微软认证辅导:服务器安全管理的四个注意事项Microsoft认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/590/2021_2022__E5_BE_AE_E8_BD_AF_E8_AE_A4_E8_c100_590093.htm 服务器虚拟化只需要较少的硬件资源就能运行多重应用程序和操作系统，能允许用户根据自身需求快速调配新的资源。但是这些灵活性也导致网络和安全管理者们不禁担心存在于虚拟环境中的安全隐患会在整个网络中蔓延开去。因为如果服务器管理程序发生问题，那么很快就会通过虚拟机在整个网络中蔓延出来。接下来，就让我们从以下四个方面看一看与服务器虚拟化的相关问题： 1.虚拟机溢出导致安全问题蔓延 管理程序设计过程中的安全隐患会传染同台物理主机上的虚拟机，这种现象被称作“ 虚拟机溢出 ”。 如果虚拟机能够从所在管理程序的独立环境中脱离出来，入侵者会有机可乘进入控制虚拟机的管理程序，进而避开专门针对保护虚拟机而设计的安全控制系统。 虚拟世界的安全问题正在试图脱离虚拟机的控制范围。尽管没有那家公司会允许安全问题通过管理程序技术的方式在虚拟主机间相互传播和蔓延，但这样的安全隐患还是存在的。因为入侵者或者安全漏洞会在虚拟机之间来回捣乱，这将成为开发者在开发过程中的必须面对的问题。 现在技术工程师通常采用隔离虚拟机的方式来保障虚拟环境的安全性。保障虚拟环境安全的传统方式是在数据库和应用程序层间设置防火墙。他们从网络上脱机保存虚拟化环境有助于缓解安全隐忧。这对于虚拟化环境来说是比较好的方法。 2.虚拟机成倍增长，补丁更新负担加重 虚拟机遇到的另外一个安全隐患是：虚拟机修补面临更大的挑战，因为随着虚拟机增长

速度加快，补丁修复问题也在成倍上升。 IT管理人们也认同补丁在虚拟化环境中的关键性，但是在虚拟机和物理服务器补丁之间实质的区别并非在于安全问题，而是量的问题。虚拟化服务器与物理服务器一样也需要补丁管理和日常维护。目前，世界上有公司采取三种虚拟化环境--两个在网络内部，一个在隔离区(DMZ)上--大约有150台虚拟机。但这样的布置就意味着管理程序额外增加了层来用于补丁管理。但即便如此，还是无法改变不管物理机还是虚拟机上补丁的关键问题。 另外当服务器成倍增长也给技术工程师及时增加补丁服务器的数量带来一定的压力，他们开始越来越关注实现这一进程的自动化的工具的诞生。 3.在隔离区(DMZ)运行虚拟机通常，许多IT管理人都不愿在隔离区(DMZ)上放置虚拟服务器。其它的IT管理者们也不会在隔离区(DMZ)的虚拟机上运行关键性应用程序，甚至是对那些被公司防火墙保护的服务器也敬而远之。不过如果用户正确采取安全保障措施，这样做也是可行的。用户你可以在隔离区(DMZ)内运行虚拟化，即使防火墙或隔离设备都是物理机上。在多数情况下，如果把资源分离出来是比较安全的方式。这个时候，不管是隔离区还是非隔离区，都可以建立虚拟化环境，他是采用在虚拟资源的集群中限制访问的办法。“ 每个集群都是自己的资源和入口，因此无法在集群之间来回串联 ”，他解释说。许多IT管理者们致力于将他们的虚拟服务器分隔开，将他们置于公司防火墙的保护之下，还有一些做法是将虚拟机放置在隔离区内-只在上面运行非关键性应用程序。 4.管理程序技术的新特性容易受到黑客的攻击 任何新的操作系统都是会有漏洞和瑕疵的。那这是否意味着黑客就有机可乘，发现虚拟操

作系统的缺陷进而发动攻击呢？ 工业观察家们建议安全维护人员要时刻对虚拟化操作系统保持警惕，他们存在潜在导致漏洞和安全隐患的可能性，安全维护人员只靠人工补丁修护是不够的。 虚拟化从本质上来说全新的操作系统，还有许多我们尚不了解的方面。它会在优先硬件和使用环境之间相互影响，让情况一团糟的情况成为可能。 虚拟化管理程序并非是人们自己所想象的那种安全隐患。根据对微软公司销售旺盛的补丁Windows操作系统的了解，象VMware这样的虚拟化厂商也在致力于开发管理程序技术时控制安全漏洞的可能性。 更多优质资料尽在百考试题论坛 百考试题在线题库 微软认证更多详细资料 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com