第六章

虚拟架构是如何影响安全的？

保护虚拟架构并不需要像保护物理网络那样复杂，关键在于保持警惕性。

★安全问题：清楚风险所在

★案例学习

★实现虚拟化安全的新方法

★实现虚拟池的安全

★预防过度管理

虚拟架构是如何影响安全的?

数据中心的安全问题非常普遍又是一直存在的，偶尔引入的新元素往往需要管理员重新审视系统的安全策略。虚拟基础架构仅仅通过变换现代数据中心的结构来做到这些。服务器虚拟化可以提供功能强大的操作模式以及其它很多优势。在运行虚拟基础架构时，物理服务器就变成可以归入到一个资源池中的计算资源。另外，服务器提供主体——终端用户交互方——就变成了虚拟机。资源池和虚拟服务提供

主体之间的竞争改变了管理员看待数据中心安全的传统方式。

安全问题：清楚风险

数据中心除了这个转换之外，虚拟基础架构也带来其自身的安全问题。新安全威胁的出现自然就需要新方法来处理。但是虚拟化将会给当前的安全实践带来什么样的影响呢？网络安全中心——一个负责起草操作系统、网络设备和其它应用设备标准的非盈利组织——的专家曾经试图通过出撰写虚拟机安全标准报告来回答这个问题，该报告标识出若干种潜在的虚拟化技术安全威胁。但是随着越来越多的单位开始部署虚拟化基础架构，各种各样的新安全威胁也不断出现。

如果关注虚拟基础架构中的安全问题，就需要在保护该架构时考虑如下几个方面。在很多情况下，每个问题就依赖于已有的工具和实施，但是这两者都必须及时更新才可以满足消除虚拟基础架构安全威胁的条件。

- 单位部署服务器虚拟化的一个主要原因就是实施物理机器的整合——把物理计算机转换成虚拟机。在整合机器设备时，在把具有不同安全背景的系统配置在同一台宿主主机上时需要格外仔细。在把承载不同操作系统的虚拟机放在同一台主机上时也需要特别注意。

  - 具有不同安全背景的机器如果配置不正确的话就会损坏系统的

安全。确保连接到每一台给定安全背景的虚拟机上的虚拟网络适配器都绑定在主机服务器上的物理网络适配器。绝对不能把具有不同安全背景的机器连接到同一个物理适配器上，因为这可能引发安全数据通信泄露到不安全的网络上。

- 承载不同操作系统的机器可能迟滞不同级别的补丁包和更新——有些机器可能没有得到特定脆弱性的保护，而其它机器有得到保护。这些容易受到安全威胁的机器就会影响到其它机器的安全。

拥有不同操作系统的机器可能支持不同级别的补丁，所以其他机器受到保护时，一台机器可能遭遇漏洞威胁。

- 在主机上运行的虚拟机，可能在虚拟机和主机之间共享剪切板。该共享剪切板不仅支持数据转化，同时也能够使恶意程序“顺便捎带”剪切板上的数据，从而影响到其它虚拟机或者主机本身。尤其在使用软件虚拟化管理程序（该应用程序采取和操作系统上应用程序相似的方式运行）时更容易出现这类问题。部分软件虚拟化管理程序是 VMware Workstation、Sun xVM VirtualBox、Microsoft Virtual Server 以及 Microsoft Virtual PC。

运行硬件虚拟化管理程序——直接运行在硬件之上——能够缓解这个问题。硬件虚拟化管理程序包括 Microsoft Hyper-V、VMware vSphere、Virtual Iron 或者 Citrix XenServer。

- 有些主机记录运行在主机上虚拟机的登录按键和屏幕操作。用户可以通过虚拟基础架构管理界面控制这个称为主机虚拟机登录的行为。如果选择记录虚拟机活动，就需要确保主机日志文件一直都是完全安全的。

- 虚拟机内的程序可能会从虚拟机“逃离”，从而影响到主机安全。因此必须保证虚拟机配置合适的防火墙和恶意软件防护程序，诸如防病毒和反恶意软件程序。还需要保证的是所有的签名和补丁能够及时更新。

- 监控可能会成为一个问题。主机可以监控虚拟机，虚拟机也可以监控其它虚拟机，虚拟机也可以监控主机服务器。在所有的这些场景中，监控记录和数据库必须是安全的。也必须控制对所有监控数据和管理界面的访问。

- 虚拟机也可能引起对主机的拒绝服务攻击，所有运行在一台主机上的虚拟机共享主机资源。可能会有虚拟机失去控制占用主机上的所有资源，拒绝向其它虚拟机提供服务器。需要通过对所有虚拟机实施合适的资源访问控制来防止此类问题的发生。

- 保护虚拟机——尤其是高安全虚拟机——不受外部不可控的修改。

防止修改的理想方案是确保构成虚拟机的所有文件都是经过数字签名的。

■ 同虚拟化管理程序的通信也应该自始至终都得到保护，因为这些数据中可能包含重要的信息，如特权账号的用户名和口令。大多数虚拟基础架构在所有的管理通信中都支持安全套接层（SSL：Secure Sockets Layer）的使用，但是这一项功能在默认情况下通常都没有安装。确保必须部署该功能来防止受到潜在的管理通信问题的影响。

同虚拟化管理程序的通信也应该自始至终都得到保护，因为这些数据中可能包含重要的信息。

■ 虚拟机也可以看作是一个文件夹中的一系列文件，但是这些文件中包括了相当敏感的信息，确保组成虚拟机的所有文件都放在同一个文件夹中。有些虚拟化管理程序默认情况下并不存储虚拟机文件，如同一个文件中的配置、虚拟磁盘、快照文件、内存内数据等。把这些文件保存在一起，更容易进行跟踪和监控以防止非授权访问，甚至是偷窃。

由于虚拟机是由不同的文件组成的，所以通过使用含有恶意软件的文件替换虚拟磁盘中的一个文件可以很容易威胁到系统安全。这就是要监控组成虚拟机文件很重要的一个原因。

案例分析：平衡安全性和功能性

医疗行业的软件生产商 Quantros Inc.正在稳健地涉入虚拟化技术，从而该公司的 IT 部门就不得不探索应对虚拟化安全问题的新方法。随着为医院和卫生部门开发的一系列宿主的软件即服务器（SaaS：Software-as-a-Service）应用程序以及其它内部应用程序，公司开始关注安全漏洞问题。

“其中一个挑战就是试图切割每一个应用程序”，该公司的 IT 和数据中心经理 Bryan Rood 说。Quantros 公司有 80 个内部使用者，也就是说该公司通过大概 2500 个医院为接近 300 万用户服务。在服务器通过网络相互发送数据流的时候，应用程序和虚拟主机之间需要相互通信，Rood 说，系统阻止潜在的入侵者以保证数据一定可以被接受。

在保证一切都安全或者工作正常运转之间有一个两难问题，Rood 说到，太强调严格配置的安全保证可能会影响到工作的正常完成，关键就是要找到一个折中点。

在 VMware 公司向 Rood 演示在两个工作环境中发生的通信量之后，Rood 非常希望知道流量的脆弱性。如果入侵者在 Quantros 的防火墙外部获取到网络流量并且向虚拟化管理程序发送可以接受的命令，则就会发生安全威胁。其它应用程序出于复制和其它工作的原因也会在网络之外共享数据——这也增加了系统的脆弱性。

Rood 和他的团队在两台虚拟机上测试 VMware Inc 公司的 vShield Zones 应用程序。这个应用程序作为一个深度包检测防火墙运行，该防火墙也允许为多个应用程序创建基于区域（Zone-Based）的控制。“必须确保设置虚拟化的方式在启动防火前时都完全一一兼容。我们首先以最低级别启动，然后逐步增加以验证是否能够正常工作。”

使网络认知和接受要求的改变一直以来都是最大的问题。Rood 说，“安全软件需要能够跟踪这些改变，这样才可以确保这些不是安全问题”，“我们曾尝试在虚拟平台上部署相同或者甚至比物理工作环境中更好的安全策略。”他继续说到。

实现虚拟化安全的新方法

传统的安全方法在虚拟化的世界里依然是可以使用的。用户不仅需要对服务器和相关的应用做保护，而且需要监控哪些人可以对哪些资源进行访问，对进入数据中心的访问者做鉴定和管理。赋予在数据中心内工作的用户以适当的通关权限，并在他们完成认证后给予相对应的访问权限。

另外，您还需要确保那些数据中心内可以做数据更改操作的人员都是拥有授权才这么做的，也就是说现有的安全方面的经验在虚拟环境里是可以获得延续的。如果您把现有的终端用户服务进程都迁移到了虚拟机和 VSO 上，那么传统的安全方法也应该位于同一级别上。

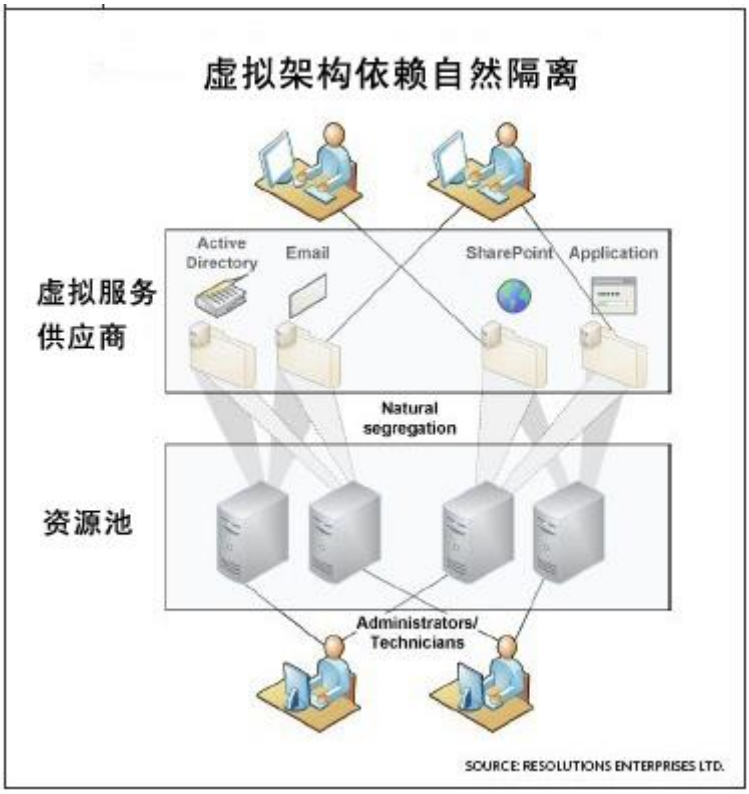
传统安全方法仍然适用于虚拟化。你不仅需要保护服务器与应用，还需要监控何人访问了何种信息。

然而不幸的是，在为 VSO 提供物理资源的资源池级别上，从设计原理看，并不具备和用户进行交互的能力。资源池内的物理机仅仅是装载了虚拟化引擎的宿主机而已。因此，也只有管理员和技术人员可以跟物理机对话。

在这些环境里（资源池和 VSO），通常运行时都带有一个特定的安全文本文件，而该文件是可以被中央目录服务所访问的。我们需要考虑分离不同环境中各自的安全文本文件。毕竟，如果资源池仅仅供管理员和

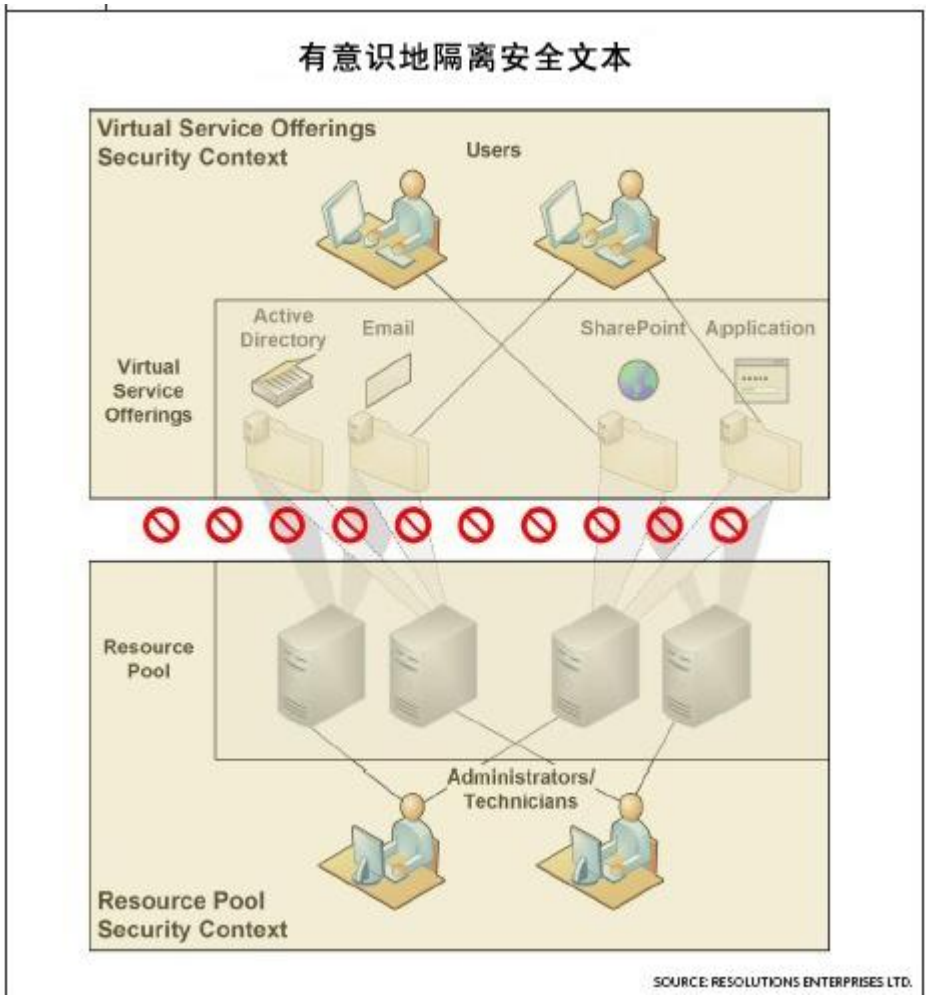
技术人员访问，看起来我们根本没有必要把资源池相关的安全文本文件开放为用户共享模式。

事实上，用户不需要对资源池做任何操作。对于最终用户而言，他们也不需要和网络环境中的路由器或交换机做交互。因此，您需要为资源池和 VSO 创建独立的安全文本文件。例如，如果您运行了 VMware 或 Citrix 的虚拟机管理程序，而您的网络服务运行于 Windows 服务器上，那么资源池的安全文本文件会自动实现和 VSO 安全文本文件的分离（图 1）。这也就是为什么宿主机环境（通常情况下是 Linux）和 VSO 通常运行于不同操作系统的原因。这种方式也自然实现了两个安全文本文件的隔离。



然而，如果宿主机和虚拟机所运行的操作系统相同的情况下，您就需要手动分离资源池和 VSO 的安全文本文件。这种情况一般发生在采用了微软的 Hyper-V 虚拟化管理程序，之上运行 Windows 网络环境的时候。同样，当我们运行了 Linux 网络环境而同时又采用了同一 Linux 系统下的虚拟化管理程序时也会发生。

以 Windows 网络环境为例，您需要分别为资源池和 VSO 创建独立的活动目录树，然后同时断开它们之间的所有连接。在两个独立的架构中创建分离的安全文本也是为了防止发生从一个环境向另一个环境中的渗漏（图 2）。



实现资源池的安全

为资源池创建独立的安全文本仅仅是实现虚拟架构安全的第一步。您还需要和其它的一些安全措施来配合使用。如下是一些额外的考虑：

- **掌控所有到资源池的访问以确保只有被信任的个体才具备访问权限。**每个访问资源池的个体应该具备一个命名账户，而该账户和普通用户用来访问 VSO 的账户命名应该是有所区别的。

- **掌控所有到资源池管理工具的访问。**只有被信任的个体拥有访问资源池组件，如物理服务器、虚拟化管理程序、虚拟网络、共享存储，及其它内容相关的管理工具的权限。向未被认证的用户开放管理工具的访问权限，就等同于向那些恶意操作开放了 IT 系统架构。

- **管理虚拟化引擎或管理程序的访问，以及其上运行的虚拟机。**所有的虚拟机都应该是首先通过系统管理员来创建和保护的。如果某些最终用户，如开发人员、测试人员或培训者，需要和网络环境中的虚拟机交互，那么这些虚拟机应该是通过资源池的管理员来创建和管理的。

- **控制虚拟机文件的访问。**通过合理的访问权限来实现所有包含了虚拟机的文件夹以及虚拟机所在压缩文件的安全。无论是在线的还是离线的虚拟机

文件都必须获得严格的管理和控制。理论上来讲，您需要同时对虚拟机文件的访问做监管。

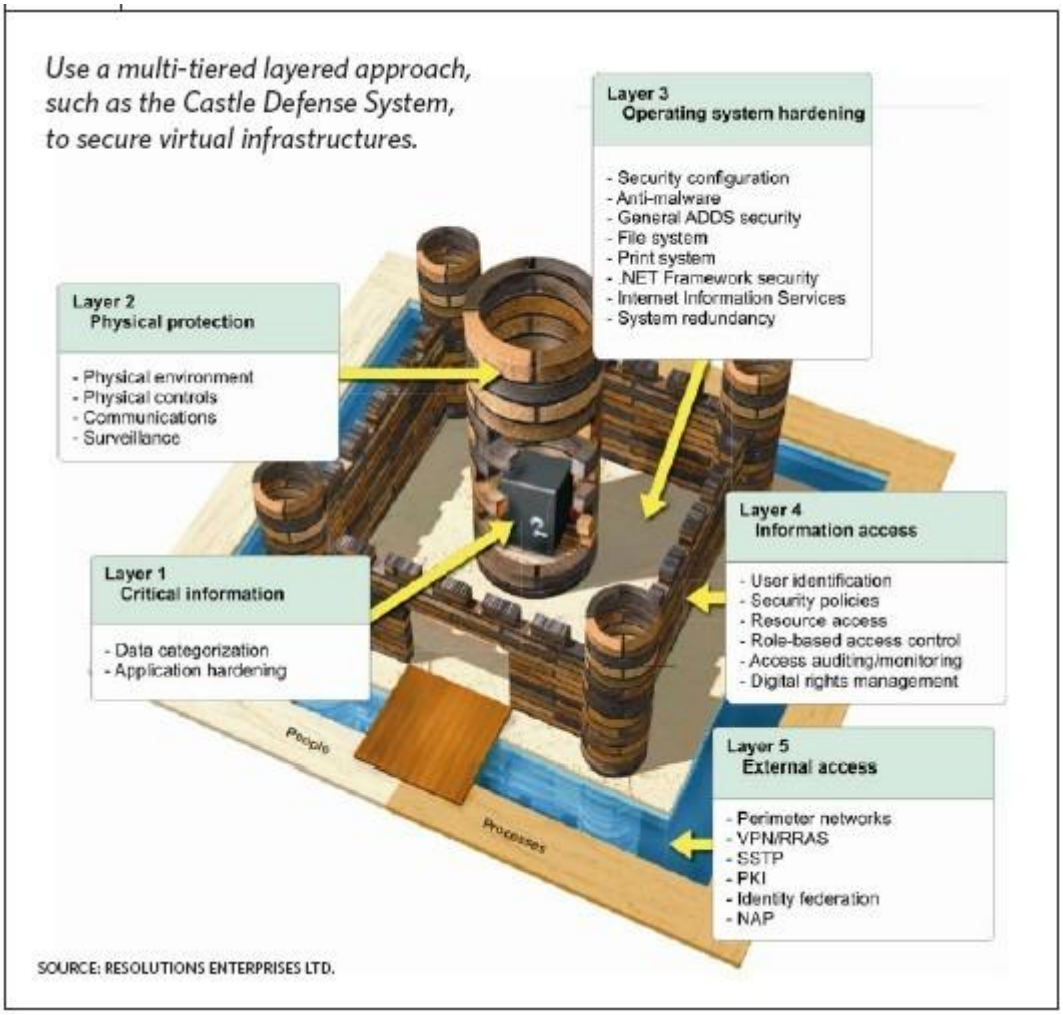
- **通过在宿主机上尽可能实现最小化安装来减少主机可能被攻击的接口。**请确保虚拟化管理程序的安装尽可能的可靠。

- **部署适合的安全工具。**为了支持合理的安全策略，您的系统架构应该包含各种必要的工具，如系统管理工具、管理清单、监管和监视工具等等，包括一些常用的安全设备。

- **分离网络流量。**在一个正确设置的资源池系统中，应该包含有几个不同的私有网络用于：管理数据流量、在线迁移流量以及存储系统流量。所有的这些网络都应该和系统架构中的公网流量相分离。

深层防护策略

除了安全文本文件的隔离外，您还应该考虑对虚拟化环境采用深层防护策略。这个像城堡一样的 CDS 防护模型是由 Resolution Enterprise Ltd.,公司提出来，该公司位于英属哥伦比亚省维多利亚地区，是一家独立的数据中心业务咨询公司，致力于推动深层防护方式。很多企业的传统服务提供网络都采用了深层防护策略，通过执行相应的策略实现对资源池的保护（图 3）。



用户可以对资源池或者 VSO 采用 CDS 防护模式。如下的表 1 也显示了在您通过部署 CDS 模式对资源池进行保护时，分别在五个不同的层次上需要去考虑的问题。在这个表里，也同时列出了在对最终用户网络和终端网络（如资源池网络）分别部署 CDS 模型时采取的组件之间的差异。

表 1

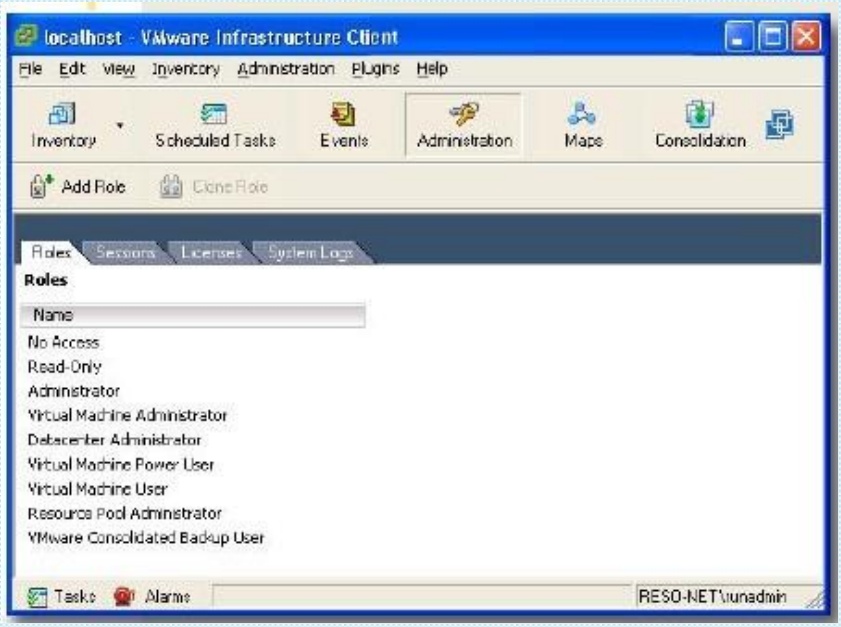
在城堡防护模型中每一层需要考虑的内容		
城堡防护层	资源池	虚拟服务提供
第一层： 关键信息	● 数据保护（虚拟机） ● 应用程序增强（管理程序）	● 数据目录 ● 应用程序增强
第二层： 物理防护	● 数据中心物理环境 ● 物理链路管理 ● 和管理员的交互问题 ● 监管	● 数据中心物理环境 ● 物理链路管理 ● 和所有用户的交互 ● 监管
第三层： 操作系统增强	● 安全配置 ● 反病毒/防止恶意攻击 ● 终端目录服务 ● 文件和打印系统 ● Web 接口 ● 系统冗余	● 安全配置 ● 防止恶意攻击 ● 生产目录服务 ● 文件和打印系统 ● Web 接口 ● 系统冗余
第四层： 信息的访问管理	● 管理员用户定义 ● 安全策略 ● 资源访问管理 ● 基于角色的访问控制 ● 访问审查/监控	● 管理员和最终用户定义 ● 安全策略 ● 资源访问管理 ● 基于角色的访问控制 ● 访问审查/监控 ● 数字化权力管理
第五层： 外围访问管理	● 周边网络 ● VPN 和 RRA ● 为管理通讯启用 SSL/PKI	● 周边网络 ● VPN 和 RRA ● SSL/PKI ● 联合定义 ● 网络访问防护

最小化访问权限防护

保护提供虚拟机服务部分（VSO）的一种方法是基于最小化访问权限的登录方式。在资源池创建这种级别的访问方式需要中央目录服务的支持。作为规则之一，中央资源池只允许被使用中的虚拟化管理程序访问，这样做是为了方式出现不一致的情况，同时也提高了安全性。

在创建中央目录服务时，建立一个终端活动目录（AD）并把它指向您的宿主机。我们可以通过 VMware vSphere 或微软的 Hyper-V 来建立。一个终端目录总包含了访问权限以及支持以管理员方式登录。它同时需要两个域控（物理的或是虚拟机的）支持。把虚拟机设置为随主机启动方式，因此确保当我们希望管理宿主机系统时它们是可用的。

创建终端目录时，建立一个包含了 vCenter 管理虚拟机在内的独立域。然后，通过在 Administration -> vCenter Management Server Configuration dialog 页面中，对 AD 启用 Light-weight Directory Access Protocol 协议。您可以采用现有的 VMware 角色（如图）或者是创建属于自己的新角色。



在 Hyper-V 中创建终端目录要复杂的多。创建两个域控并且把所有的主机都指定为成员服务器。Hyper-V 依靠 Windows 中的 e Authorization Manager (AzMan)实现基于角色的管理方式，默认创建的唯一角色就是具备全管理能力的管理员。为了创建新的角色，需要为每个角色定义任务、创建角色、分配角色定义然后把角色连接到目录中的某个组。而且 AzMan 存储的角色都是在宿主服务器本地的，所以您还需要执行同样的方式在其它的宿主机上。

预防过度管理

改善资源池安全性的另外一个方法就是限制资源池管理的数量。拥有两个具备系统环境完全访问权的管理员已经足够了。然后，根据数据中心规模大小的不同，您可以基于每个角色所需完成的任务内容分配不同的权限和角色定义。资源池管理员应该可以管理 VSO 网络。

如果你人员充足，最好分离角色。

如果您有足够的人手，那么最好把不同的管理角色分开。如果做不到的话，至少要确保管理在每个不同的环境中使用不同权限的管理角色登录。请理解，如果管理员在某个环境中扮演了指定的角色，那么他在不同的环境中完成同一动作时所扮演的角色是不同的。

最后，任何时候都要注意对虚拟机的保护。例如，虚拟机在暂停休息的状态下和活动的虚拟机相比其风险更高。因为当虚拟机处于保存状态时，会在内存中生成一个文件，而该文件保留了虚拟机所有相关内容。通过分析这个文件可以找到相应的用户名和密码相关信息。同样，如果有人窃取了虚拟机文件并带出了办公室，也会带来很大的风险。一旦他们在私有环境中搭建了该虚拟机，那么就很容易闯入我们的环境中。

我们的编辑团队

您若有何意见与建议，欢迎与我们的编辑联系。

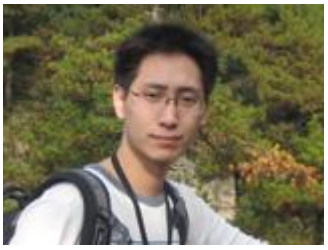
诚挚感谢以下人员热情参与 TechTarget 中国《高级虚拟化系列手册》的内容编辑工作！


关于作者

Danielle Ruest 与 Nelson Ruest 是无间断服务、可用性和基础架构优化领域的 IT 专家。他们合著了大量书籍，其中包括 Virtualization: A Beginner’ s Guide 以及 Windows Server 2008。联系方式：infos@reso-net.com。

李哲贤

TechTarget中国特邀技术编辑。六年存储行业从业经验。曾先后服务于国内外几家知名存储厂商，对存储虚拟化、容灾备份、数据中心建设等方面有较深入了解。现服务于某跨国企业，从事服务器存储销售支持工作。



王越

TechTarget特约技术编辑。毕业于北京大学，主要研究方向是虚拟化体系结构安全和可信计算技术。爱好读书、登山、旅行。