程最佳实践：工具

确定有助于您了解虚拟和物理计算、存储和网络基础架构之间的对象关系的 VMware 或第三方工具。基础架构域之间的相关性有助于将问题范围快速缩小到特定域，从而无需使用多个特定于域的工具。

一般情况下，针对虚拟和物理环境专门设计的新式工具是最佳选择，如 vRealize Operations、Arkin、Riverbed 等。这些工具可提供端到端的拓扑、应用运行状况、利用率和容量视图。

请注意，单一供应商的解决方案可能并不能提供最好的可见性。多种工具组合可能是实现最优监控、警报和故障排除的最佳方案，物理网络目前也是如此。例如，您可能将不同的工具用于流量分析（如 SolarWinds、NetQoS）、数据包分析（如 Wireshark、SteelCentral）和警报（如 Netcool、OpenNMS）。

虚拟网络通过标准协议提供与物理网络相当的检测水平（例如，通过 SNMP 和 API 的数据包和字节统计信息、SPAN/L3 SPAN、NetFlow/IPFIX、端口镜像和 Syslog）。这使得组织可以从现有的监控、警报和故障排除工具开始，随后过渡到新式工具（如前文所述）。

关于流程的结束语

网络虚拟化和 NSX 为您评估现有流程提供了充分的理由，并明确了一个更好、更高效的方法向前推进。修整所有流程的庞大工程也许令人怯步：可采取渐进式方法构建自动化流程以避免工作中断。精益的持续改进方法是最好的工作推进方式。

技术

在本节中，我们将探索规划、部署以及实施网络虚拟化和 NSX 过程中的体系结构和基础架构考虑事项。我们还将讨论与微分段和灾难恢复相关的实际用例。

设计简单的物理网络

对 NSX 而言，物理网络的体系结构设计仅是为了实现连接和性能。它可以像您当前使用的 L2 结构那样简单，也可以是一个基于“分支-主干”体系结构的 L3 结构。您可以从前者开始，逐渐向后者过渡。

NSX 没有对 L2 的边界位置进行严格要求。由于物理网络只是提供主机之间的连接而已，因此，应相对减少物理网络的配置更改。这样有助于避免手动配置错误。

网络服务和拓扑与物理硬件相分离的设计，使 L3“主干-分支”结构得到广泛应用。这使得您可以建立一个采用相同逻辑网络连接、安全和管理模式的公共平台。

通过从物理拓扑中提取虚拟机监视到的虚拟网络拓扑，NSX 使更改网络体系结构变得更加容易。借助 NSX，网络设计人员能够更轻松地向使用 L3 路由，且在架顶式交换机之间采用非阻断 ECMP 的“主干-分支”体系结构转变。

底层物理网络可以独立于虚拟网络不断演进发展，其体系结构设计遵循可扩展性、吞吐量和稳定性标准。单个设备或链路故障不会影响应用连接。

ECMP L3 结构设计可实现配置一致性，并加强设备的互操作性。可以脱离 NSX 进行硬件升级（例如，部署新交换机），以避免对虚拟网络上正在运行的工作负载造成影响。NSX 支持来自任何供应商的交换机，并且这些交换机可以互相连接在一起。

网络虚拟化覆盖结合“主干-分支”体系结构能够实现更强大的恢复能力和更高的运维效率，提高带宽使用效率和可扩展性，以应对数据中心内不断增加的东西向通信量。与此同时，较小的 L2 广播域则能够增强网络的稳定性。

循序渐进地实施网络虚拟化

NSX 网络虚拟化并非一种“要么全搞，要么都不搞”的方案。NSX 虚拟网络不需要更改底层物理网络。网络虚拟化可以与物理网络上现有的应用部署实现透明化共存。

技术组织可以灵活地对网络的各个部分进行虚拟化，而只需向 NSX 平台添加 hypervisor 节点。此外，NSX 软件网关或架顶式交换机（即来自 VMware 合作伙伴的硬件）能够在虚拟网络与物理网络之间建立无缝互连。可以使用这些网关来支持连接到虚拟网络的工作负载进行 Internet 访问，或者将传统 VLAN 和裸机工作负载直接连接到虚拟网络。

技术最佳实践：从一个项目开始

您应循序渐进地推进网络虚拟化和安全性。我们建议您从一个用例和一组应用开始。确定具有可观风险报酬系数的工作负载以利用新功能。第一次实施时，选择风险较低的工作负载，但它同时应具备足够的复杂性，以实现在您的环境中验证 NSX 的目的。

您选择实施的用例将在很大程度上决定在您的虚拟网络中对哪些 NSX 功能性服务实施自动化。例如，如果您要实施网络调配自动化，需要首先对 L2 逻辑交换、L3 路由和边缘服务实施自动化。如果您要实施微分段自动化，则需要从实施逻辑防火墙自动化开始。

确定一个策略和方法，以不断地向您的客户推出新的 NSX 功能特性。建立一个规律性的节奏，让业务团队有所期待，并让他们相信他们的项目能够从新功能中获利。您会发现，定期发布新功能更有利于提高用户参与度、服务质量和客户满意度。不断提升服务质量，而非试图强硬地推动大规模采用。

技术最佳实践：研讨会

与所在组织内的业务和技术同行保持互动是确保每一步计划（包括网络虚拟化）取得成功的绝佳方法。考虑开展有用户参与的定期研讨会，以就所提供的网络虚拟化和安全服务对相关人员进行宣传引导，并让他们了解您的最新路线图计划。鼓励应用和基础架构所有者携手合作，提供他们对未来版本的要求以及对现已在生产环境中提供的各项功能的反馈。

用例：应用边界处的分段

微分段是大多数 NSX 客户在早期执行和实施的一个主要用例。长期以来，微分段被视为安全体系结构的最佳实践。当攻击者在未经授权的情况下接入网络时，分段的应用有助于限制他们的行动和防止数据泄露。然而，在过去，微分段并没有实现广泛应用。这缘于传统物理网络中的体系结构限制使微分段难于实施。

NSX 使微分段在操作上变得可行。该平台自身具有隔离和分段功能。高级服务插入功能使第三方安全设备得以利用 NSX 操作模型。

隔离是大多数网络安全机制的基础，无论是为了确保合规性、控制力，还是仅仅用于防止开发、测试和生产环境之间发生交互。虚拟网络彼此隔离，并且在默认情况下与底层物理网络隔离，除非专门连接在一起。操作员不需要处理任何物理子网、VLAN、ACL 以及防火墙规则。

分段与隔离相关，但应用于多层虚拟网络中的各个层。过去，网络分段是物理防火墙或路由器的一项功能，旨在允许或拒绝各网段或各层之间的流量。例如，路由器和防火墙对 Web 层、应用层和数据库层之间的流量进行分段。

当今的挑战：过去，配置分段的过程需要手动操作，非常耗时，而且极易出现人为错误，从而导致安全泄露。实施过程需要具备设备配置语法、网络寻址、应用端口和协议方面的专业知识。

网络虚拟化解决方案：对于 NSX，安全策略应用于虚拟化层。您可以摒弃各种东西向流量迂回技巧。安全机制甚至在数据包到达第一个虚拟网络端口之前就已透明启用。由于一开始就被保护起来，延迟敏感型东西向流量得以从延迟最低的路径直接传输到目的地。

集中控制与分布式的服务实施方法相结合，意味着可以通过操作上可行的方法将非常精细的策略应用于每个虚拟接口。例如，对于一个三层应用，同一层中的虚拟机可以与其他层通信，但它们相互之间却不能通信。实际上，每个工作负载都有自己的安全机制。

NSX 允许您基于高级业务结构（如应用、用户或组）而非低级基础架构结构（如 IP 地址、应用端口和协议）设置安全策略。由于无需人为解读，安全策略的应用可以更加精准，并更好地与企业策略保持一致。

工作负载移动性和可恢复性设计

过去，物理网络拓扑和地址空间要求 IT 在移动应用时更改 IP 地址。有时，IP 地址被硬编码到应用中，由于需要更改代码和进行回归测试，成本变得更加高昂。

NSX 将工作负载从 VLAN 和 IP 寻址中释放出来，可实现工作负载在整个数据中心结构中的无限制移动和安置。使用 NSX 后，工作负载的安置将不再依赖于指定位置的物理拓扑及物理网络服务的可用性。

从网络连接角度来看，无论虚拟机所处物理位置如何，它所需要的一切内容均通过 NSX 提供。工作负载可在子网、可用区或数据中心之间自由移动，运维人员不必重新为其设置 IP 地址。如果移动了某个工作负载，则该工作负载的所有网络和安全服务会自动随之移动，无需人为干预。

组织利用 NSX 工作负载移动性和安置来执行如下操作：

- 更快地调配应用
- 将工作负载迁移到新数据中心
- 更新或刷新底层物理基础架构

用例：利用网络虚拟化提高服务器资源利用率

组织还将 NSX 用于访问当前数据中心的其他位置或另一个数据中心提供的服务器容量。这将显著提高服务器资源利用率和整合率。所有这些用例都能大幅降低运维成本并提高敏捷性，从而增加网络虚拟化和 NSX 投资的总体价值。

在传统网络拓扑中，每个集群或单元都有自己的服务器容量。将网络再配置为可从其他单元或集群加以访问的过程十分耗时，且容易出现人为错误。可用的服务器容量也将被白白浪费掉。我们有时将这类容量称为“隐秘的服务器容量”，因为它不易获取。实际上，传统网络拓扑和设备的复杂性限制了技术部门的能力，以致于他们无法更好地利用可用服务器容量。

借助 NSX，您可以通过扩展网络来访问数据中心内任意位置提供的容量。无需对现有物理基础架构进行更改。要向不同子网或可用区中的服务器添加另一个虚拟机，只需启动该虚拟机并将其连接到逻辑交换机。这两个工作负载现在呈 L2 相邻，尽管它们将跨越物理网络上的多个子网和可用区。

用例：灾难恢复

您还可以使用 NSX 来完善现有灾难恢复解决方案。使用传统网络连接方法时，要利用备份站点进行灾难恢复就需要在成本和功能之间取得平衡。相对在另一个位置按原样重现网络拓扑和服务，大多数组织都会选择一款所谓“出色”的解决方案。他们往往会通过削弱主要数据中心相关功能的方式来折中实现降低成本的目的。

NSX 实现了不折不扣的灾难恢复。借助 NSX，您可以为整个应用体系结构（包括网络连接和安全性）创建快照，而不仅限于虚拟机。将副本发送至处于备用状态的灾难恢复站点，此副本可以位于任何硬件上，但不能存在任何功能缺陷。

发生灾难时，只需将虚拟机投入运行即可。恢复站点已在运行该虚拟机希望连接的网络。您的恢复时间目标将大幅缩短，因为您无须为工作负载和安全设备重新配置新的 IP 地址。

有关技术考虑因素的最终想法

网络虚拟化和 NSX 为您的技术环境带来了极大的灵活性。它可以提供大量重要的用例。不要被这些可能性搞得不知所措，要记住，一开始应先关注服务质量。扩大首个用例的影响，然后选择第二个要实施的用例。仅当您的团队和用户均对质量水平感到满意时，再提供新功能。

后续步骤

应将实施网络虚拟化和安全性视为一段旅程。在此期间，随着您转向软件定义的数据中心并向业务增添更多价值，您的组织也不断变得更加成熟和复杂。

您的组织和各个团队成员可以通过多种途径来了解如何实现网络虚拟化和 NSX 提供的全部运营优势，以及网络虚拟化和 NSX 如何适应和完善 IT 组织其余人员的要求。

步骤一：学习

首要步骤是向组织和个人提供学习机会。综合不同形式的培训和学习，包括正式（如研讨会、课程、动手练习、计划）和非正式（如午餐交流会、辅导、指导）的活动。为了激发学习兴趣，请设法将培训和学习目标纳入个人 MBO 中。

首先，您的团队可以参加 VMware 动手练习 (labs.hol.vmware.com)，以及由 VMware Education (vmware.com/education) 提供、由讲师指导的研讨会和课程。此外，VMware 还提供了 NSX 操作指南，重点介绍了监控和故障排除。

步骤二：转型服务

寻求旁观者的观点以帮助向网络虚拟化和 NSX 过渡，可以显著加快整个流程。VMware 提供了运营转型服务及相关的研讨会 (vmware.com/consulting)。例如，“网络即服务 (NaaS) 展望”研讨会可帮助您明确新网络和安全运营模式的愿景、目标和目的。而在“NaaS 发现”研讨会的帮助下，您可以确定需要增强或创建哪些运营和组织功能，从而实现新运营模式以及预期目标和成效。

步骤三：简单试用

要了解 NSX 及其实施方式，其中一个最佳方式是利用一个用例和多个工作负载来启动生产试验。选择风险较低但又足够复杂的工作负载，以便您充分了解 NSX 的实施方式。

请联系您的 VMware 或合作伙伴客户代表，以帮助您开始体验。

附录

最终状态性能特征

下表从人员、流程和技术角度总结了 NSX 实施的最终状态特征。您可以将此作为旅程指南：

向量	当前/开始状态	未来/最终状态
组织结构	• 界线分明，各自为政，不得不处理多项繁重的流程 • 正式的请求规程 • 踢皮球 • 相互指责：我们和他们 • 目标、目的和激励不同且不一致	• 通过直接交互形成融合 • 开放的交流 • 精简的反馈流程 • 高度协作 • 共同的目标和 KPI • 共同的风险和职责
人员	• 专业化 • 专业知识局限于一个领域 • 使用 CLI 和脚本 • 广泛可用的知识 • 职业发展受限 • 以硬件基础架构为中心	• 跨领域和学科 • 具有多个领域的专业知识 • 使用 API 和自动化工具 • 持续学习 • 有机会通过战略项目形成业务影响 • 以服务和应用为中心
流程	• 手动流程，容易出错 • 复杂的请求支持系统 • 需要协调和交接 • 存在复杂性和瓶颈 • 等待服务部门响应 • 高 OPEX • 以基础架构为中心	• 自动化、标准化、一致且可审核 • 降低人为错误带来的风险 • 缩短周转时间/受 SLA 支持 • 实时交互 • 降低 OPEX • 以服务或应用为中心
工具使用	• 传统，特定于领域 • 孤立，有多款工具 • 仅物理工具 • 以基础架构为中心 • 难以隔离服务问题 • 各个组件 CLI	• 新式的跨领域工具 • 针对虚拟和物理工具而设计 • 以应用为中心 • 集成式基础架构和服务监控 • 易于隔离服务问题 • 针对工具基础架构的集中式 CLI 和 API
体系结构	• 经典的 3 层体系结构限制 • 工作负载限制 • 检查点防火墙 • 超额预定的核心 • 链路性能 • 集中化、受限于位置的服务	• 采用非阻断 ECMP 的主干-分支结构 • 以松耦合和抽象化覆盖 • 工作负载可移植性和可移动性 • 本机隔离和分段 • 可扩展性和恢复能力 • 分布式服务
基础架构	• 物理基础架构，底层变化缓慢 • 受限于基础架构的安全性	• 虚拟基础架构，覆盖层呈动态变化 • 以应用为中心的安全性

向量	当前/开始状态	未来/最终状态
	• 缩减的“足够好”的 DR • 人为解读策略 • 以基础架构为中心的策略 • 低级基础架构结构 • 管理分散 • 局限于一家供应商的硬件 • 难以执行服务链功能	• 不折不扣的 DR • 可供虚拟机读取的安全策略 • 以业务为中心的策略 • 高级业务结构 • 集中化的管理 • 高性价比之选 • 易于执行服务链功能

云计算网络连接和安全性角色

以下说明可帮助您定义云计算网络连接和安全性员工的角色和职责。这些云计算角色由“传统的”网络和安全领域的专业人员担任；即，由团队中的既有人员担任。

在中小型企业中，一人同时分担两个或更多角色的做法十分常见。例如，一名网络工程师可能要兼任网络架构师、开发和/或运维人员。当然，并非所有组织都需要不同人员来担任各个不同的职位。

与此形成鲜明对比的是，大型企业的常见做法是多人担任同一/类似角色。例如，我们了解到许多跨国公司拥有多名云计算网络架构师或云计算网络工程师。

云计算网络连接角色

云计算网络架构师 (CNA) 负责根据基于服务的使用模式（网络即服务）开发端到端的云计算网络体系结构和标准。CNA 的职责如下：

- 确定技术和运营方面的网络要求
- 设计满足应用要求（例如容量和性能）的物理和逻辑网络
- 开发和验证测试，以确保满足所有要求
- 对规划和实施云计算网络解决方案提供指导

云计算网络工程师 (CNE) 负责网络服务和基础架构的详细设计、网络功能的开发和测试、容量调配以及定义网络配置。CNE 的职责如下：

- 确保达到客户的要求及相关服务级别
- 将要求转换成逻辑蓝图和配置模板
- 为日常任务（如集成、开发、监控和合规）设计、开发和测试自定义流程和脚本
- 协助第 2 级和第 3 级支持进行故障排除，同时建议相应的解决方案并请求解决办法

云计算网络操作员 (CNO) 全面负责后续运维的各个方面，满足应用运维要求（如性能和容量）并维护云计算网络基础架构、工具和平台。CNO 的职责如下：

- 执行和控制调配、管理、监控、警报和故障排除的自动化
- 主动监控云计算网络基础架构，并在服务受到影响之前对事件采取操作
- 执行故障排除和根本原因分析，并应用 CNE 建议的解决方案和修复办法
- 提供第 2 级和第 3 级支持，并管理突发事件、难题和上报

云计算安全性角色

云计算安全架构师 (CSA) 全权负责云计算安全基础架构的架构、设计和支持事宜的各个方面。跨网络安全性执行虚拟化、自动化、编排和监控。CSA 的职责如下：

- 评估云计算基础架构和应用的安全风险，并针对安全战略和解决方案提供权威性指导
- 从技术层面确定满足云计算安全性要求和目标所需的安全策略、流程和审核功能
- 开发验证测试以验证云计算安全解决方案，规划实施并提供实施指导
- 对降低威胁和风险的相关战略保持全面了解

云计算安全工程师 (CSE) 负责将安全性策略转换为可以审核的安全性控制。CSE 的职责如下：

- 设计并实施可对云计算安全性进行控制的物理和逻辑解决方案
- 编排并自动执行云计算安全流程（控制、监控和审核）
- 集成和实施可达到一定要求和服务级别的云计算安全服务和工具
- 参与上报、调查违规事件，推荐和实施修复解决方案

根据组织策略和风险评估，*云计算安全操作员 (CSO)* 负责了解、实施、强制执行、验证和维护特定安全控制。CSO 的职责如下：

- 监控、检测和分析安全异常、漏洞和威胁
- 管理安全日志、确保符合日志记录标准并协助进行安全审核
- 发生突发事件时，调查、诊断和解决云计算安全问题
- 实施安全解决方案并修复漏洞

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
威睿信息技术（中国）有限公司
中国北京海淀区科学院南路 2 号融科资讯中心 C 座南楼 1 层 邮编：100190 电话：+86-10-5993-4200
中国上海办公室 上海市淮海中路 333 号瑞安广场 15 楼 1501 室 邮编：200021 电话：+86-21-6034-9200
中国广州办公室 广州市天河路 385 号太古汇一座 3502 室 邮编：510610 电话：+86-20-87146110
中国香港公司 香港港岛东太古城太古湾道 12 号太古城中心 4 期 4 楼 电话：852-3696 6100 传真 852-3696 6101 www.vmware.com/cn