

Security

Environments^N

Dave Shackelford

'' J J H - .i
sij!

''ij

li

in:

John Wiley & Sons, Inc.

Contents

Chapter 1 • Fundamentals of Virtualization Security	1
Virtualization Architecture	1
Threats to a Virtualized Environment	4
Operational Threats	4
Malware-Based Threats	5
VM Escape	6
Vulnerabilities in Virtualization Platforms	9
How Security Must Adapt to Virtualization	9
Challenges for Securing Virtualized Environments	10
Challenges of Vulnerability Testing in a Virtualized Environment	10
Chapter 2 • Securing Hypervisors	15
Hypervisor Configuration and Security	15
Configuring VMware ESXi	17
Patching VMware ESXi	17
Securing Communications in VMware ESXi	27
Change and Remove Default Settings on VMware ESXi	33
Enable Operational Security on VMware ESXi	34
Secure and Monitor Critical Configuration Files in VMware ESXi	38
Secure Local Users and Groups on VMware ESXi	40
Lock Down Access to Hypervisor Console	47
Configuring Microsoft Hyper-V on Windows Server 2008	52
Patching Hyper-V	53
Securing Communications with Hyper-V	53
Changing Hyper-V Default Settings	56
Enabling Operational Security for Hyper-V	59
Securing and Monitoring Critical Configuration Files for Hyper-V	60
Secure Local Hyper-V Users and Groups	63
Lock Down Access to the Hyper-V Hypervisor Platform	68
Configuring Citrix XenServer	72
Patching XenServer	72
Secure Communications with XenServer	75
Change XenServer Default Settings	76
Enabling XenServer Operational Security	80
Secure and Monitor Critical XenServer Configuration Files	81
Secure Local Users and Groups	81
Lock Down Access to the XenServer Platform	88

Chapter 3 • Designing Virtual Networks for Security	93
Comparing Virtual and Physical Networks	93
Virtual Network Design Elements	95
Physical vs. Virtual Networks	98
Virtual Network Security Considerations	99
Important Security Elements	99
Architecture Considerations..	100
Configuring Virtual Switches for Security	102
Defining Separate vSwitches and Port Groups	103
Configuring VLANs and Private VLANs for Network Segmentation	112
Limiting Virtual Network Ports in Use	117
Implementing Native Virtual Networking Security Policies	122
Securing iSCSI Storage Network Connections	125
Integrating with Physical Networking	129
 Chapter 4 • Advanced Virtual Network Operations	 131
Network Operational Challenges	131
Network Operations in VMware vSphere	133
Load Balancing in vSphere Virtual Environments	133
Traffic Shaping and Network Performance in VMware vSphere	135
Creating a Sound Network Monitoring Strategy in VMware vSphere	136
Network Operations in Microsoft Hyper-V	141
Load Balancing in Hyper-V Virtual Environments ...:	141
Traffic Shaping and Network Performance in Hyper-V	142
Creating a Sound Network Monitoring Strategy in Hyper-V	144
Network Operations in Citrix XenServer	145
Load Balancing in XenServer Virtual Environments	145
Traffic Shaping and Network Performance in XenServer	148
Creating a Sound Network Monitoring Strategy in XenServer	148
 Chapter 5 • Virtualization Management and Client Security	 151
General Security Recommendations for Management Platforms	151
Network Architecture for Virtualization Management Servers	152
VMware vCenter	155
vCenter Service Account	157
Secure Communications in vCenter	158
vCenter Logging	160
Users, Groups, and Roles in vCenter	163
Role Creation Scenarios	167
vSphere Client	168
Microsoft System Center Virtual Machine Manager	168
SCVMM Service Account	169
Secure Communications with SCVMM	170
SCVMM Logging	171
Users, Groups, and Roles in SCVMM	172
Client Security	175

Citrix XenCenter	175
Secure Communication with XenCenter	175
Logging with XenCenter	176
Users, Groups, and Roles in XenCenter	176
Chapter 6 « Securing the Virtual Machine	177
Virtual Machine Threats and Vulnerabilities'	177
Virtual Machine Security Research	178
Stealing Guests	179
Cloud VM Reconnaissance	179
Virtual Disk Manipulation	180
Virtual Machine Encryption	180
Locking Down VMware VMs	185
VMware Tools	188
Copy/Paste Operations and HGFS	188
Virtual Machine Disk Security	189
VM Logging	189
Device Connectivity	190
Guest and Host Communications	191
Controlling API Access to VMs	192
Unexposed Features	193
Locking Down Microsoft VMs	195
Locking Down XenServer VMs	197
Chapter 7 « Logging and Auditing	201
Why Logging and Auditing Is Critical	201
Virtualization Logs and Auditing Options	202
Syslog	203
Windows Event Log	204
VMware vSphere ESX Logging	205
VMware vSphere ESXi Logging	207
Microsoft Hyper-V and SCVMM Logging	211
Citrix XenServer and XenCenter Logging	218
Integrating with Existing Logging Platforms	221
Enabling Remote Logging on VMware vSphere	221
Enabling Remote Logging on Microsoft Hyper-V	223
Enabling Remote Logging for XenServer	225
Effective Log Management	226
Chapter 8 ⁰ Change and Configuration Management	229
Change and Configuration Management Overview	229
Change Management for Security	230
The Change Ecosystem	231
How Virtualization Impacts Change and Configuration Management	234
Best Practices for Virtualization Configuration Management	235

Cloning and Templates for Improved Configuration Management	237
Creating and Managing VMware vSphere VM Templates and Snapshots	238
Creating and Managing Microsoft Hyper-V VM Templates and Snapshots	242
Creating and Managing Citrix XenServer VM Templates and Snapshots	247
Integrating Virtualization into Change and Management	249
Additional Solutions and Tools	250
Chapter 9 • Disaster Recovery and Business Continuity	253
Disaster Recovery and Business Continuity Today	253
Shared Storage and Replication	254
Virtualization Redundancy and Fault Tolerance for DR/BCP	256
Clustering	256
Resource Pools	262
High Availability and Fault Tolerance	270
Setting Up High Availability and Fault Tolerance in VMware vSphere	270
Setting Up High Availability and Fault Tolerance in Microsoft Hyper-V	274
Setting Up High Availability and Fault Tolerance in Citrix XenServer	277
Chapter 10 • Scripting Tips and Tricks for Automation	281
Why Scripting Is Essential for Admins	281
VMware Scripting: Power CLI and vCLI	282
Scripting with PowerCLI	282
Configuring VMs with PowerCLI	283
Configuring VMs with vCLI	285
Configuring VMware ESXi with PowerCLI	286
Configuring VMware ESXi with the vCLI	289
Configuring VMware Virtual Networks with PowerCLI	290
Configuring VMware Virtual Networks with the vCLI	293
Configuring VMware vCenter with PowerCLI	294
Microsoft Scripting for Hyper-V: PowerShell	297
Getting Information about VMs	298
Getting Information about the Virtual Network	299
Assessing Other Aspects of the Virtual Environment	299
Citrix Scripting: Shell Scripts	300
Chapter 11 • Additional Security Considerations for Virtual Infrastructure	303
VDI Overview	303
VDI Benefits and Drawbacks: Operations and Security	304
Security Advantages and Challenges	304
VDI Architecture Overview	307
Leveraging VDI for Security	310
Storage Virtualization	310
Application Virtualization	313