使用 VMWARE NSX DATA CENTER 实现多云网络连接

企业数字化转型面临的挑战

由于组织要满足不断增长的基础架构需求并实施冗余计划，许多组织已经采用多数据中心策略。RightScale 进行的 2018 年云调查表明，81% 的受访者采用多云策略，各组织所利用的云环境数量平均约为五个。[1] 就跨整个数据中心管理、保护、连接和维持合规性而言，IT 组织常常面临着严峻的挑战。这些数据中心通常需要手动重新配置网络，以在数据中心站点或云环境之间实现移动性。

各组织都在采用成本高昂的灾难恢复计划来保护关键任务应用并减少潜在的重大收入或业务运营损失，设法做好准备以应对从自然灾害到网络攻击的一切情况。2016 年的一份报告指出，数据中心故障造成的平均损失为 740,357 美元[2]，与此同时，其他公共故障造成的损失高达 1.5 亿美元。一直以来，业务连续性和灾难恢复 (BCDR) 计划都比较复杂、在运维方面颇具挑战性，或者根本不存在。随着应用的分布性日益提升，可能需要数小时甚至数天来手动进行重新配置以便进行故障转移。

企业转而采用公有云以提高敏捷性和可扩展性，因此面临着大量挑战。公有云拥有自己的网络连接和安全性结构以及策略管理。这会导致出现一系列新的技术小环境，从而增加费用、复杂性和风险。多元化网络拓扑、安全性模式和管理环境以及不同的软件版本都可能为实现移动性和互操作性带来障碍，从而降低云的采用速度并导致使用情形受限。

“借助 VMware NSX Data Center，我们创建了一个安全的世界级数据中心体系结构，有了它，信用合作社将能够提供新一代成员服务。无需停机，我们将可以节省成本并简化管理。”

AMY HYSELL
高级副总裁兼首席信息官
亚利桑那州联邦信用合作社

打破网络障碍

要克服这些挑战，IT 部门必须采用现代网络连接解决方案，以提供跨异构站点的网络连接一致性和安全性，以及自动化级别（以简化多云运维）。

VMware NSX® Data Center 将底层硬件的网络运维提取到分布式虚拟化层上，从而实现以前在物理网络中无法达到的较高敏捷性、安全性和经济性级别。交换、路由、防火墙和负载均衡等网络服务更贴近应用并且分布在整个环境中。

NSX Data Center 和 VMware NSX® Cloud 强强联手，通过允许 IT 管理员拥有多个私有云和公有云环境，同时针对网络功能和一致安全性制定一项统一策略，来创建混合云模式以实现网络连接和安全性。该解决方案能够在适当情况下延伸数据中心之间的第 2 层域，从而跨多个站点维护应用的 IP 地址并支持故障转移场景。这样一来，不必再手动配置和重新配置网络，通过网络自动化即可实现出色的运维效率。网络和安全性策略与应用环境绑定，因此它们在整个生命周期中保持应用到单个工作负载。

1 State of the Cloud Report，RightScale Inc.，2018 年 www.rightscale.com/2018-cloud-report

2 Cost of Data Center Outages，Ponemon Institute，2016 年 1 月 https://www.ponemon.org/blog/2016-cost-of-data-center-outages

关键要点

- 提供统一网络连接和安全性模式，利用这种模式，不必再手动配置和重新配置网络，通过网络自动化即可实现出色的运维效率
- 使组织能够在极少停止甚至不停止应用运行的情况下，将虚拟机或整个数据中心从一个位置迁移到另一个位置
- 帮助实现安全、无缝的应用移动性，从而轻松向云或从云进行迁移或者在物理站点之间迁移

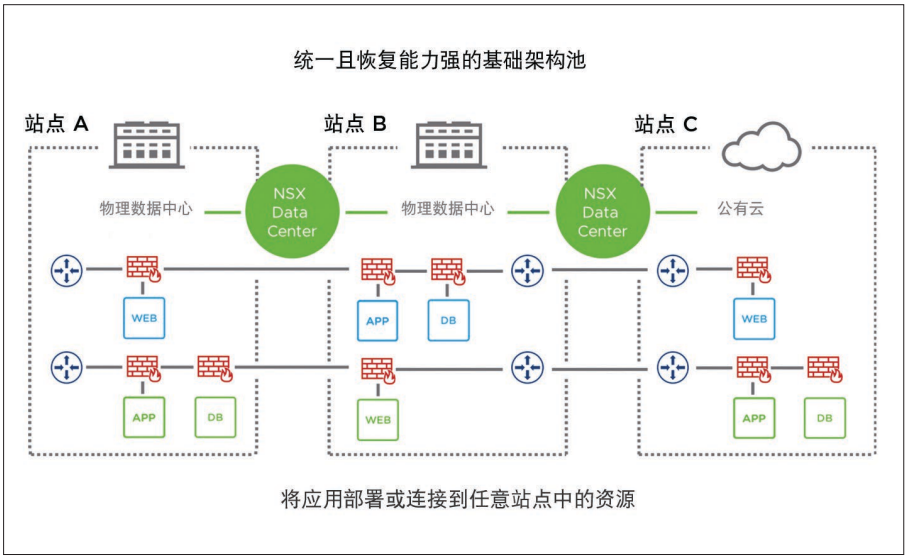

图 1. 使用多站点池化功能最大限度降低故障影响

关键客户场景

数据中心延展

NSX Data Center 可将本地数据中心无缝延展到其他物理站点以及使用 NSX Cloud 的云中，使组织能够充分利用规模、冗余和经济性优势。此外，使用 VMware NSX Hybrid Connect，IT 管理员可以在 VMware vSphere® 环境之间安全、无缝地移动应用，实现零停机实时迁移以及停机时间较短的计划内大规模迁移。

NSX Data Center 通过将服务绑定到应用工作负载来维护应用的网络连接服务（如相同的 IP 地址、安全性策略和其他服务），能够实现快速迁移和故障转移。因此，与工作负载相关联的 IP 地址和安全性策略（基于虚拟机 (VM) 或容器）在工作负载以动态方式从一个位置移动到另一个位置时保持一致。

利用 NSX Data Center，用户还可以采用加密方式安全地访问专用企业应用 (SSL VPN) 以及 NSX Edge 网关和远程站点（采用来自其他供应商的可选 VPN 网关或硬件路由器）之间的站点间连接 (IPsec VPN)。

灾难规避和恢复

现代数据中心设计需要实现更好的冗余，并且需要能够在发生灾难性故障时实现业务连续性和灾难恢复 (BCDR)。要求实现高应用可用性的组织可依赖与灾难恢复（主动-被动部署）相反的灾难规避策略（主动-主动部署）。

NSX Data Center 可跨受保护站点和恢复站点提供一致的逻辑网络连接和安全性，从而降低灾难发生时的恢复时间目标。由于网络和安全性跨多个站点保持一致，应用可以在恢复站点中恢复并保留其网络 (IP) 和安全配置。此外，NSX Data Center 可轻松创建测试网络，以在测试恢复计划时利用，且不会影响生产环境。

在灾难规避的环境下，多站点池化功能可创建统一、无缝且恢复能力强的基础架构池，以便跨多个数据中心运行应用以及将应用迁移到云（由一致的单一网络连接平台启用）。同样，应用可以部署在任何位置并连接到位于各站点的资源，以实现灾难规避、应对计划内/计划外故障或提高资源利用率。

工作负载移动性

工作负载经常需要在站点之间移动，以执行数据中心迁移、整合、数据中心升级/安全修补、云登录、云突发和灾难规避等任务。

NSX Data Center 和 NSX Cloud 通过将 IT 组织在其基础架构上使用的相同虚拟化网络和安全平台延展到云中，实现工作负载无缝移动，从而为私有和公有云资源提供单一网络连接和安全性配置。这样一来，企业便能够在运维继续向公有云模式转变时做好准备，确保工作负载及其策略可在不同环境之间移动并保持一致性。

生产应用可以移动到公有云以便开始利用原生云服务，无需进行任何复杂转换，也无需重新设计。在基于 vSphere 的云和 NSX Hybrid Connect 之间进行的迁移可以更加快速，从而可以实现大规模和零停机迁移方案以及站点间持续网络路由。

组织能够无缝地将工作负载从一个位置移动到另一个位置（从数据中心移动到数据中心，或从数据中心移动到云），无需担心虚拟机格式兼容性。NSX Hybrid Connect 能够自动将映像转换为所需的云格式，因此，可以轻松放置或迁移虚拟机。

小结

VMware 提供现代网络虚拟化解决方案，以便跨异构站点提供一致的网络连接和安全性。因此，NSX Data Center 可实现大量的多云使用情形，从无缝数据中心延展到多数据中心池化，再到工作负载快速移动。全球客户都依赖 NSX Data Center 及其多云网络连接功能来构建能以最佳方式运行数以万计工作负载的可靠、灵活、敏捷且高度可用的数据中心环境。

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
中国北京办公室 北京市朝阳区新源南路 8 号启皓北京东塔 8 层 801 邮编：100027 电话：+86-10-5976-6300
中国上海办公室 上海市淮海中路 333 号瑞安大厦 805B-809 室 邮编：200021 电话：+86-21-8024-9200
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