

《虚拟化安全解决方案》

图书基本信息

书名：《虚拟化安全解决方案》

13位ISBN编号：9787111522311

出版时间：2015-12-1

作者：戴夫·沙克尔福

页数：268

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu000.com

《虚拟化安全解决方案》

内容概要

本书共11章，第1章主要讲述虚拟化安全的基本理论；第2章阐释如何配置常用的管理程序平台：VMwareESXi、MicrosoftHyper-V和CitrixXenServer等；第3章讲述如何设计安全的虚拟网络，涉及虚拟网络与物理网络、虚拟网络安全考虑因素等；第4章讲述高级虚拟网络操作，内容包括网络运营挑战和解决方案，虚拟环境中的负载均衡等；第5章讲述虚拟化管理和客户端安全，涉及保护VMwarevCenter、MicrosoftSCVMM和CitrixXenCenter相关的内容；第6章讲述如何保护虚拟机，涉及安全考虑因素、威胁，虚拟机的缺陷等；第7章讲述日志和审计方面的实践，涉及日志和审计的重要意义、虚拟日志和审计选项，以及与现有日志平台集成和有效的日志管理；第8章讲述虚拟化安全的变更和配置管理，内容包括虚拟机如何影响变更和配置管理，将虚拟化集成到变更管理，虚拟化配置管理的佳实践等；第9章讲述如何应对虚拟化安全的不良后果，实现灾难恢复和商业可持续性；第10章讲述脚本自动化的技巧；第11章讲述虚拟化安全要考虑的其他因素。

书籍目录

目录	
译者序	
序言	
致谢	
第1章 虚拟化安全基础	1
1.1 虚拟化架构	1
1.2 虚拟环境的威胁	4
1.2.1 运行威胁	4
1.2.2 恶意软件威胁	5
1.2.3 虚拟机逃逸	6
1.2.4 虚拟化平台漏洞	8
1.3 安全必须适应虚拟化	8
1.3.1 安全虚拟化环境的挑战	9
1.3.2 虚拟化环境中脆弱性测试的挑战	9
第2章 安全虚拟机管理程序	12
2.1 管理程序配置和安全	12
2.2 配置VMware ESXi	14
2.2.1 给VMware ESXi打补丁	14
2.2.2 VMware ESXi的安全通信	23
2.2.3 在VMware ESXi上改变和删除默认设置	27
2.2.4 在VMware ESXi上开启运营安全	28
2.2.5 在VMware ESXi中保护和监控关键配置文件	32
2.2.6 在VMware ESXi上保护本地用户和组	34
2.2.7 锁定对虚拟机管理程序控制台的访问	40
2.3 在Windows Server 2008上配置Microsoft Hyper-V	43
2.3.1 给Hyper-V打补丁	44
2.3.2 与Hyper-V安全通信	45
2.3.3 改变Hyper-V默认设置	47
2.3.4 启用Hyper-V的运行安全	48
2.3.5 保护和监控Hyper-V关键配置文件	49
2.3.6 保护本地Hyper-V用户和组	53
2.3.7 锁定对Hyper-V管理程序平台的访问	56
2.4 配置Citrix XenServer	58
2.4.1 给XenServer打补丁	59
2.4.2 用XenServer进行安全通信	61
2.4.3 改变XenServer默认设置	62
2.4.4 启用XenServer运行安全	65
2.4.5 保护和监控关键XenServer配置文件	66
2.4.6 保护本地用户和组	67
2.4.7 锁定对XenServer平台的访问	73
第3章 设计安全的虚拟网络	77
3.1 虚拟和物理网络比较	77
3.1.1 虚拟网络设计元素	78
3.1.2 物理网络与虚拟网络	81
3.2 虚拟网络安全考虑因素	82
3.2.1 重要的安全元素	82
3.2.2 架构考虑因素	83

- 3.3 虚拟交换机安全配置 85
 - 3.3.1 定义独立的vSwitch和端口组 86
 - 3.3.2 为网络分段配置VLAN和私有VLAN 93
 - 3.3.3 限制使用中的虚拟网络98
 - 3.3.4 实现本地虚拟网络安全策略101
 - 3.3.5 iSCSI存储网络安全连接105
- 3.4 与物理网络集成 108
- 第4章 高级虚拟网络操作 110
 - 4.1 网络运营挑战 110
 - 4.2 VMware vSphere上的网络运营 111
 - 4.2.1 在vSphere虚拟环境中的负载均衡 112
 - 4.2.2 VMware vSphere中的流量整形和网络性能 114
 - 4.2.3 在VMware vSphere中建立合理的网络监控 115
 - 4.3 Microsoft Hyper-V中的网络操作 119
 - 4.3.1 Hyper-V虚拟环境中的负载均衡119
 - 4.3.2 在Hyper-V中进行流量整形和网络性能 120
 - 4.3.3 在Hyper-V中创建一个合理的网络监控策略 121
 - 4.4 Citrix XenServer中的网络操作 122
 - 4.4.1 在XenServer虚拟环境中的负载均衡 122
 - 4.4.2 XenServer上的流量整形和网络性能 124
 - 4.4.3 在XenServer中创建合理的网络监控策略 125
- 第5章 虚拟化管理和客户端安全 128
 - 5.1 管理平台的一般安全建议128
 - 5.2 虚拟化管理服务器的网络架构129
 - 5.3 VMware vCenter 132
 - 5.3.1 vCenter服务账户133
 - 5.3.2 vCenter中的安全通信134
 - 5.3.3 vCenter日志135
 - 5.3.4 vCenter中的用户、组和角色137
 - 5.3.5 角色创建场景 141
 - 5.3.6 vSphere客户端142
 - 5.4 Microsoft系统中心虚拟机管理器142
 - 5.4.1 SCVMM服务账户142
 - 5.4.2 SCVMM的安全通信143
 - 5.4.3 SCVMM日志145
 - 5.4.4 SCVMM中的用户、组和角色145
 - 5.4.5 客户端安全 147
 - 5.5 Citrix XenCenter 148
 - 5.5.1 XenCenter的安全通信148
 - 5.5.2 XenCenter的日志149
 - 5.5.3 XenCenter中的用户、组和角色 149
- 第6章 保护虚拟机 150
 - 6.1 虚拟机的威胁和漏洞150
 - 6.2 虚拟机安全研究 151
 - 6.2.1 盗取客户 152
 - 6.2.2 云虚拟机侦查 152
 - 6.2.3 虚拟硬盘操作 153
 - 6.2.4 虚拟机加密 153
 - 6.3 锁定VMware虚拟机 158

- 6.3.1 VMware工具160
- 6.3.2 复制/粘贴操作和HGFS 161
- 6.3.3 虚拟机磁盘安全161
- 6.3.4 虚拟机日志 162
- 6.3.5 设备连接 163
- 6.3.6 客户和主机通信163
- 6.3.7 控制访问虚拟机的API164
- 6.3.8 未曝光的功能 164
- 6.4 锁定Microsoft虚拟机 166
- 6.5 锁定XenServer虚拟机 168
- 第7章 日志和审计 171
 - 7.1 为什么日志和审计非常关键171
 - 7.2 虚拟日志和审计选项172
 - 7.2.1 Syslog 172
 - 7.2.2 Windows事件日志174
 - 7.2.3 VMware vSphere ESX日志 175
 - 7.2.4 VMware vSphere ESXi日志 176
 - 7.2.5 Microsoft Hyper-V和SCVMM日志 180
 - 7.2.6 Citrix XenServer和XenCenter日志 186
 - 7.3 与现有日志平台集成189
 - 7.3.1 在VMware vSphere上启用远程日志 189
 - 7.3.2 在Microsoft Hyper-V上启用远程日志 191
 - 7.3.3 启用XenServer远程日志 192
 - 7.4 有效的日志管理 193
- 第8章 变更和配置管理 196
 - 8.1 变更和配置管理概述196
 - 8.1.1 变更管理的安全197
 - 8.1.2 变更生态系统 198
 - 8.2 虚拟化如何影响变更和配置管理200
 - 8.3 虚拟化配置管理的佳实践200
 - 8.4 提高配置管理的复制和模板202
 - 8.4.1 创建和管理VMware vSphere虚拟机模板与快照 203
 - 8.4.2 创建和管理Microsoft Hyper-V虚拟机模板与快照 207
 - 8.4.3 创建和管理Citrix XenServer虚拟机模板与快照 210
 - 8.5 将虚拟化集成到变更和管理212
 - 8.6 附加解决方案和工具214
- 第9章 灾难恢复和业务连续性 215
 - 9.1 当今灾难恢复和业务连续性215
 - 9.2 共享存储和复制 216
 - 9.3 DR/BCP的虚拟化冗余性和容错性218
 - 9.3.1 集群 218
 - 9.3.2 资源池 223
 - 9.4 高可用性和容错性 229
 - 9.4.1 在VMware vSphere中设置高可用性和容错性 229
 - 9.4.2 在Microsoft Hyper-V中设置高可用性和容错性 233
 - 9.4.3 在Citrix XenServer中设置高可用性和容错性 235
- 第10章 脚本使用提示和自动化技巧 238
 - 10.1 为什么脚本对管理员重要238
 - 10.2 VMware脚本：PowerCLI和vCLI 239

- 10.2.1 PowerCLI脚本239
- 10.2.2 用PowerCLI配置虚拟机 240
- 10.2.3 用vCLI配置虚拟机 242
- 10.2.4 用PowerCLI配置VMwareESXi 243
- 10.2.5 用vCLI配置VMware ESXi 245
- 10.2.6 用PowerCLI配置VMware虚拟网络 246
- 10.2.7 用vCLI配置VMware虚拟网络 249
- 10.2.8 用PowerCLI配置VMwarevCenter 250
- 10.3 Microsoft Hyper-V脚本：PowerShell 253
 - 10.3.1 获得关于虚拟机的信息254
 - 10.3.2 获得关于虚拟网络的信息255
 - 10.3.3 评估虚拟环境的其他方面255
- 10.4 Citrix脚本：命令行脚本256
- 第11章 虚拟基础设施的其他安全考虑因素 258
 - 11.1 VDI概述 258
 - 11.1.1 VDI的优势和缺点：运营和安全259
 - 11.1.2 安全优势和挑战259
 - 11.1.3 VDI架构概述261
 - 11.2 VDI的安全利用264
 - 11.2.1 存储虚拟化 264
 - 11.2.2 应用程序虚拟化267

《虚拟化安全解决方案》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu000.com