服务器虚拟化技术在NSTL的应用实践

□ 张婧 关越 / 中国科学技术信息研究所 北京 100038
胡铁军 / 国家科技图书文献中心 北京 100038

摘要：随着网络化、数字化文献信息量的不断增长，文献信息服务机构的数据中心一般都会拥有一定数量的服务器和至少TB级的存储容量。如何利用更有效的技术手段以支撑数据中心未来业务的快速发展与高效管理，构筑能够更好地适应业务信息系统的平台，使IT系统真正成为提升业务能力的竞争武器，是目前对IT系统进行虚拟化规划改造的主要目标。本文介绍了NSTL利用服务器虚拟化技术开展的具体应用实践。

关键词：虚拟化，数据中心，云计算，网络
DOI：10.3772/j.issn.1673—2286.2013.11.011

1 引言

服务器虚拟化技术旨在通过运用虚拟化技术充分发挥服务器的硬件性能，为信息化业务的快速部署提供标准平台，降低IT固定资产的运营成本，对服务器资源、计算资源、存储资源进行动态分配，从而提高资源的利用率。如今虚拟化已成为数据中心变革的助推器，越来越受到人们的广泛关注。

NSTL数据中心拥有近百台应用服务器，承载着文献服务系统、数据加工、联合联机编目、文献综合等业务系统，数据量在逐年增长。2012年，NSTL在业务体系中部署了虚拟化，利用虚拟化技术将资源池化，增加了业务部署的灵活性和便捷性，缩短了应用部署周期，有效控制了设备采购成本，解决了原有系统中资源分布与应用需求不匹配及部署僵化的问题，并逐步实现了业务系统整合和数据的集中统一备份，为下一步向云计算迈进积累了宝贵经验。

2 服务器虚拟化技术的优势

传统服务器与应用一对一的部署方式相对服务器虚拟化部署应用在资源的有效利用及系统的管理维护上，前者存在很多难以解决的问题，包括扩展性、可用性、灵活性、应用兼容性等问题。而这些问题在基于服务器虚拟化的基础平台系统部署规划中能够很方便地解决，并且效果十分明显。在一个构建了弹性资源池的服务器虚拟架构中，用户可以把资源看成是专属于自己的，管理员则可在企业范围内管理和优化整个资源。

虚拟化架构的优势可以让IT部门达成以下目标：

（1）实现TCO（Total cost of ownership）的节省

通过整合多个物理服务器到一个物理服务器，降低约40%的软硬件成本；每个服务器的平均利用率从5%-15%提高到60%-80%。

（2）提高运维效率

将所有服务器的资源整合统一进行管理，并按需自动进行动态资源调配，无中断的按需扩容，不再担心旧系统的兼容性、维护和升级等一系列问题，业务连续性也会得到极大的保证。

（3）减少硬件支出

虚拟化技术可以将剩余的计算资源整合到一起再加以利用，硬件支出可以相对减少。

（4）满足不同应用对系统资源的不同要求

采用虚拟架构后，由于每个虚拟机所需使用的系统资源都是由虚拟架构软件统一进行调配，这种调配可以在虚拟机运行过程中在线实时地发挥作用，使得任何一个应用都可以有充分保证的资源来稳定

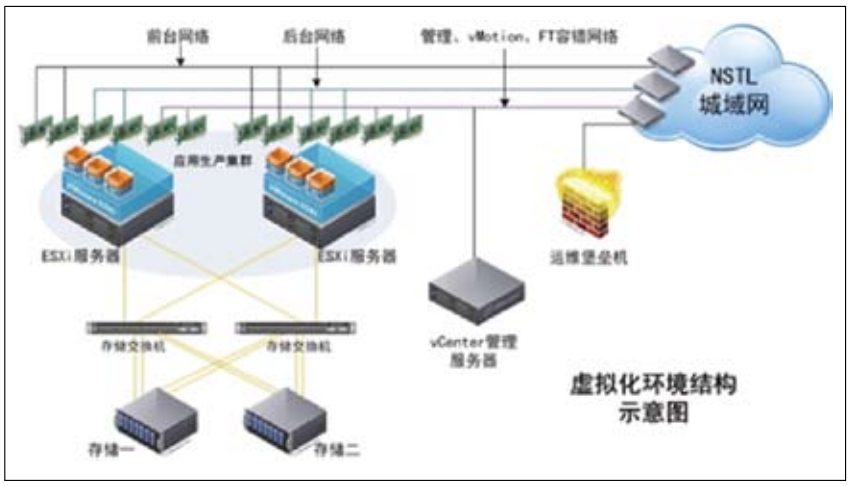

图1 虚拟化环境结构示意图

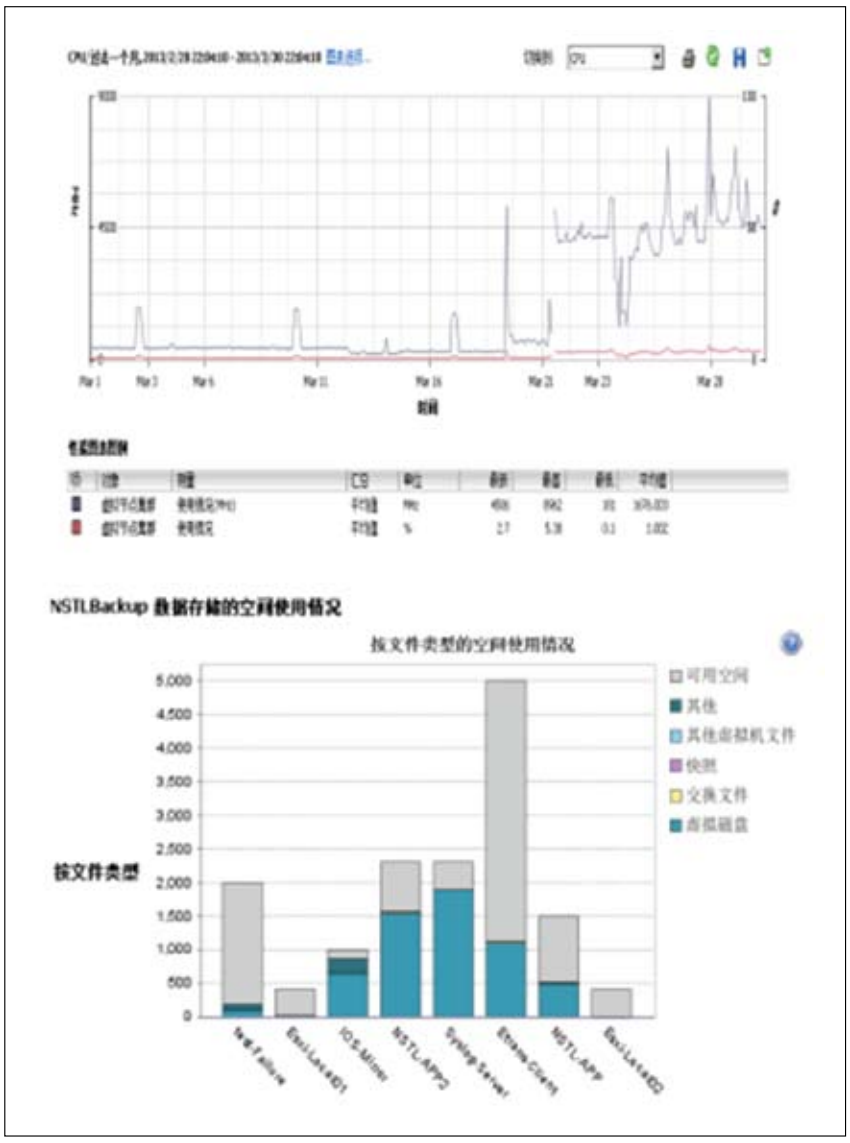

图2 虚拟节点集群单月CPU、内存、存储性能图表

运行。同时，某些应用在此时用不到的资源又可以被其他更需要资源的应用临时借用过去，最大限度地提高系统资源的利用率。

3 NSTL虚拟化应用的特点

NSTL虚拟化环境由应用生产服务器（ESXi Server物理机）、虚拟数据中心管理服务器（vCenter物理机）、SAN存储阵列、运维网关堡垒机和若干物理交换机构成。每台物理服务器安装有VMware vSphereESXi裸机虚拟化管理程序，配置了8个千兆网口，分别用于虚拟机的业务应用网络、ESXi服务器的管理网络、vMotion心跳网络及容错日志记录网络。每台服务器通过HBA卡与存储形成了冗余FC SAN环境。同时，还基于iSCSI协议，通过专用IP网络形成了IPSAN环境，以增加虚拟化环境的灵活性和扩展性。另外，考虑到虚拟化环境中每个虚拟机的操作安全，在虚拟化环境网络中还部署了一台“运维网关”，实现对虚拟化环境虚拟服务器的访问审计和运维安全管理。虚拟化环境结构示意图参见图1。

3.1 虚拟数据中心管理

VMware vCenter提供了功能较完善的图形化的管理界面，可同时支持物理主机和虚拟机的管理。仅部署一台vCenter Server就能够实现所有虚拟机的日常管理工作，包括各虚拟机控制管理、CPU内存管理、用户管理、存储管理、网络管理、日志收集、性能分析、故障诊断、权限管理、在线维护等。NSTL虚拟机CPU、内存、存储容量使用分析参见图2。

VMware vCenter还提供了富有弹性的资源池管理特性，每个资源池内的虚拟服务器可专属使用该资源池内的资源而不被资源池以外的虚拟服务器所影响。利用这一特性并结合NSTL自身业务系统的需求，我们创建了面向业务属性具有层次结构的共享资源池，使共享资源池内的虚拟服务器能够按照不同的策略和业务负载情况动态地获得计算资源。通过制定相关的资源分配策略，也使得在资源池内的虚拟服务器增加或减少CPU和Memory资源变得更加灵活。实践表明，部署虚拟化架构一定要合理地利用资源池特性，才能有效地提高计算资源的效率和使用率。NSTL资源池划分参加图3。

图3 NSTL资源池划分

3.2 虚拟化的计算资源

虚拟化环境主体初期采用了2台vSphereESXi的物理服务器作为动态的虚拟化架构基础。VMware vSphereESXi是一个强健的经过生产验证的裸机虚拟化管理程序，它直接安装在物理服务器上，统一管理物理服务器上可用的CPU、内存、网卡、存储等资源。每台物理机最大可支持64个虚拟机（理论值），这些虚拟机可共享物理机的处理器、内存、存储和网络资源，灵活地将资源调配给虚拟机，提高了硬件利用率。按照NSTL实际业务负载情况和应用部署需要，单台ESXi物理服务器的虚拟机服务器部署能力可达到16：1，可最大化地利用计算资源。

3.3 虚拟化的存储资源

存储是服务器不可或缺的重要组成部分，为了充分利用虚拟化软件的各项增强功能，NSTL在虚拟化环境中采用的是FC/IPSAN的集中存储融合方式：即需要高性能IO和稳定吞吐的业务优先通过FC SAN使用存储资源，而IO需求较少、存储量较大的业务使用IPSAN获得较多存储资源分配。为了满足在线业务系统的需要，充分利用VMware虚拟架构中虚拟机可动态在线迁移的特性，配置冗余的交换机组成共享的SAN存储架构，可以最大化地发挥虚拟架构的优势，实现动态的资源管理（VMware DRS），为以后的容灾提供扩展性打下基础。

初期建设可用存储空间共30TB，每个虚拟服务器的存储资源标配为500G，标准空间部署模式为Thin Provisioning精简置备。利用vCenter提供的可用存储空间统计功能，当虚拟机需要更多数据存储空间时，可以随时进行扩容，而当前的操作系统基本都支持在线存储容量扩容无须重启。

在虚拟化环境存储架构中，我们还基于NSTL业务应用的情况，充分考虑了以下因素：

（1）存储架构的访问路径冗余、IOPS与吞吐量的需求；

（2）每个ESXi服务器内虚拟机并发IO队列长度与HBA适配卡设置保持一致；

（3）根据应用需要设置LUN的RAID结构，对于随机读写的数据库如Oracle、SQL数据库，则在LUN级别采用RAID10结构；对于数据库日志通常为连续写或恢复时连续读，则在LUN级别采用RAID5结构。

（4）对于IO密集型的应用尽量采用单独的VMFS存储，避免在存储端与其他应用产生IO争用。

（5）多个虚拟机共用一个数据存储或者多个主机共享一个数据存储时，可以启用存储队列QoS，确保核心应用的延时在可控范围和对数据存储读写的优先级。

（6）对于ALUA磁盘阵列（非双活磁盘阵列），为了防止多路径读写冲突，在多路径策略选择时设置为MRU（最近使用策略），该策略可以保证只有在某个路径故障

时才启用另一个存储处理器连接LUN。

通过“服务器群－SAN网络－存储池”的存储架构为虚拟化应用平台提供存储资源，有效提高了存储利用率，简化了管理和维护的工作量，提升了虚拟化环境的扩展性和可靠性。

3.4 拟化的网络架构

虚拟化平台网络构建在NSTL千兆城域网内，基于已有业务考虑，将它划分成了管理网络、VMotion实时迁移网络、容错日志记录网络和业务应用四个独立网络，业务应用网络又包含了前台业务和后台业务。其网络架构具有以下特点：

（1）管理网络、前台业务应用网络和后台业务应用网络各自独立。

（2）前台与后台业务应用网络安全控制策略差异化。

（3）每个虚拟交换机配置两个上行链路物理网络端口，冗余策略遵循在不同PCI插槽的物理网卡之间配置。

（4）物理交换网络进行冗余设置，避免单点故障。

（5）对多个端口捆绑做负载均衡，满足大吞吐量和高并发网络带宽使用要求。

（6）虚拟交换机端口启用802.1q的VLAN标记，按业务需求创建专有VLAN。

通过上述网络架构设计方式，虚拟化环境能够灵活地为NSTL城域网用户提供虚拟化资源服务，既能满足NSTL前台业务，也能满足后台业务的应用部署需求，且在NSTL网络安全策略的保护范围之内。ESXi服务器网络示意图参见图4。

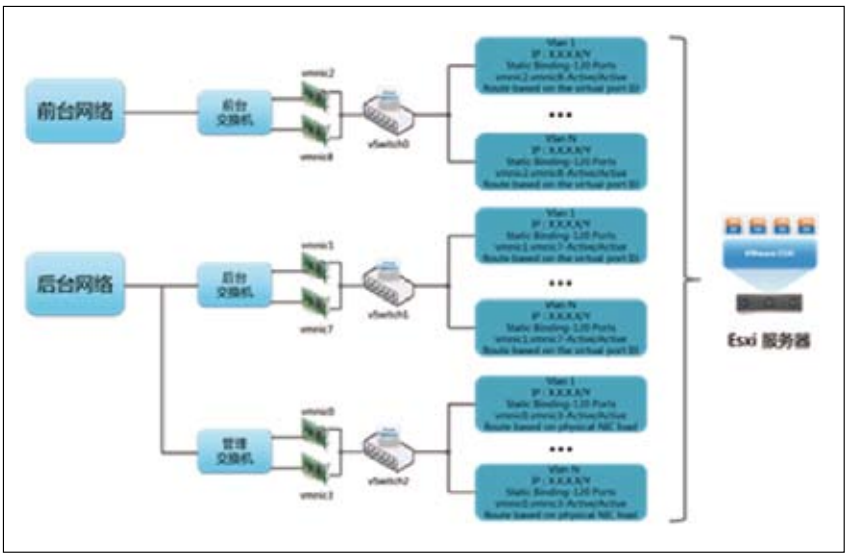

图4 ESXi服务器网络示意图

图5 安全审计系统

4 虚拟化环境中的运维安全

虚拟化环境中的运维管理比单台服务器的维护管理复杂度要大得多，涉及了系统、网络、应用、数据库、中间件等多种应用，涉及的运维人员也分散在不同的部门，其维护的操作也是多样化的，可以是Telnet、SSH、http、https、FTP、远程桌面、KVM终端维护等。对于X86系统每台虚拟服务器还需要考虑防病毒和系统补丁等问题。因而，做到对虚拟化服务器中各类设施的安全监控和对操作行为的审计，避免出现问题却无法追溯的情况发生，是实施虚拟化建设值得关注的问题。

4.1 运维审计

为了降低运维风险， NSTL在实际应用中采用了运维堡垒机对虚拟化中的各类主机、应用系统实行访问控制和运维操作审计。起着操作网关作用的运维堡垒机能

实现对人员、设备、操作行为等诸多要素的统筹管理和策略定义。因此，建立一个具有完备控制和审计功能的管理系统可为虚拟化业务提供安全保障。安全审计系统示意图见图5。

运维堡垒机采用“操作网关”的模式实现集中管理。这种部署模式的优点是在部署过程中无需在被管理设备上安装任何代理程序或插件，也不需要调整设备之间原有的网络架构，对用户当前的运维环境几乎不会造成任何影响。用户使用唯一的帐号登录到运维操作管理系统中，系统会根据预先设置好的访问控制规则，提示用户选择可以访问的目标设备和相应系统帐号，用户选择后自动登录到目标设备。运维堡垒机同时记录了用户的全部操作过程，可对操作过程进行回放。通过部署运维节点机达到了以下目的：

（1）实现单点登录

全部运维人员集中通过运维管理系统来管理后台的服务器、网络设备等资源，同时对运维人员进行统一的身份认证。

（2）实现统一授权

统一部署访问控制和权限控制等策略，保证操作者对后台资源的合法使用，同时实现对高危操作过程的事中监控和实时告警。

（3）快速定位问题

对操作人员原始的操作过程进行完整的记录，并提供灵活的查询搜索机制，从而在操作故障发生时，快速地定位故障的原因，还原操作的现场。

（4）简化密码管理

实现账号密码的集中管理，在简化密码管理的同时提高账号密码的安全性，满足等级保护安全要求。

4.2 病毒防护措施

计算机病毒对应用系统的危害极大，常见的传播途径一种是通过存储介质进行传播，另一种是通过网络恶意传播。对此，NSTL在部署虚拟化环境时也从多个维度采取了安全防护措施。

（1）首先基于业务配置了两个网络既前台网络与后台网络，将这两个网络的设备分别连接到不同的物理接入交换机上，依托NSTL城域网对于前后台网络的安全策略，实现基本的网络安全保障。再将前后台网络分别划分各自的VLAN，而对于运行在虚拟化环境中的虚拟机还可再进行逻辑上的划分，通过VLAN间的访问策略进行本地的安全控制。

（2）VMware Tools是一个驱动程序和实用程序的集合，每台虚拟服务器上都安装了Vmtools工具，利用Vmtools禁止两台虚拟机之间的文件共享，以及相互间的复制和粘贴等操作，在一定程度上可降低病毒传播的风险。

（3）预先配置好操作系统模板，安装专业杀毒软件并定期更新这些模板的补丁和病毒库，以降低系统风险，实现应用的快速部署。

（4）利用Esxi服务器的内置防火墙策略对虚拟化环境中的关键服务通信进行监控，控制入站和出站连接。

（5）利用运维网关的代理审计功能对虚拟机文件传输实现安全控制。

随着网络安全问题的日趋严重及新型安全风险的出现，需要持续关注虚拟化环境的网络安全问题，在规避传统网络安全问题的同时，还应对未来网络安全可能出现的风险未雨绸缪，以增强虚拟化环境的安全防护能力，保障虚拟化平台的稳定运行和应用安全。

5 服务器虚拟化技术在NSTL应用的思考

服务器虚拟化技术有各种优点，但是在实际应用中也存在着运维难度高、应用对虚拟化服务器的适应性、虚拟层升级带来的应用维护的复杂度等诸多问题。比如：

(1) 虚拟机的模板在制作过程中如果激活了操作系统，当从模板部署虚拟机后，新产生的系统仍然为激活状态，从而导致存在不符合软件正版化的风险。

(2) 随着时间的推移，需要不断更新虚拟硬件驱动、操作系统补丁和病毒库，从而导致所有虚拟机和模板需要运维人员和应用人员共同参与处理，增加复杂性。

(3) 某些商业化应用软件需要厂商根据硬件环境生成运行许可，由此会导致虚拟化的功能特性无法实现。

(4) 管理手段相对滞后，传统数据安全技术尚不能完全适应虚拟化环境，导致数据安全保护手段与虚拟机环境不匹配，可能影响到数据安全。

以上罗列了一些在实践中碰到的实际情况，有些是传统管理方面对虚拟化新技术带来变革的不适应，有些也确实是虚拟化技术产生的需要应对的新局面。因此，还需要在实践中不断地总结和完善。

6 结语

目前，NSTL 虽已实现基于虚拟化环境的在线业务系统的各种

应用服务，但仍有许多工作尚待完善。虚拟化环境有别于传统的物理服务器环境，维护人员对虚拟化环境中的虚拟设备和运维管理中的角色等存在认知差别，只有准确把握各个角色职责，逐步规范管理流程和制度，才能使虚拟化应用在使用和管理上更加高效便捷。同时，虚拟化平台的投入使用，也给以往的IT运维习惯带来了很大的挑战。NSTL必须积极应对这种挑战，通过技术手段、管理制度、人员培训等保障虚拟化平台持久、稳定运行，从而实现部署虚拟化平台的阶段性目标。

参考文献

[1]鲁松.计算机虚拟化技术及应用[M].北京:机械工业出版社,2008:32-48.
[2] NSTL数字业务服务平台备份体系系统设计方案，2011
[3]虚拟化是实现数据中心云计算的基础[EB/OL].[2013-03-02].http://www.jifang360.com/news/2010816/n73639209.html.

作者简介

张婧，高级工程师。研究方向：计算机网络安全等。E-mail:zhangj@istic.ac.cn
关越，系统管理员。研究方向：网络安全、虚拟化技术。E-mail:guany@istic.ac.cn
胡铁军，研究员。研究方向：计算机网络建设与管理、文献信息基础理论研究与建设。E-mail：hutj@nstl.gov.cn

The Application of Server Virtualization Technology in NSTL

Zhang Jing, Guan Yue / Institute of Scientific and Technical Information of China, Beijing, 100038
Hu Tiejun / National Science and Technology Library, Beijing, 100038

Abstract: With the rapid growth of networking and digital information.,In general, its data center has numerous servers and at least terabytes of storage. Accordingly, it will be the main objective of virtualization planning of IT systems, which is about how to use more effective techniques to support rapid development and efficient management of data center in the future. That is for establishing a platform that well adapts business information systems, and makes IT systems become real competitive tools for enhancing business level. This article describes the concrete practice of NSTL in using server virtualization technology.

Keywords: Virtualization, Data center, Cloud computing, Network

（收稿日期：2013-05-30）