ESX 与 ESXi 安全管理

ESX 与 ESXi 安全管理

ESX是性能比较稳定的虚拟化产品，但是也存在一些安全漏洞。ESXi是VMware免费嵌入式hypervisor，它也存在安全缺陷。对于这两款产品，我们该如何安全地管理它们？本指南将从网络和管理方面入手，提供一些实用技巧。

网络安全

在各种融合网络环境下运行 VMware 容易导致数据混合，该如何合理地融合网络和安全区域？用户在隔离区内配置 VMware ESX 或者 VMware ESXi 宿主虚拟机的话，网络安全如何保证？如何让 VMware 虚拟架构里的混合模式端口组不受到威胁？

- 如何在 VMware 虚拟融合网络中防止安全漏洞？
- 如何防止在隔离区出现 VMware ESX 和 ESXi 网络安全漏洞？
- 如何最小化混合模式端口组安全漏洞？

安全管理

和 VMware ESX 相比，VMware ESXi 存在安全缺陷，该怎样解决？VMware ESX 内置管理工具，不过第三方应用提供了更好的性能管理能力。该怎样使用第三方应用监控 VMware ESX？那么对于 VMware ESX 3.5 存在的漏洞又应该如何修补呢？

- 如何安全地管理 VMware ESXi？
- 如何使用第三方应用监控 VMware ESX？
- 修补 VMware ESX 3.5 漏洞的工具

注意事项

在虚拟环境里，有三个常见问题会导致安全问题。为了更好地确保安全，我们定义了虚拟环境的范围，并且讨论在操作系统、应用和网络级别的一些安全威胁。我们还讨论了最普遍的十大问题，这些问题涵盖了不恰当的网络到过分信任 SSL 和 VLAN 技术等一系列方面。

- 确保虚拟环境安全的三个考虑事项
- 威胁安全性的十大虚拟化问题

如何在 VMware 虚拟融合网络中防止安全漏洞？

在各种融合网络环境下运行 VMware 容易导致数据混合，尽管从直观上看这种混合并没有坏处，但是如果有错误的数据混合进来的话，就会出现问题了。之所以出现融合网络是因为并不是很多人都完全利用 10Gb 以太网网络带宽，甚至很多人都没有充分利用 1Gb 的以太网连接。融合网络的目的就是让网络的其他方面充分利用未使用的带宽，这是由于缺少网卡（NIC，即 Network Interface Card），部署新的电缆不太可能，并且时间成本和资金成本也比较高。

最简单的解决方案就是在同一条光缆上不仅仅传输一类数据信息，这就是所谓的数据混合。只要所有的数据具有同样的安全等级和安全区域，在数据混合中就没有必要考虑安全问题。然而，如果同一条线路上传输的数据不属于相同的安全等级或者安全区域的话，数据融合就会成为一个比较令人头疼的问题。

安全等级定义不同主体可以访问同一传输线路上的不同数据，而安全区域指的是传输线路所连接的区域，也可能包括对其如何使用。例如，与称为生产的安全区域相比，一个 DMZ（隔离区）很有可能是一个敌对环境。两个区域的数据融合将会提高系统正常风险级别，正常风险级别是指在一个融合网络中没有数据混合的情况下的风险级别。

对每一台 VMware ESX 主机来讲，使用虚拟化的话，至少有四种可能的网络：服务控制台或者管理设备、存储网络、VMware VMotion 或 Storage VMtion 网络和虚拟机网络。另外至少有四个不同的安全区域：管理程序（Hypervisor）、虚拟机、存储和管理。

如何合理地融合网络和安全区域？

选择要融合网络和安全区域取决于很多方面，但是为了简化问题，我们这里忽略硬件限制。沿着当前的思路往下走：为什么各种各样的安全区域和网络需要保持隔离？这并不表示我不喜欢虚拟局域网（VLAN），但是 VLAN 确实不能保证安全性。VLAN 是一个网络中（物理的或者虚拟的）确保一个数据包传送到合适端点的工具，但并不是一种保护网络的方法。

最近在 VMware 社区，“Secured with VLANs”这个词谈论得非常热。RFC（Request for Comment）802.1q 中并没有提及到安全问题。VLAN 并不保证安全性，但是可以被安全地使用。然而，为了确保安全地使用融合网络，有一些问题还是需要注意的：

- 直接（vmkernel 虚拟网卡）或者间接地（管理设备与应用）通过网络连接对 Hypervisor 的任何访问都必须受到严格的控制。因为取得对 Hypervisor 的访问控制权限就会带来对 VMware ESX 主机或 VMware ESXi 主机内任何信息取得访问控制权限的风险。
- 对 VMotion 网络的任何访问也会带来风险：由于正在使用的内存信息以明文方式在线路上传输，虚拟机内的证书和身份数据很容易暴露。
- 通过一台虚拟机、备份服务器，或者是间接地通过 Hypervisor 和管理工具对存储网络的访问控制必须受到严格的控制。由于可以对存储网络信息以明文的方式访问，对虚拟存储网络的访问可能会带来暴露虚拟机内虚拟硬盘上内容的风险。

最好的实现方式

鉴于所有的上述信息，对于使用融合网络的虚拟网最好的建议是什么呢？理想的情况就是不融合 VMware ESX 主机和 VMware ESXi 主机内的任何网络，但是这个似乎有点不太现实。用户可以选择不融合从 VMware ESX 主机和 VMware ESXi 主机到物理网关的网络，但是如果这样的话，虚拟网就会形成集群来穿越整个公司交换结构中的其它物理网关。

交换结构中的薄弱环节实际上可能是物理网络，因为虚拟网关可以防止当前来自 VLAN 第二层攻击，尽管攻击不是来自第三层。不过也不是所有的物理网关都可以阻止来自第二层 VLAN 的攻击。

人们通常混合来自同一条线路上 VMware ESX 主机和 VMware ESXi 主机管理设备的数据和 VMotion 的数据，因为他们认为这两者应该是和其它任何网络一样具有同样的风险程度。VMotion 是具有最高风险的网络，然而如果有恶意用户可以攻破 VMware ESX 主机和 VMware ESXi 主机管理设备的话，就可以获得对所有磁盘数据的访问控制权限，然而未必是 VMotion 数据。但是如果这两者在通一条线路上传输的话，风险就比较高了。

其它经常混合的数据是存储数据和虚拟机数据。换句话说，虚拟机可以和 ESX 主机访问到同样的存储空间。如果虚拟机不是一个存储管理节点或者形式的管理节点，也可能导致虚拟环境中安全漏洞出现的高风险性。

当前没有减轻这个问题的好方法。VMware ESX 和 VMware ESXi 现在都不支持 IPsec（Internet Protocol Security）。IPsec 使用预置共享密钥和一个很好的公钥密码体系可以对融合网络上的所有数据完成强加密，加密过程基于不同数据来源使用不同的密钥体系。这个方法可以在很大程度上降低整体风险性。

选择融合何种网络需要对要传输的数据有一个很详尽的了解，如这些数据传送的目的地、传送方式、加密的可能性以及数据传输错误带来的风险等。

关于作者：Edward L. Haletky是企业级VMware ESX Server方面的作者：Planning and Securing Virtualization Servers。他最近离开了惠普公司，以前他在虚拟化、Linux和高性能计算部门里工作。Haletky自己拥有AstroArch Consulting公司，他还是VMware社区论坛的拥护者和版主。

（作者：Edward L. Haletky 译者：王越 来源：TechTarget 中国）

如何防止在隔离区出现 VMware ESX 和 ESXi 网络安全漏洞？

如果用户在隔离区（DMZ：Demilitarized Zone）内配置 VMware ESX 或者 VMware ESXi 宿主虚拟机的话，需要格外注意网络问题。VMware 网络包括 VMotion 和存储 VMotion 网络、虚拟机网络、存储网络以及管理控制台所必需的网络。如果网络问题不能很好地处理的话，这些网络就会绕过现有的保护措施，而这些保护措施通常情况下用来阻止隔离区与外部通信。

在隔离区内部署 VMware ESX 和 VMware ESXi 的一个关键问题就是要意识到这是一个混合网络和混合计算资源，而不是一个单一操作系统或者应用设备。相应的，同时也应该评估一下在隔离区内是否应该有一台虚拟机。

很多安全管理员不允许在隔离区内实现多宿主系统，多宿主系统就意味着一个系统同时可以和很多网络建立连接。多宿主系统中，令人担心的问题就是这些系统会不自觉地成为安全区域和外部预定义的防火墙、路由器和网关通信的桥梁，其中这些防火墙、路由器、网关是安全部门早期建立的。

使用 VMware ESX 或者 VMware ESXi 的话，情况就不会是这个样子。在 Hypervisor 内部的 Layer 2 虚拟网关使用起来同 Layer 2 物理网关一样简单。鉴于这些虚拟网关的存在并且这些虚拟网关不能相互通信（除非是和不同的物理网关），所以存在一些系统可以为此建立连接。VMware ESX 或者 VMware ESXi 不会作为这样一个桥梁，但是却可以维持虚拟网关作为其自身的一个实体。虚拟机被连接到虚拟网关的 portgroups 上，这个虚拟网关作为一个 VLAN，其实并不必需。虚拟网关之间不能直接通信，不同 portgroups 的虚拟机也不可以直接通信。除非是 ID 为 4095 的 VLAN portgroups 内的虚拟网关，这是因为 ID 为 4095 的 VLAN 是供安全软件和控制 VLAN 的虚拟机使用的。

对于每一个 VMware ESX 主机来讲有四个可能网络：服务控制台或者管理设备、存储网络、VMware VMotion 或者存储 VMotion 网络和虚拟机网络。前三个网络是关键性网络，不能部署在隔离区内。最后一个网络是唯一个可以部署在隔离区内的网络。

很多人都认为最好的实现方式就是不要把前三个网络部署在隔离区内，但是却没有合适的理由。以下是我的理由：但都是基于这样一个假设，在持续威胁和可能性攻击情况下，隔离区可以会成为一个恶意网络环境。它一旦被攻破，就会成为对保护的网络进一步攻击的枢纽。

服务控制台

服务控制台或者管理设备是虚拟网关上的 portgroups 的门户，并且部署在它们自身虚拟网关上的 portgroups 内。所有的管理性的工作都在这个网络上完成，所谓管理性的工作通常包括登录每一个系统的认证信息。这个网络一般通过 SSL 得到保护，访问这个网络可以给予攻击者从最基本的层次渗透到虚拟环境中的可能性，悄无声息地窃取数据的机会也会有很大增长（所谓的数据，我这里是指虚拟磁盘文件及其内容）。进一步来讲，这也就提供一个直接攻击 VMware ESX 主机和 VMware ESXi 主机上账户的机会，也就等于是给了攻击者访问所有信息的权限。

存储网络

存储网络是另外一个经常部署在其自身虚拟网关内部的重要网络。当前所有负责存储的协议在物理线路上都以不加密形式传送数据。攻击者获得访问这个网络的权限就可以访问虚拟磁盘数据。进一步来讲，如果使用的是 iSCSI，就会有另外一种攻击服务控制台或者管理设备的可能，这是因为服务控制台或者管理设备也参与 iSCSI 网络。

VMotion 和存储 VMotion 网络

VMware VMotion 和 Storage VMotion 网络通常情况下在其自身的虚拟网关上，一般以明文方式在物理线路上传送虚拟机的内容和磁盘信息。由于攻击者可以获得虚拟机内存和磁盘内容的信息，所以这个网络是不安全位置中最危险的一处。通过这些信息，攻击者可以得到访问认证信息的权限。通过收集到的认证信息，这个网络也就成了攻击用户网络的枢纽。

虚拟机网络

获得虚拟机网络访问控制权限不会带来获得其它三个网络访问控制权限同样的风险。

有必要进一步阅读 VMware 其它文档，因为我发现在一个隔离区内开始部署 VMware ESX 主机和 VMware ESXi 主机之前，阅读这些文档是相当重要的。列举部分如下：

- VMware whitepaper on virtual networking concepts
- VMware whitepaper on VMware ESX 802.1q VLAN solutions
- VMware whitepaper on iSCSI design and deployment
- VMware whitepaper on placing a VMware ESX host within a DMZ

（作者：Edward L. Haletky 译者：王越 来源：TechTarget 中国）

如何最小化混合模式端口组安全漏洞？

如何让VMware虚拟架构里的混合模式端口组不受到威胁？许多网络安全工具，如Blue Lane、Catbird和Reflex Systems都可用，不过它们需要激活。另外，一些检查网络数据包的新工具，如VMware vCenter AppSpeed，也需要激活混合模式设置。

这些程序也需要你设置端口组的 VLAN ID 为 4095。这个特殊的 VLAN ID 用于直接传递数据到虚拟机，而不需要通过 vSwitch 里 VLAN 进程的解释（通常用于执行虚拟子标记）。不过这个端口组也允许混合模式的虚拟机看见所有的数据包，这是由于它们不通过 VLAN 而穿过 vSwitch。如果端口组的 VLAN ID 不是设置成 4095，混合模式的以太网适配器只能看见某个端口组的数据，而不是整个 vSwitch。

不过你如何安全地执行？你如何激活混合模式端口组并且保持其他的都没影响？由于从一个端口组移动虚拟机到另一个的颗粒度保护不存在于目前的 VMware ESX 或 ESXi 版本里，所以这是个棘手的问题。有几种方法可以将虚拟机从一个端口组移动到另一个。

- 关闭虚拟机后手动编辑虚拟机 VMX 文件，或者直接在虚拟机文件系统上或使用远程命令行接口 VIF 工具得到原始文件，然后将修改后的文件放回系统。
- 使用 VMware Converter 或其他工具执行虚拟到虚拟（V2V）迁移。
- 使用 VMware Infrastructure Client（VI Client）连接到 VirtualCenter（现在叫做 vCenter Server）以作修改。
- 在 VI Client 里连接到主机虚拟机以作修改。

有如此多的方法将虚拟机移动到混合模式端口组，一些角色和权限设置的安全性降低了。

信任

安全，尤其是没有阻止同事管理员做一些无意识（或有意）的破坏性事件的安全设置，需要信任其他管理员。除了信任其他系统管理员，你需要经常审计你的架构以获取可能的安全威胁。不幸的是，在虚拟架构里没有设置用来监控这些问题的告警，所以你需要依赖手动监控或第三方工具。

防火墙

由于每个行为都需要管理员权限，宿主 vCenter、管理工作站和 VMware ESX Management 设备（服务器控制台和 VMware ESXi 管理设备）的虚拟化管理网络应该位于自身防火墙的后面。这样的话，你能控制哪个工作站能够访问基础设施管理工具，哪个不能，也包括如何访问这些工具。理想中，你想让管理员使用 VPN 访问他们的内部——虚拟化管理——网络虚拟机。这就是说一般情况下，工作站不是每天都在网络里。换句话说，保护虚拟化管理网络类似保护数据中心，要尽可能多的控制。这种类型的设置也可能有助于远程到虚拟化主机的访问。

远程控制台

由于也可以通过控制台发生一些变更，所以保护对远程控制台的访问也很重要。远程控制台应该是网络里另外一个需要隔离的部分。

VMware Converter

VMware Converter 是能轻易饶过安全防护的工具之一，所以唯一的方法是通过增加审计减少风险。

角色与权限

最后一个需要实施的控制是限制对能宿主虚拟机的网络的修改。对非管理员设置以下权限控制这些功能：

- 主机、配置及网络配置
- 主机、配置及变更设置
- 虚拟机、相互影响及设备连接
- 虚拟机、配置及添加或移除设备
- 虚拟机、配置及修改设备设置
- 虚拟机、配置及高级设置

总结

不幸的是，这些更改都不能最终防止恶意虚拟机对混合模式端口组的攻击，但是可以减少这种可能。不过，没有什么方法能够取代定期地对基础设施作出更改。有几家公司的产品可以做到：Tripwire 和 Configuresoft。其他公司的产品通过在虚拟机周围放置 Catbird 与 Reflex Security，防止有疑问的虚拟机输入输出信息。

（作者：Edward Haletky 译者：唐琼瑶 来源：TechTarget 中国）

如何安全地管理 VMware ESXi？

使用 VMware ESXi 也有不方便的情况，比如在没有 VMware 技术支持人员帮助的情况下，你就不能使用 Dropbear SSH 客户端或者其它技术支持模式。可是，系统管理员为了解决问题或者管理空闲网络连接，可能会倾向于使用技术支持模式（或者激活的 Dropbear）。但是打破这一层安全防护可能会导致 VMware ESXi 的证书的失效和技术支持合同的破坏。TechTarget 中国的特约作者 Edward L. Haletky 在本文中将介绍另外一种管理 ESXi 虚拟机的方法。这个方法不会影响到虚拟机的安全，但是可能会破坏技术支持合同。

我曾经写文章明确提出，和 VMware ESX 相比，VMware ESXi 存在的安全缺陷，写那篇评论文章主要是由于一些 ESXi 用户立即使用了 Dropbear SSH 客户端。如果这样做的话，就等于是打破了这个防护层。这样做将会导致 VMware 证书无效，进而导致技术支持合同失效，所以一般不推荐使用。

VMware 进一步声称只有在 VMware 技术支持人员的严格指导下，用户才可以使用技术支持模式。然而，系统管理员经常需要或者希望使用技术支持模式解决他们的特定问题，所以说这个界限如何设置是一个问题。那么是不是在没有 VMware 技术支持人员的帮助下，一旦触及到这个界限就会导致证书的失效？如果在用户的 VMware ESXi 主机上有 ILO（Intergrated Lights Out）或者是 DRACs（Dell Remote Assitant Cards）的话，这个问题又如何处理？在对这些问题提出一些解决方案之前，我们可以先看一下 VMware ESXi 内置的安全属性。

VMware ESXi 确实考虑到了安全问题

ESXi 的安全防护层是这样的：除非用户可以使用 SSH 或者通过技术支持模式登录到系统，否则当前是没有其它的方法进入系统内部的。VMware ESXi 安全方面另外一个新颖之处是引导过程的特性：在引导过程中，ESXi 首先创建一个 RAM 磁盘，然后在这个磁盘上运行一个操作系统。数据存储设备挂载在个 RAM 磁盘上，虚拟机从这个磁盘加载系统运行。这样做的话就可以保证对操作系统的任何改动在重启之后将不会被保存，除非这些改动是在永久性存储设备上的。但是，众所周知，有一些改动在系统重启后还是会保存下来的。通过 VMware Infrastructure Client（VI Client）、远程命令行接口

（Remote CLI：Remote Command Line Interface）、控制台、或者 CLI 的 vicfg 命令，可以完成可接受的改动。其它任何形式的改动，如添加一个新的守护进程、新增一个文件夹等，在重启后都不被保存。

管理 VMware ESXi

VMware 在通过一个新型的控制台来创建一个 VMware ESXi 方面没有做太多的工作，其中用户可以通过这个控制台做诸多与安全相关的配置工作。另外，也有一些对 VI Client 做出的修改，通过这些修改可以允许配置部分操作，这些操作主要涉及用来规定手动修改的，如网络时间协议（NTP：Network Time Protocol）。最后，VMware ESXi 使用 vicfg 命令作为 Remote CLI 的一部分。各种方法的组合导致用户对于正常的配置工作根本不需要 CLI。现在用户可以远程控制 VMware ESXi 了。

保护 ESXi

针对如何保护 VMware ESXi，我只做简单介绍。在 VMware ESXi 内需要有一个审计迹、深度防御以及对一个目录的访问控制权限，这些都是我们在保护 VMware ESX 中经常使用到的方法。那么如何保护 VMware ESXi 呢？在回答这个问题之前，需要先分析一下 VMware ESXi 基础架构内部的网络部署和外部的为虚拟机创建的配套服务。主要有四个网络架构：

- 把管理工具相互连接起来的管理网
- 为 ILO、DRAC 等提供服务的控制网
- VMotion 网
- 存储网

保护VMware ESXi意味着保护这些网络和对ESXi配置所作的修改，主要依据VMware v. 3.5 Hardening Guidelines对ESXi的推荐配置。如：

- 完全关闭VMware ESXi的防护层
- 允许远程登录
- 对每一个虚拟机配置隔离的工具箱，防止通过后门程序使用、剪切和粘贴以及其他必要的操作

除了上述提到的和准则中讲到其他事项，还需要认识到对于这四个网络的任何访问都可能破坏到 VMware ESXi 的运行环境，因此还需要注意以下几点：

- 控制网和管理网之间需要很好的隔离，并且只有登录网络这些后才可以访问
- 管理主机需要在管理网上并需要得到很好的保护
- 管理网和其它的环境之间需要很好地隔离
- 如果使用虚拟中心，则这个虚拟中心需要放置在管理网上
- 对管理网络的访问需要受到严格控制
- 考虑在 ESXi 管理设备和管理网之间配置防火墙

这些要求在某种程度上看起来是比较严格的准则，但是要知道 VMware ESXi 自身并没有防火墙。因此用户需要增强监控和连接管理的能力，这也正是防火墙所做的工作。

在管理的过程中，尽量简化流程和相关事务。最好是尽可能使用虚拟中心，除非有些业务不能使用。这样做可以集中授权和认证能力，这也正是 ESXi 做不到的。如果没有使用虚拟中心的话，就需要为每一个相关用户配置合适的角色以及相应的权限；也需要为每一个 ESXi 增加一个用户，但是如果同时拥有多个 VMware ESXi 主机的话，这就可能成为管理中一个比较麻烦的问题。

（作者：Edward L. Haletky 译者：王越 来源：TechTarget 中国）

如何使用第三方应用监控 VMware ESX?

当监控虚拟基础架构性能时，专门的虚拟化报道工具是确保测量结果准确的关键因素。除 VMware ESX VI3 的内置工具之外，许多第三方应用甚至提供了更好的性能管理能力。

传统的操作系统性能报道工具使用在虚拟机上时通常不准确，这是因为它们没有注意到虚拟化层和下面的物理硬件。VI3 的标准性能管理工具包允许基础的虚拟机事件和性能监控；不过，它们的功能有限，不如一些免费的和商业的工具好用。

ESX 本身具备非常有限的历史性能监控。它只能监视实时统计信息以及先前 60 分钟的信息。VirtualCenter 扩展了时限，允许用户以更长的时间保留这些信息。在 VirtualCenter 里，你能配置每天、每周、每月以及每年模式，也可以配置保留性能数据的时限。

另外，VirtualCenter 也提供了对某些事件的告警。这些事件包括 CPU、内存、磁盘和网络使用率过高或过低，还有主机或虚拟机的状态。这些告警不包括诸如主机和虚拟机上的磁盘空间低或某些事件发生在 ESX 主机服务器上。

Esxtop 服务器控制台也能提供性能监控（不过是实时的本文格式），显示关于 CPU、内存、磁盘和网络性能的详细信息。Esxtop 输出的信息能直接指向 CSV 文件，因此稍后能输入 Windows Performance Monitor，在这就能以图象的形式显示和分析这些信息。

除了监控主机和虚拟机的事件、日志和性能，也能监控可能发生故障的主机硬件。有缺陷的内存是在主机服务器里发现的一个常见问题，这是由于虚拟机主机使可用内存最大化，不像物理服务器那样未完全使用内存。

多数主要的硬件厂商有专门设计用于安装在 ESX Service Console 上的代理，提供对主机服务器的硬件监控。ESXi 将这些代理内置，由于没有可用的 Service Console，ESXi 利用内置在 VMKernel 里的 CIM（公用信息模式）的中间装置。

除了用于监控 ESX 主机和虚拟机的内置工具，也有大量免费的商业的应用提供更强劲的报告、分析和监控。

下面复习一些可用的应用：

Nagios 不专用于 ESX，它是一个免费的、开源的服务与网络监控应用，能安装并配置在 Linux 服务器上。它也可以作为一个预配置的虚拟应用安装在 ESX 主机上。

Nagios 能配置成监控许多设备的应用，包括 Windows 服务器、Linux 服务器和 Unix 服务器、网络打印机、路由器或交换机以及像 HTTP、SSH、FTP 这样的服务等。Nagios 也能配置成从其他应用，如 VirtualCenter 和硬件代理接受 SNMP。虽然没有其他一些企业监控系统功能强大，Nagios 也是个不错的选择，因为它功能可以，价格较便宜。

Vizioncore 的 vCharter Pro 是一个功能强大的报告和监控应用，专门用于监控和分析 ESX 主机。

Vizioncore 的产品集成 VirtualCenter，提供增强型的报告功能、可配置的仪表盘、智能的规则和警告以及自定义报告以识别趋势与瓶颈。它内置的智能统计功能有助于更好地了解 ESX 主机在做什么。

eG VM Monitor 是另一款功能强大的专门用于 ESX 主机的报告和监控应用。eG VM Monitor 在专用于 VMware 环境的一个基于 web 的应用，它也属于 eG Enterprise Suite 的一部分。它包括对基于代理和无代理（主要是 ESXi）服务器监视的支持，并且只需要安装在 ESX 主机上，不用安装在每台虚拟机上。

eG 提供了丰富的功能，并且使用 In-N-Out 监视方法以提供虚拟机性能的外观图。它有广泛的报告功能，能跨宿主在 VMware 环境的应用分析性能，帮助发现虚拟机的从属关系，也有助于识别性能瓶颈。

Veeam Management Suite 包括报告、监控和配置产品，这些产品可单独购买。

Veeam Reporter 自动地发现并收集 VI3 环境上的信息，并提供分析报告，还有文档形式的环境。

Veeam Monitor 整合 VirtualCenter，提供增强型的环境健康与性能的监控与警告，也能不使用 VirtualCenter 监视单个的 ESX 主机。

Veeam 套件的第三个应用 Configurator 有助于更容易地配置 ESX 主机，提供 GUI 更改 ESX 命令行的更改设置。

VMware 的 Hyperic HQ 是 Hyperic HQ 套件的一部分，能监控大量产品。它允许从外向内分析性能阐述，站在一个较好的视角分析物理主机与虚拟机是如何执行的。它提供历史制图、时间相关功能以及可配置图象以分析性能数据。

用于 VMware Monitoring 的 NimBUS 是用于 Server Monitoring 的 NimBUS 产品的一部分，它提供对 ESX 主机、虚拟机以及 VirtualCenter 服务器的全面监控。它监控所有 ESX 和虚拟机性能参数、虚拟机操作系统，还有运行在虚拟机上的应用的响应次数。它也能监控 VirtualCenter 服务器和应用以及数据库的性能和状态。

nWorks 附加到 Systems Center 上的 Microsoft Systems Center Operations Manager 提供了详细监控和管理 VMware VI3 环境的功能。这款产品整合了 VMware APIs，集成到 VirtualCenter，通过一个特殊的基础架构集成组件收集信息。nWorks 附加物提供了访问所有 ESX 主机和虚拟机的详细信息。这样的整合允许 Microsoft Systems Center 监视和报道 ESX 主机服务器的性能、事件和警告。此外，即将发布的 Virtual Machine Manager 2008 产品将提供更好的整合能力以管理和监视 ESX 主机服务器。

Tivoli Monitoring for Virtual Servers 是 IBM Tivoli Monitoring 产品系列的扩展，它能监视 VMware ESX 主机。它既能监视资源性能和服务器可用性，还可以在物理和虚拟化层扩展传统的 Tivoli 监控功能。使用它能创建资源基准服务器级别，以帮助在识别问题和瓶颈的时候测量性能。

上面所列出的产品都超越了 VMware 提供的内置工具的基础监控。寻找第三方提供的监控工具很容易，它们能简单、有效地识别潜在的问题和性能瓶颈。

（作者：Eric Siebert 译者：唐琼瑶 来源：TechTarget 中国）

修补 VMware ESX 3.5 漏洞的工具

随着 VMware ESX Server 3.5 的发布，VMware 现在为每个虚拟化管理员提供了大量企业级的功能。这些功能不仅使 ESX 3.5 更漂亮，如我能命名具体某个新发布的主要操作系统。所有 ESX 3.5 的增强功能都是管理员真正需要的。

不过，ESX 3.5 仍然缺少许多功能。在本文中，TechTarget 中国的特约虚拟化专家 David Davis 将描述这些缺失的功能，并说明虚拟化管理员在需要的时候如何找到它们。

ESX Server 3.5 新在哪里？

我们来讨论一下 ESX Server 3.5 的新功能。我不会描述 ESX Server 3.5 的所有新功能。（详细信息你可以参见网站上的内容，例如我之前的文章“what's new in VMware ESX Server 3.5。）ESX 3.5 主要功能有：

扩展的 SATA 存储：你可能挣扎于为低端或测试系统使用 SCSI 或 FC 存储要求。在 ESX 3.5 之前的版本，你可能有一个 iSCSI 阵列或使用开源 iSCSI。有了 ESX Server 3.5，它能支持 SATA 磁盘。

VMware Storage VMotion：这个新功能允许虚拟机为其重新配置存储，而不需要关闭虚拟机。有了 VMotion，只要虚拟机位于 SAN 存储就可以迁移虚拟机，并且虚拟机的存储位置不变。使用 Storage VMotion，子虚拟机及其存储都能同时移动。过去，你可能关闭虚拟机或者使用像 VMware Converter 或其他产品才能进行热迁移。

VMware Update Manager：这个功能不仅允许你更新 VMware ESX Server，也允许更新任何 Windows 子操作系统。后者确实是有吸引力的功能。在过去，你必须使用 esx-update 来更新 Windows Servers。

VMware Guided Consolidation：有了向导整合，整合物理服务器到虚拟服务器更容易。之前，需要使用像 Platespin 的 PowerConvert 这样的工具进行整合。

VMware Site Recovery Manager：这是 VMware Infrastructure 套件有吸引力的功能。有了 Site Recovery Manager，你可以自动化灾难恢复过程，并且由于存储系

统的帮助，为多个数据中心提供高可用性。缺少的是将虚拟机带入 DR 站点的方法。这在广域网上不会发生，不像使用 VMotion 在你的 LAN 上那样。你必须使用存储厂商所提供的数据复制功能。在这之前，可能你只是手动地创建 DR 计划和 ESX Server 恢复过程。

我相信随着 VMware 加强 ESX Server，他们会增加更多功能以尝试消除对第三方软件的需求。这类似于微软过去对 Windows 所作的努力。

ESX Server 3.5 缺失的东西及如何修补

ESX Server 3.5 与 VMware Infrastructure 套件里仍然有一些主要的弱点，可能需要虚拟化企业使用第三方的虚拟化产品。在我看来。主要有以下几个弱点：

强劲的性能监控与管理：你能通过在 VMware Infrastructure 管理客户端里的图象获取。你将发现这没有提供你企业所需的容量规划和历史信息。所以，许多管理员使用 Vizioncore 的 vCharter，还有像 chargeback 工具 VKernel 获取这些信息。

跨广域网的虚拟子操作系统 VMDK 复制：在你使用来自存储厂商提供的数据复制工具时，这些工具一般都非常昂贵。对于这么昂贵的解决方案跨广域网复制虚拟机，我使用 Vizioncore 的 vReplicator，还有不是专为虚拟化设计的工具，如 Double-Take。

Virtual Desktop Infrastructure（VDI）：VDI 是一个复杂的话题。使用 VDI 的话，有个代理直接指在网络上的瘦客户端到 ESX Servers 上的虚拟 PC。这种所需的虚拟桌面整合代理不包含在 VMware Infrastructure 套件里。直到最近，VMware 的 VDI 产品才提供这个功能。不过我所知道的 VMware 和其他第三方的 VDI 产品目前都非常昂贵。希望能及时有开源的或更具成本效率的 VDI 中介出现。

增强的虚拟化备份：VMware Infrastructure 套件里不包含 VMware Consolidated Backup（VCB）。如果你尝试使用这个应用，很快你就希望有其他一些东西。虚拟化管理员确实需要的是图形化和增强型的备份应用，只适用于虚拟化环境，能支持各种不同的 VMFK 子操作系统。我所知道的两个最好的第三方应用是 Vizioncore 的 vRanger Pro 和 PHD Technologies 的 EsXpress。

总结

总之，VMware ESX Server 3.5 和 VMware Infrastructure 套件是 VMware 虚拟化的一大进步。在我看来，这是最成熟强劲的虚拟化产品。不过现在在企业环境里，如果就像 Windows Server，仍然需要第三方工具提供虚拟化管理员所需要的所有功能。

（作者：David Davis 译者：唐琼瑶 来源：TechTarget 中国）

确保虚拟环境安全的三个考虑事项

在虚拟环境里，有三个常见问题会导致安全问题：关于明确虚拟环境的组成问题，并且因此会给此环境带来什么样的威胁；虚拟机里应用与操作系统的管理；如何使用虚拟管理网络来管理虚拟主机。为了更好地确保安全，本文定义了虚拟环境的范围，并且讨论在操作系统、应用和网络级别的一些安全威胁。最终目的是帮助虚拟化管理员确保整个虚拟环境的安全。

什么是虚拟环境？

虚拟化安全方面的统一定义至关重要。如果你对安全虚拟环境的理解与流行的标准定义不同，会产生混淆和矛盾的安全措施。需要定义有关虚拟化的两个主要问题。首先第一个问题是虚拟环境包括什么？第二个问题是什么对这个环境有威胁？

虚拟环境并不只是虚拟主机。它是与虚拟主机有直接关系或间接关系的所有事物的结合。虚拟环境的组件包括（但并不局限于）管理工具、备份工具、存储以及虚拟与物理网络。这就是当人们谈到虚拟化安全时，我所定义的虚拟环境。

从虚拟化主机的角度来看，危险的环境包括所有虚拟机。这是因为对虚拟环境有最大威胁的是饶过虚拟机的方法，因此可以使用一些方式访问到 hypervisor。幸运的是还没有这样的一种方法。

另一个问题是饶过虚拟机到达 hypervisor 的管理设备。如果虚拟机能通过管理设备到达网络，这就能通过网络做到。尽管多数人很迷惑，但访问管理设备并不通常意味着你能访问 hypervisor。例如，VMware ESXi 在 hypervisor 里运行其管理设备，但是 VMware ESX 上的管理设备是作为一个独立的入口而运行。虚拟机如果没有通过安全组织的查证，不应该宿主在下面这些与 VMware ESX 主机相连的虚拟网络上：

- 存储网络
- VMotion/SVMotion 网络
- VMware Consolidate Backup 网络
- 管理网络

本质上，虚拟机不应该看见或使用与虚拟化主机和 vmkernel 相同的资源。vmkernel 资源包括存储和 VMotion 网络。主机所使用的另一个资源出于管理和备份的目的。访问这些网络应该考虑到各种对环境的攻击。因此，虚拟机对虚拟环境也有威胁。

记住了这些定义，我们现在来看看其他两个与安全有关的问题。

管理子操作系统

子操作系统的管理不需要访问虚拟机管理工具；也就是说要访问远程控制台。通常需要访问控制台，不过能通过使用像 Remote Desktop Protocol（RDP）、Virtual Network Computing（VNC），或者 Secure Shell（SSH）这样的工具来达到目的。访问管理虚拟环境的工具，如 VMware Virtual Infrastructure Client，应该只有虚拟化管理员才有权限。

如果人们想要使用 CD-ROM 安装软件，这通常会引起问题。比如在运行 Microsoft Windows 的虚拟机里，使用 VCD 这样的工具启动 ISO 镜像。

限制访问虚拟架构客户端的主要原因是在目前，客户端里的角色和权限保护颗粒度不足于有效限制行为。只因为子操作系统管理员能使用它，但这并不意味着它应该使用。这也包括 VI Web Access，访问 VMware Infrastructure Software Developer's Kit（VI SDK），以及任何其他访问虚拟化主机管理设备的监控工具。

确保虚拟化管理网络的安全

使用虚拟化管理网络非常棘手，因为对任何管理工具的访问将导致深层访问，无论是否通过使用虚拟架构客户端、VI SDK，还是其他工具。使用虚拟管理网络的另一方面是在网络里放置合适的系统。

每个虚拟化管理网络应该包括 VMware ESX 或 VMware ESXi 主机服务器控制台或管理设备，VMware vCenter 服务器和 VMware Infrastructure Management Appliance，或者你所使用的系统，不管是物理的还是虚拟的，都用于管理虚拟环境。

尽管 SSL（安全套接层）用在所有通信中，但是这个网络也应该使用防火墙与环境中的其他网络隔离，实施 SSL 中间人攻击很容易，即使在你更换正在使用的许可证之后也

会发生攻击。在一些情况下，我会使用虚拟专有网络访问虚拟化管理网络。这个网络本身应该看作是进入数据中心的入口。

对虚拟环境的不恰当定义能导致忽略关键安全问题。不明确子操作系统和虚拟化管理网络所关注的问题可能导致环境的不安全。虚拟环境安全从你怎么看待整个环境起步，而不仅仅是 hypervisor 或者管理设备。

（作者：Edward L. Haletky 译者：唐琼瑶 来源：TechTarget 中国）

威胁安全性的十大虚拟化问题

我在编撰下一本书的过程中，对虚拟化安全性做了调查，发现很多系统管理员都在某些共同方面无意识地破坏了他们的计算架构的安全性，导致了可能受攻击的漏洞。这些问题涵盖了不恰当的网络到过分信任 SSL 和 VLAN 技术等一系列方面。这里，我将列举我发现的最普遍的十大问题。

1.虚拟化管理员不是安全性管理员

虚拟化管理员既不是安全性管理员，也不时常听取安全性管理员的意见或和他们协商。要解决这个问题，可以给安全性管理员培训一些虚拟化的知识，同时也给虚拟化管理员一些安全性方面的培训。

2.虚拟服务器的管理设备处于保护不当或未受保护的网络中

我曾经在英特网、生产和 DMZ 网络上发现过服务控制台。服务控制台和所有的管理工具是应该放在自己的管理网络中的，而不能到处随便放。

3.绝对信任SSL

SSL 并不是绝对安全的，有一种针对 SSL 的攻击可以在两秒钟之内轻松攻破 SSL。不要以为 SSL 足够安全。除非使用了预共享证书，否则它就会有风险。如果你一定要使用基于 SSL 的管理工具，就在管理网络中使用这些工具，在管理网络中你可以信任网络中的用户。另外，从外部网络接入管理网络时，使用好一点的 VPN。

4.误以为虚拟机是安全的环境

隔离区（DMZ）的虚拟机或其它面向 Internet 的虚拟机不是一个安全的环境，但是对于虚拟化来说所有虚拟机都是危险的。对一个虚拟机的攻击永远不应该直接或间接指向虚拟主机。

5.NFS和iSCSI存储网络没有与其它网络分开

NFS、iSCSI 和 SAN 存储都是采用明码传输数据，这就意味着磁盘数据可能被其它用户读取。如果一个虚拟机从用于存储虚拟磁盘的存储网络载入了一个 iSCSI 对象，那么这就有可能成为一个攻击点。

6.VirtualCenter放在管理网络之外

尽管 VMware ESX 有防火墙保护，但 VirtualCenter 是在防火墙之外的，它应该和虚拟主机一样受到保护。利用 VI Client、Remote CLI 或 SDK 对 VirtualCenter 或主机的访问都应该只能来自管理网络内部。

7.存在额外的服务控制台端口

连接 NFS 服务器与 ESX 时，会创建一个服务控制台端口。这是一个错误，iSCSI 需要的是服务控制台的参与，而不是 ESX。服务控制台应该通过路由器、网关访问存储网络，最好是通过防火墙。因为，没增加一个服务卡控制台端口，当前的攻击向量（attack vectors）就会增加一倍。

8.服务控制台放在DMZ或不安全环境

这是大家的一个通病，服务控制台绝对不应该放在不安全的环境中。这包括 Internet 或 DMZ。

9.误以为VLAN会保护网络

尽管使用 vSwitch 可以防止由虚拟机发出的 VLAN 攻击和对虚拟机的攻击，但使用虚拟化不会阻止来自虚拟主机之外的 VLAN 攻击。你需要非常好的交换硬件来阻止大多数有名的 VLAN 攻击。VLAN RFC 并不意味着 VLAN 是可以保障安全性。而且，使用 VLAN 还会导致线缆中的数据混杂（data co-mingling）。

10.不了解hypervisor中的安全性

如果你不了解 hypervisor 的安全性，你将很难清楚如何保护好你的虚拟化环境。

这十大问题决不是仅有的安全性问题，只是最具代表性的问题。不久前，我向 VMware 公司讨教了 28 个安全性问题，请他们做出评论和回答，只有两个问题我没有得

到答案。所以，我建议大家向值得信赖的人或机构询问自己所有不清楚的安全性问题，以便为自己的环境建立最好的安全性。总之，安全性决不应该是一个可有可无的附带考虑，而是至始至终都应该慎重对待的一部分。

关于作者：Edward L. Haletky是企业级VMware ESX Server方面的作者：Planning and Securing Virtualization Servers。他最近离开了惠普公司，以前他在虚拟化、Linux和高性能计算部门里工作。Haletky自己拥有AstroArch Consulting公司，他还是VMware社区论坛的拥护者和版主。

（作者：Edward L. Haletky 译者：涂凡才 来源：TechTarget 中国）