



SVEN AHNERT

Virtuelle Maschinen mit VMware und Microsoft

Für Entwicklung, Schulung, Test und Produktion

- › Sofort nachvollziehbare Praxisworkshops
- › VMware Server, Player, Workstation 5.5, ESX Server 3, Microsoft Virtual Server 2005 R2, Virtual PC 2004

 ADDISON-WESLEY

VMware Server, Player
und Workstation
Tools, Treiber, Skripte



Virtuelle Maschinen mit VMware und Microsoft

Netzwerke, Betriebssysteme, Sicherheit ... hierzu bietet Ihnen die Reihe net.com umfassende, praxisnahe Information. Neben Fragen der Systemverwaltung greift sie auch Themen wie Protokolle, Technologien und Tools auf. Profitieren Sie bei Ihrer täglichen Arbeit vom Praxiswissen unserer erfahrenen Autoren.



Planungsbuch Microsoft-Netzwerke

Thomas Joos

624 Seiten, € 59,95 [D]

ISBN 3-8273-2386-X

IT-Leiter, -Administratoren und -Berater erhalten mit diesem Buch kompetente Informationen zur Planung eines Netzwerks mit Microsoft-Technologien (Windows Server 2003 R2, Exchange Server 2003 SP2, ISA 2004 SP2, WSUS, SharePoint u.v.m.). Themen sind u.a. Viren- und Spamschutz, Notfallkonzepte, VPN und Terminalserver. Sie finden einen Vergleich der verschiedenen Serverversionen und Speichermedien und erfahren alles über das perfekte Zusammenspiel der wichtigsten Produkte.



Windows Server 2003 R2

Eric Tierling

1416 Seiten, € 49,95 [D]

ISBN 3-8273-2463-7

Der Bestseller zu Windows Server 2003 jetzt aktuell zur Version R2. Die detaillierte Beschreibung von Active Directory, Gruppenrichtlinien, Windows NT-Domänenupgrade, TCP/IP-Diensten und Sicherheitsmerkmalen ermöglicht Unternehmen einen optimalen Einsatz. Clustering, E-Mail-Server, GPMC, Terminaldienste, Remote-Desktop und Webverwaltung, Volumen-Schattenkopie sowie die Smartcard-Integration und sichere Wireless-LAN-Unterstützung stellen weitere Highlights dieses Buches dar. Ebenfalls berücksichtigt werden WSUS sowie 64-Bit-Computing. Mit einer 180-Tage Trial-Version von Windows Server 2003 R2 auf zwei CDs.

Sven Ahnert

Virtuelle Maschinen mit VMware und Microsoft

Für Entwicklung, Schulung,
Test und Produktion



ADDISON-WESLEY

An imprint of Pearson Education

München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Bibliografische Information Der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt. Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Für Verbesserungsvorschläge und Hinweise auf Fehler sind Verlag und Herausgeber dankbar.

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung der in diesem Produkt gezeigten Modelle und Arbeiten ist nicht zulässig.

Fast alle Hard- und Softwarebezeichnungen und weitere Stichworte und sonstige Angaben, die in diesem Buch verwendet werden, sind als eingetragene Marken geschützt. Da es nicht möglich ist, in allen Fällen zeitnah zu ermitteln, ob ein Markenschutz besteht, wird das ® Symbol in diesem Buch nicht verwendet.

Umwelthinweis:

Dieses Buch wurde auf chlorfrei gebleichtem Papier gedruckt.

10 9 8 7 6 5 4 3 2

08 07

ISBN-13: 978-3-8273-2374-3

© 2007 by Addison-Wesley Verlag,
ein Imprint der Pearson Education Deutschland GmbH,
Martin-Kollar-Straße 10–12, D-81829 München/Germany

Alle Rechte vorbehalten

1., korrigierter Nachdruck

Einbandgestaltung: Marco Lindenbeck, webwo GmbH, mlindenbeck@webwo.de

Fachlektorat: Thomas Joos, thomas.joos@web.de

Lektorat: Sylvia Hasselbach, shasselbach@pearson.de

Korrektorat: Sandra Gottmann, sandra.gottmann@t-online.de

Herstellung: Claudia Bäurle, cbaurle@pearson.de

Satz: mediaService, Siegen, www.media-service.tv

Druck und Verarbeitung: Bercker Graph. Betrieb, Kvelaer

Printed in Germany

Inhaltsverzeichnis

Einleitung	21
Eine Technologie revolutioniert die IT-Branche – Virtualisierung!	21
Was sind virtuelle Maschinen?	22
Nützen Ihnen virtuelle Maschinen?	23
Welche Vorteile haben virtuelle Maschinen?	24
Größere Flexibilität gegenüber echter Hardware	24
Hardware-Unabhängigkeit der Gastsysteme in den VMs	25
Vorteile virtueller Maschinen im täglichen Einsatz	25
Die Hemmschwelle: Nachteile, Stabilität, Sicherheit virtueller Maschinen	26
Erfahrungen mit dem Einsatz virtueller Maschinen	26
Nachteile und Grenzen virtueller Maschinen	26
Was ist das Anliegen dieses Buches, und für wen habe ich es geschrieben?	27
Neueinsteigern helfen	27
Erfahrenen Anwendern weiteres Know-how vermitteln	27
Praxisbezogener Sofort-Einstieg mit Workshops	28
VMware Player, Workstation und Server sowie Microsoft Virtual PC und Server	28
VMware-Produkte in diesem Buch	28
Microsoft-Produkte in diesem Buch	28
Der Aufbau dieses Buches in drei Teilen	28
Teil 1 – Einstieg: allgemeine Einführung und Grundlagen	29
Teil 2 – Praxis: sofort nachvollziehbare Workshops	29
Teil 3 – Technik: Hintergründe, Tipps und Tricks	29
E Die Icons in diesem Buch	30
Verwendung dieses Buches – wie kommen Sie schnell zum Ziel?	30
Wie sollten Sie als Einsteiger die Kapitel durcharbeiten?	31
Wie sollten Sie als erfahrener Anwender die Kapitel durcharbeiten?	32
Teil 1 Allgemeine Einführung und Grundlagen	33
1 Grundlagen virtueller Maschinen und Hinweise zur Hardware	35
1.1 Wichtige Begriffe bei der Arbeit mit virtuellen Maschinen	35
1.1.1 Was ist der Host bzw. der Wirt?	36
1.1.2 Was ist eine VM bzw. ein Gast?	36
1.1.3 Was macht der Virtualisierungslayer?	36
1.2 So funktioniert eine virtuelle Maschine	37
1.2.1 Die wichtigsten Eigenschaften einer VM	37
1.2.2 Der Unterschied von Virtualisierung und Emulation	38
1.2.3 Was passiert intern in einer VM?	39

1.3	Das Wichtigste zur Hardware auf dem Host und in den VMs	44
1.3.1	Die Prozessoren auf dem Host und im Gast	44
1.3.2	Der Hauptspeicher auf dem Host und in den Gästen	47
1.3.3	Platten, CD und Floppy in den virtuellen Maschinen	49
1.3.4	Arten von physischen Host-Datenträgern als Speicherplatz für virtuelle Platten und ISO-Images	50
1.3.5	Physische und virtuelle Netzwerkkarten	56
1.3.6	USB, Sound und Schnittstellen	57
1.3.7	Physische SCSI-Geräte aus den Gästen ansprechen	58
1.3.8	VGA, Tastatur und Maus zwischen Gast und Host teilen	58
1.3.9	Nicht unterstützte Hardware in den Gästen	59
1.3.10	Wie geht es jetzt weiter?	60
2	Das richtige Virtualisierungsprodukt für Sie	61
2.1	Anforderungen an virtuelle Maschinen für Testumgebungen oder Produktion	61
2.2	Die Desktop-Produkte VMware Workstation, Player und MS Virtual PC	63
2.2.1	VMware Player	63
2.2.2	VMware Workstation 5.5/6	65
2.2.3	Microsoft Virtual PC 2004 SP1 und 2007	66
2.3	Die Hosted Server-Produkte VMware Server und Microsoft Virtual Server	68
2.3.1	VMware Server 1.0	68
2.3.2	Microsoft Virtual Server 2005 R2	70
2.4	Das Data Center-Produkt VMware ESX Server 3	72
2.5	Vorteile und Nachteile eines Host-Betriebssystems als Zwischenschicht	74
2.5.1	Direkter Hardware-Zugriff ohne Wirts-OS	74
2.5.2	Umweg über ein Wirts-OS	75
2.5.3	Aspekte der Bedienung	75
2.6	Die weiteren VMware-Produkte im Überblick	75
2.6.1	VMware Virtual Center	75
2.6.2	VMware ACE (Assured Computing Environment)	77
2.6.3	VMware Virtual Desktop Infrastructure (VDI)	77
2.6.4	VMware Technology Network (VMTN) als Jahresabo aller Produkte für Entwickler	78
2.6.5	VMware Virtual Appliance Marketplace – vorkonfigurierte lauffähige VMs zum Herunterladen	79
2.6.6	VMware Virtual Lab Manager 2.4 – Verwaltung von Testumgebungen	79
2.6.7	VMware-Hilfsprogramme wie P2V, Converter oder Importer	79
2.6.8	Wie geht es jetzt weiter?	79
3	Installation und Konfiguration der einzelnen Produkte	81
3.1	Allgemeine Voraussetzungen und Vorbereitung für die Installation	81
3.1.1	Hardware-Voraussetzungen auf dem Host	81
3.1.2	Voraussetzungen an das Host-Betriebssystem	85
3.1.3	Vereinfachte Lizenzierung von Microsoft Windows Server 2003 R2 Enterprise Edition in VMs	86

3.2	Installation der Produkte	87
3.2.1	Installation von VMware Workstation und VMware Player	87
3.2.2	Installation von VMware Server	89
3.2.3	Die VMware-Produkte unter Linux installieren	93
3.2.4	Installation von VMware ESX-Server 3	95
3.2.5	Installation von Microsoft Virtual PC 2004 SP1/2007	96
3.2.6	Installation von Microsoft Virtual Server 2005 R2	97
3.2.7	Wie geht es jetzt weiter?	101
4	Bedienung der Produkte – wichtige Funktionen und Tipps	103
4.1	Was sind die VMware Tools?	103
4.2	Bedienung des VMware Players	105
4.3	Bedienung von VMware Workstation und VMware Server	106
4.3.1	Die Bedienoberflächen von VMware Workstation und VMware Server im Überblick	106
4.3.2	Die wichtigsten Funktionen und Tipps zur Bedienung von VMware Workstation und Server	110
4.4	VMware Tools in Windows- und Linux-Gästen installieren	125
4.4.1	Installation der VMware Tools in Windows-Gästen	125
4.4.2	Installation der VMware Tools in Linux-Gästen	126
4.5	Microsoft Virtual Machine Additions	132
4.5.1	Was sind die Microsoft Virtual Machine Additions?	132
4.5.2	Installation der Virtual Machine Additions im Gast	133
4.6	Bedienung von Microsoft Virtual PC	134
4.6.1	Unterschiede von Virtual PC und Virtual Server	134
4.7	Bedienung von Microsoft Virtual Server	135
4.7.1	Die Bedienoberflächen von Microsoft Virtual Server im Überblick	136
4.7.2	Die wichtigsten Funktionen und Tipps zur Bedienung von Microsoft Virtual Server	137
Teil 2	Praxis-Workshops mit nachvollziehbaren Projekten	153
1	Eine Testumgebung mit VMware Workstation oder Server aufbauen	155
1.1	Vorteile virtueller Maschinen in Testumgebungen	156
1.1.1	Unterschiede zwischen VMware Server und VMware Workstation	156
1.1.2	Weiterführende Workshops zu den Produkten	157
1.2	Voraussetzungen zur Arbeit mit virtuellen Maschinen unter VMware	157
1.2.1	Der Host-Rechner oder Wirt als Basis für die VMs	158
1.2.2	Installieren und Einrichten von VMware Workstation und VMware Server	158
1.3	Die erste virtuelle Maschine erstellen und konfigurieren	159
1.3.1	Grundausstattung der VM mit dem Virtual Machine Wizard konfigurieren	159
1.3.2	Die Erstellung der ersten VM als Zusammenfassung auf einen Blick	167

1.4	Das VMware-Fenster und seine wichtigsten Bedienelemente	168
1.5	Installation des Betriebssystems in der neuen VM	169
1.5.1	Installation von CD oder ISO-Image	169
1.5.2	Verwendung von Tastatur und Maus in einem Gast	170
1.5.3	Die Funktion der VMware Tools in einem Gast	171
1.6	Mit Snapshots Systemzustände sichern	172
1.6.1	Zustände sichern und Änderungen verwerfen	172
1.6.2	Snapshots mit VMware Workstation und VMware Server anlegen und verwalten	173
1.6.3	Platten vor Datenverlust durch Revert schützen	175
1.7	Kommunikation und Datenaustausch der Gäste	176
1.7.1	Drag&Drop sowie Shared Folders zum Datenaustausch mit dem Host	176
1.7.2	ISO-Images als CD im Gast verwenden	177
1.7.3	Netzwerk zum Datenaustausch und zur Kommunikation mit dem Host und dem LAN	177
1.8	Die Betriebssysteminstallation und Konfiguration der VM auf einen Blick	179
1.9	Klonen von Gästen und weitere VMs für die Testumgebung erstellen	180
1.9.1	Kopieren virtueller Platten zum Klonen eines Gastsystems	180
1.9.2	Linked Clones mit VMware Workstation zum schnellen Klonen	180
1.9.3	Teams fassen mehrere VMs zusammen	182
1.10	Wie geht es jetzt weiter?	183
2	Mobile virtuelle Entwicklungs- und Demo-Umgebung mit Virtual PC	185
2.1	Virtueller Webserver für Test und Demo	186
2.2	Voraussetzungen für Virtual PC	187
2.2.1	Einrichtung von Virtual PC	187
2.3	Die erste VM zusammenbauen	188
2.3.1	Assistent für neuen virtuellen Computer	189
2.3.2	Einstellungen einer VM	190
2.3.3	Die virtuellen Platten einer virtuellen Maschine unter Virtual PC	191
2.3.4	Der Zusammenbau der virtuellen Maschine auf einen Blick	193
2.4	Die Virtual PC-Konsole	194
2.5	Installation des Betriebssystems in der VM	195
2.5.1	Das Wichtigste zur Bedienung der VM	196
2.5.2	Virtual Machine Additions im Gast installieren	198
2.6	Zustände des Gastes sichern und Änderungen rückgängig machen	199
2.6.1	Rückgängig-Datenträger verwenden	200
2.6.2	Differenzierende Platten für die Sicherung des Zustandes und schnelles Klonen	202
2.6.3	Datenplatten vor versehentlichem Verwerfen schützen	204
2.7	Klonen von fertig installierten virtuellen Maschinen	204
2.7.1	Ordner einer VM oder nur die virtuellen Platten kopieren	204
2.7.2	Klonen von virtuellen Systemen mit differenzierenden virtuellen Festplatten	205
2.7.3	Einbinden der geklonten Platten und Nacharbeit am Klon	205

2.8	Kommunikation und Datenaustausch der Gäste mit dem LAN und dem Host	205
2.8.1	ISO-Images für häufig verwendete CDs	206
2.8.2	Drag&Drop oder freigegebene Ordner zum einfachen Datenaustausch	206
2.8.3	Netzwerk zur Kommunikation der Gäste mit dem LAN oder Internet	206
2.9	Webserver fertig stellen und weitergeben	208
2.10	Weitere VMs in der Testumgebung erstellen und vernetzen	209
2.11	Umsetzung der Testumgebung mit VMware	209
3	Virtuelle DMZ mit Firewall und Webserver im Internet	211
3.1	Praktische Anwendung virtueller Netzwerke	212
3.1.1	Mehrstufiger Ausbau des Workshops vom einfachen Surfschutz bis zur vollwertigen DMZ	213
3.2	Anforderungen an den Host-PC	215
3.2.1	Die physischen Netzwerkkarten im Host-PC	216
3.3	Der Aufbau der Firewall-VM in Ausbaustufen	216
3.3.1	Die Software in der Firewall-VM	216
3.3.2	Die virtuellen Netzwerkkarten der Firewall-VM	218
3.3.3	Zusammenbauen der Firewall-VM	219
3.3.4	Netzwerkconfiguration der Firewall-VM	220
3.3.5	Installation von IPCop in der Firewall-VM	224
3.3.6	Netzwerkconfiguration von IPCop	227
3.3.7	Abschluss der IPCop-Installation	229
3.4	Ergänzungen zu den ersten beiden Ausbaustufen	230
3.4.1	Ausbaustufe 1, Kommunikation mit der Firewall ohne LAN-Anbindung	230
3.4.2	Ausbaustufe 2, LAN-Anbindung über das Bridged-Netz VMnet0	232
3.4.3	Testen der Ausbaustufen 1 und 2	233
3.4.4	Verwendung eines Routers am roten Interface von IPCop	234
3.5	Internet-Zugang der Firewall einrichten	238
3.5.1	Konfiguration mit dem Web-Interface von IPCop	238
3.5.2	Einstellungen an den LAN-Clients	239
3.6	Die Server in der DMZ installieren	240
3.6.1	Netzwerkconfiguration in der DMZ	240
3.6.2	Zugriff auf die DMZ vom Internet aus zulassen	240
3.6.3	DynDNS für DSL-Anschlüsse ohne feste IP-Adresse einrichten	241
3.7	Abschließende Einstellungen am Host und an den VMs	243
3.8	Ausblick auf die Möglichkeiten von Ausbaustufe 4 der DMZ	244
3.8.1	Beispiele für den weiteren Ausbau der DMZ	244
3.9	Sicherheit – sind Löcher in der VM möglich?	245
3.9.1	VMs in der DMZ optimal isolieren	246
3.10	Umsetzung mit Microsoft Virtual PC 2004/2007 und Virtual Server 2005 R2	247

4	Linux-Host mit VMware Server und Integration ins Windows-Netz	249
4.1	VMware unter Linux als kostenlose Einstiegslösung	250
4.2	Beschreibung des Projekts	250
4.2.1	Windows-Integration des Linux-Hosts	251
4.2.2	Debian als Host-System	251
4.2.3	SUSE als unterstütztes Host-System	251
4.3	Vorbereitung der Installation des Host-Systems	252
4.3.1	Hardware-Voraussetzungen für den Host	252
4.3.2	Benötigte Software für die komplette Installation von Debian und VMware	252
4.4	Installation von Debian Linux als Basis auf der Hardware	253
4.4.1	Grundinstallation von Debian auf dem Host	253
4.4.2	Weitere Pakete auf dem Host installieren	258
4.4.3	Netzwerk auf dem Host konfigurieren und vorbereiten	259
4.5	Installation von VMware auf dem vorbereiteten Host	260
4.5.1	Vorbereitung zur VMware-Installation	260
4.5.2	Installation des VMware Servers	260
4.5.3	Installation des Web-Interface vom VMware Server	261
4.5.4	Steuerung von VMware direkt am Host	261
4.6	Bedienung und Konfiguration des VMware Servers von einem Windows-Client	262
4.6.1	Das Web-Interface und die Remote-Konsole des VMware Servers	262
4.6.2	Besonderheiten unter Linux bei der Arbeit mit VMware	263
4.6.3	Weitere nützliche Programme für die Bedienung vom Client – putty und winscp	264
4.7	Die weitere Konfiguration des Hosts zur Windows-Anbindung	264
4.7.1	Host-Verzeichnisse im Windows-Netzwerk mit Samba freigeben	264
4.7.2	Vom Host auf Windows-Freigaben anderer Server zugreifen	265
4.7.3	Eine NTFS-Partition am Linux-Host einbinden und lesen	266
4.8	Die gesamte Installation und Konfiguration auf einen Blick	267
4.9	Mehr als 4 GB RAM im Host mit PAE verwenden	268
4.9.1	Kernel mit PAE-Option neu übersetzen	269
4.10	Installation des VMware Servers unter SUSE Linux	271
4.10.1	Installation von SUSE Linux 10	271
4.11	Links zur benötigten Software	275
5	Virtuelle Umgebungen mit dem VMware Player weitergeben	277
5.1	Praktische Verwendung von VMware Player	278
5.1.1	Unterschiede und Gemeinsamkeiten zu den Vollprodukten	278
5.1.2	Versionen des VMware Players	280
5.1.3	Anwendungsbeispiele des Players für verschiedene Einsatzzwecke	280

5.2	Umgang mit dem VMware Player	282
5.2.1	Einschalten einer virtuellen Maschine und Abschalten mit PowerOff oder Suspend	282
5.2.2	Geräte und RAM einer VM zuweisen	284
5.2.3	Der virtuelle Bildschirm der Gäste	284
5.3	VMs für den Einsatz im Player vorbereiten und optimieren	284
5.3.1	Die virtuellen Platten optimieren	284
5.3.2	Snapshots mit dem VMware Player benutzen	285
5.3.3	Linked Clones mit dem VMware Player benutzen	288
5.3.4	Der Player kennt keine Teamfunktion der VMware Workstation	289
5.3.5	Dualprozessor-VMs im Player betreiben	289
5.3.6	VMs von einem Linux-Host im Player benutzen	289
5.3.7	Lauffähige VMs verteilen und weitergeben	290
5.4	Platz in den Gästen sparen	290
5.5	Netzwerkunterstützung des VMware Players	291
5.6	Versteckte Funktionen zutage fördern	292
5.6.1	Netzwerkkarten hinzufügen oder im Custom-Modus betreiben	292
5.6.2	Virtuelles CD-Laufwerk mit ISO-Image betreiben	293
5.6.3	Virtuelle Platten hinzufügen	293
5.6.4	UUID-Abfrage nach dem Kopieren unterdrücken	293
5.6.5	Arbeit mit Snapshots, die in den Vollprodukten gesetzt wurden	293
5.7	Gäste von Microsoft Virtual PC im VMware Player betreiben	294
5.8	Neue VMs für den Player ohne Vollprodukt erstellen	294
6	Schulung und Demo mit VMware Player und Workstation	297
6.1	Virtuelle Maschinen in Schulungen einsetzen	298
6.1.1	Vorteile und Nachteile einer virtuellen Schulungs- oder Demo-Umgebung	298
6.2	Konzept der Schulungsumgebung mit dem VMware Player	299
6.2.1	Der Master-PC zum Erstellen und Verwalten der Vorlagen	299
6.2.2	Die Schüler-PCs als Wirtsrechner für die Schulungs-VMs	300
6.2.3	Die Vorlage-VM auf der Buch-CD	300
6.2.4	Andere Lösungsansätze mit einem zentralen VMware Server anstelle des Players	301
6.3	Erstellen der Muster-VMs als Vorlage für die Schulungssysteme unter dem Player	302
6.3.1	Schritt für Schritt: Anleitung zur Installation der Muster-VM	302
6.4	Installation der VMware Tools in einem Gast unter dem VMware Player	306
6.5	Erweiterte Konzepte für die Verwendung der virtuellen Maschinen	307
6.5.1	Zentrale Ablage der virtuellen Basisplatte mit linked Clones für die Schüler	307
6.5.2	Personalisierte Verwendung der Schüler-VMs	309
6.5.3	Wichtiger Hinweis zum Redo-Log der Vorlage-VM	309
6.5.4	Basis-PC durch Vollbild vor dem Teilnehmer verbergen	310
6.5.5	Zusammenarbeit mit der Workstation oder dem Server als Master-PC	311

7	Eine virtuelle Pilotumgebung als Testfeld für produktive Einsätze	313
7.1	Einstieg mit einer Pilotumgebung	314
7.1.1	Vorstellung der Vorgehensweise an einem exemplarischen Beispiel	314
7.2	Vorbereitung der Verwendung von Microsoft Virtual Server 2005 R2	315
7.3	Die erste VM mit Virtual Server erstellen und installieren	316
7.3.1	Erstellen der ersten virtuellen Maschine	317
7.3.2	Installation des Betriebssystems in der virtuellen Maschine	322
7.4	Virtuelle Netzwerke unter Microsoft Virtual Server 2005 R2	325
7.4.1	Anschlusstypen virtueller Netzwerkadapter	325
7.5	Wiederanlaufpunkte durch Differenzplatten oder Rückgängig-Datenträger	326
7.5.1	Mit Differenzplatten den Zustand einer Installation sichern oder weitere Duplikate klonen	326
7.5.2	Mehrere Wiederanlaufpunkte mit kaskadierenden Differenzplatten erzeugen	329
7.5.3	Verwendung von Rückgängig-Datenträgern zur Sicherung des Gastsystems	330
7.6	Klonen virtueller Maschinen und Ausbau der Testumgebung	332
7.6.1	Internes Testnetzwerk aufbauen	333
7.7	Physische Maschinen in die Pilotumgebung übernehmen	333
7.7.1	Ausblick – komplette Virtualisierung der produktiven Umgebung	334
8	Cluster mit VMs und einem iSCSI-Target als externem Speicher	335
8.1	Clusterlösungen testen oder produktiv einsetzen	336
8.1.1	Was ist ein Cluster?	336
8.1.2	Wie funktioniert ein Cluster?	337
8.1.3	Besonderheiten eines Clusters mit virtuellen Maschinen	341
8.1.4	Cluster-Konstellationen – VM mit VM oder Hardware mit VM	343
8.2	Das Konzept – stufenweiser Ausbau eines Clusters mit virtuellen Maschinen	345
8.2.1	Der Aufbau des Clusters mit VMs und die eingesetzte Software	345
8.2.2	Die einzelnen Ausbaustufen des virtuellen Clusters und das Vorgehen zur Realisierung	346
8.3	Realisierung der einzelnen Ausbaustufen des virtuellen Clusters	347
8.3.1	Stufe 1 – Installation von Windows 2003 und Klonen unabhängiger VMs	348
8.3.2	Stufe 2 – Aufbau einer Infrastruktur mit virtuellem Netzwerk und Domänencontroller	351
8.3.3	Stufe 3 – Installation des iSCSI-Targets und Einrichten des Zugriffes	354
8.3.4	Stufe 4 – Installation und Test des Clusters auf einem einzigen Host	362
8.3.5	Stufe 5 – Einrichten einer Dateifreigabe und einer IP-Adresse als Cluster-Ressource	367
8.3.6	Stufe 6 – Verteilen der virtuellen Maschinen auf verschiedene Hosts und weitere Möglichkeiten	369

8.4	Besonderheiten und Ergänzungen zum Thema Cluster und VMs	372
8.4.1	Cluster mit einer gemeinsamen virtuellen SCSI-Festplatte anstelle von externem Speicher	372
8.4.2	Host-Cluster – komplette VMs als Ressourcen von Host zu Host verschieben	374
8.5	Praxistauglichkeit der vorgestellten Lösung mit iSCSI Software Initiator	376
8.6	Fazit – konsequenter Einsatz von Virtualisierung auf allen Ebenen	376
9	VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2	377
9.1	Begriffe und Funktionen der VMware Infrastructure 3	378
9.1.1	Die Komponenten von Virtual Infrastructure 3 im Überblick	378
9.1.2	Der ESX Server 3 als Basis für die virtuellen Maschinen	380
9.1.3	Das clusterfähige Dateisystem VMFS 3 als Ablage für die virtuellen Maschinen	381
9.1.4	Festplattenspeicher ohne VMFS verwenden	383
9.1.5	Der Virtual Infrastructure Client zur Bedienung aller Komponenten über das LAN	384
9.1.6	VMware Virtual Center 2 zur zentralen Verwaltung von Hosts, Gästen und Ressourcen	386
9.1.7	VMotion verschiebt laufende VMs zwischen unterschiedlichen Hosts	387
9.1.8	VMware DRS zur Verteilung von Gästen zwischen den Hosts mittels Load Balancing	387
9.1.9	VMware HA als Hochverfügbarkeitslösung für virtuelle Maschinen	388
9.1.10	VMware Consolidated Backup als zentrale Datensicherung für die Gastsysteme	389
9.1.11	Weitere besondere Eigenschaften des ESX Servers 3	392
9.2	Editionen von ESX Server 3 – Starter, Standard und Enterprise	394
9.3	Den ersten ESX Server installieren und einrichten	396
9.3.1	Voraussetzungen zur Installation	397
9.3.2	Evaluierungssoftware und Lizenzen bei VMware anfordern	400
9.3.3	Installation des ESX Servers	401
9.3.4	Den Virtual Infrastructure Client installieren	404
9.3.5	Lizenzierung von ESX Server 3	405
9.3.6	Anlegen des VMFS-Dateisystems auf einem externen oder lokalen Datenträger	407
9.3.7	Die erste virtuelle Maschine erstellen und einen Resource Pool anlegen	414
9.3.8	Eine virtuelle Maschine von VMware Server oder Workstation auf den ESX Server übernehmen	416
9.3.9	Konfiguration des Netzwerks auf dem ESX Server 3	419

9.4	Einige Tipps zum Umgang mit dem ESX Server 3	425
9.4.1	Benutzer für die tägliche Verwaltung und Probleme mit eingeschränkten Rechten	425
9.4.2	Zugriff auf das Dateisystem des ESX Servers von einem Client aus zum Kopieren und Verwalten	427
9.4.3	Fernbedienung der Service Console von einem Client aus	428
9.4.4	SMB-Freigaben eines Windows Servers am ESX Server mounten	428
9.4.5	Verbindung zur Service Console verloren?	430
9.4.6	An der Kommandozeile einen Snapshot für ein Hot-Backup setzen	430
9.5	Installation von Virtual Center 2 mit Einbinden der ESX Hosts und der VMs	431
9.5.1	Installation des Virtual Center Management Servers	432
9.5.2	Erste Schritte im Virtual Center 2	434
9.6	Ausblick	435

Teil 3 Konzepte und Technik im Detail 437

1	Virtuelle Netzwerke – Schnellstart	439
1.1	Die emulierten Netzwerkkarten in virtuellen Maschinen	439
1.2	Produktübergreifende Anschlussarten der virtuellen Adapter	440
1.2.1	Extern (Bridged) – direkt verbunden mit einer physischen Netzwerkkarte	441
1.2.2	Intern (Custom) – abgeschottete Netze für virtuelle Maschinen	441
1.2.3	Host-only – direkte Verbindung einer VM mit dem Host	442
1.2.4	NAT – ins LAN unter der Identität des Host-PC	442
1.2.5	Anschlussart der virtuellen Netzwerkkarten im laufenden Betrieb ändern	443
1.2.6	DHCP-Server in den virtuellen Netzwerken	443
1.3	Die Konfiguration virtueller Netzwerkkarten unter VMware	444
1.3.1	Ausblick auf die erweiterte Netzwerkkonfiguration unter VMware	446
1.4	Die Konfiguration virtueller Adapter unter Microsoft Virtual Server und Virtual PC	447
1.4.1	Kommunikation mit dem Host (Host-only) über den Microsoft Loopbackadapter	449
1.5	Anwendungsbeispiele für den Einsatz aller Anschlusstypen der Produkte	450
1.5.1	Einsatzbeispiele für extern angeschlossene Adapter (Bridged/externes Netzwerk)	450
1.5.2	Einsatzbeispiele für intern angeschlossene Adapter (Custom/lokal/internes Netzwerk)	451
1.5.3	Einsatzbeispiele für Host-only/Microsoft Loopbackadapter	451
1.5.4	Einsatzbeispiele für NAT-Adapter	452

1.6	Die Netzwerkkonfiguration und die IP-Adressen in den Gastsystemen	453
1.6.1	Automatische IP-Konfiguration in den Gästen mittels DHCP	453
1.6.2	Manuelle IP-Konfiguration in den Gästen	455
1.6.3	Anpassung der Gast-IP nach einem Wechsel des Anschlusstyps im laufenden Betrieb	455
1.7	Ausblick und Erweiterungen zur Netzwerkkonfiguration	456
2	Virtuelle Netzwerke – die ganze Wahrheit	457
2.1	Allgemeine Netzwerkgrundlagen als Vorbereitung	457
2.1.1	Einige grundlegende Komponenten eines Netzwerks	457
2.1.2	Kurze Einführung zum Aufbau einer IP-Adresse	458
2.1.3	Das Zusammenspiel der Komponenten eines Netzwerks	459
2.1.4	Die Komponenten virtueller Netzwerke	461
2.1.5	Spezielles zu den virtuellen Netzwerken der unterschiedlichen Produkte	464
2.2	Virtuelle Netzwerke unter VMware	465
2.2.1	Unterschiede in der Netzwerkkonfiguration von VMware Workstation, Server und ESX	465
2.2.2	Virtuelle Netzwerkkarten unter VMware	465
2.2.3	Die virtuellen Switches VMnet0 – VMnet9 unter VMware	470
2.2.4	VMware Bridge Protocol – die Brücke in die reale Welt	474
2.2.5	Dienste DHCP und NAT in den virtuellen Netzen von VMware	475
2.2.6	Simulierte schlechte Leitungsqualität virtueller Netzwerke von VMware Workstation mit Teams	480
2.2.7	Konfiguration der virtuellen Netzwerke auf einem Linux-Host mit VMware	481
2.3	Die Netzwerkkonfiguration unter MS Virtual Server 2005 R2	484
2.3.1	Virtuelle Netzwerkkarten unter Virtual Server	484
2.3.2	Virtuelle Netzwerke unter Microsoft Virtual Server	486
2.3.3	Virtual Machine Network Services – die Verbindung zur Außenwelt	489
2.3.4	Die Dienste DHCP und NAT in den virtuellen Netzwerken	490
2.3.5	Virtuelle Adapter auf dem Host – der Microsoft Loopbackadapter	491
2.4	Zusammenfassung zum Netzwerk für alle Produkte auf einen Blick	494
2.5	Kleines Experiment – die Welten von VMware und Microsoft verbinden	495
2.6	Virtuelle Umgebungen als eigene Netzwerksegmente ans LAN anbinden	497
2.6.1	Routing über eine VM oder über den Host	498
2.6.2	NAT mittels Internet-Verbindungsfreigabe direkt auf dem Host einrichten	499
2.7	Performance beim Netzwerkzugriff der Gäste optimieren	501
2.7.1	Performance virtueller Maschinen im 100-Mbit-Netzwerk	501
2.7.2	Performance im Gigabit-Netzwerk mit virtuellen Adaptern	501

2.8	Eindeutige MAC-Adressen der virtuellen Adapter	506
2.8.1	MAC-Adressen beim Klonen und Kopieren von VMs automatisch anpassen	506
2.8.2	MAC-Adresse in den Gästen manuell festlegen	507
2.8.3	MAC-Adressen virtueller Adapter unter VMware und die UUID	507
2.8.4	MAC-Adressen virtueller Adapter unter Microsoft Virtual PC/Server	511
2.9	Geister-Netzwerkkarten bei Änderung der virtuellen Hardware in einem Gast	512
3	Die virtuellen Platten als Herzstück der Gastsysteme	513
3.1	Virtuelle Platten aus der Gast-Perspektive oder aus der Host-Perspektive	513
3.1.1	So sieht der Host eine virtuelle Platte	513
3.1.2	So sieht der Gast eine virtuelle Platte	514
3.2	Arten virtueller Platten und deren grundsätzlicher Aufbau	515
3.2.1	Köpfe, Spuren, CHS-Geometrie und LBA-Adressierung physischer und virtueller Platten	515
3.2.2	Virtuelle Zuwachsplatten verwenden oder den gesamten Platz der virtuellen Platte vorreservieren	517
3.2.3	Monolithische Platten als große Dateien am Stück oder aufgeteilte Platten in 2-GB-Segmenten	521
3.2.4	Empfehlungen für die Verwendung der virtuellen Plattentypen	523
3.3	Schreibzugriffe direkt ausführen oder in Redo-Logs bzw. Differenzplatten puffern	524
3.3.1	Redo-Logs unter VMware einschalten	525
3.3.2	Rückgängig-Datenträger und Differenzplatten unter Microsoft aktivieren	525
3.3.3	Wie funktionieren Redo-Logs und Differenzplatten konkret?	526
3.4	Die Dateien und Konfigurationseinträge der virtuellen Platten einer VM	527
3.4.1	Dateien virtueller Platten unter VMware	527
3.4.2	Die Parameter der virtuellen Platten in der Konfigurationsdatei (*.vmx) unter VMware	530
3.4.3	Dateien und Konfiguration der virtuellen Platten unter Microsoft	533
3.5	Physische Datenträger in einem Gast direkt verwenden – Raw Device Mapping	534
3.5.1	Physische Platten unter VMware einbinden	534
3.5.2	SCSI-Geräte, wie Streamer, in einem VMware-Gast verwenden	534
3.5.3	Physische Platten unter Microsoft einbinden	535
3.5.4	Gefahren bei der Verwendung physischer Platten in einer VM	536
3.5.5	Dual-Boot-Konfigurationen lassen Systeme wahlweise auf der Hardware oder in einer VM laufen	536
3.6	Fragmentierte Dateien auf dem Host sowie im Gast und die Auswirkungen	538

3.7	Virtuelle SCSI-Controller und die passenden Treiber in den Gästen	539
3.7.1	SCSI-Controllertypen und die passenden Treiber in den Gästen unter VMware	540
3.7.2	Der virtuelle SCSI-Controller unter Microsoft	544
3.8	Tools und Tricks für die Arbeit mit virtuellen Platten	545
3.8.1	Einbinden virtueller Platten am Host mit VMware DiskMount	545
3.8.2	Erstellen und Verändern virtueller Platten mit VMware vDisk Manager	546
3.8.3	Grafische Oberflächen für die Kommandozeilentools von VMware	547
3.8.4	Direktes Mounten virtueller Platten von Microsoft	547
3.8.5	Verdichten virtueller Zuwachsplatten unter VMware und Microsoft	547
3.8.6	Vergrößern virtueller Platten	549
3.8.7	Umwandeln einer virtuellen IDE-Platte in eine SCSI-Platte unter VMware	550
4	Die Snapshot- und Clone-Funktion der VMware-Produkte	553
4.1	Was ist ein Snapshot, und wozu brauchen Sie das?	553
4.2	Besonderheiten der Snapshots unter VMware	554
4.2.1	Snapshots im laufenden Betrieb sichern auch den Laufzeitzustand einer VM	554
4.2.2	Multiple Snapshots von VMware Workstation und ESX Server 3 sichern mehrere Zustände eines Gastsystems	554
4.3	So funktionieren Snapshots unter allen VMware-Produkten	555
4.3.1	Die Funktionen Snapshot und Revert zum Sichern und Verwerfen von Zuständen eines Gastes	555
4.3.2	Was passiert beim Setzen eines Snapshots?	556
4.3.3	Die Revert-Funktion zur Rückkehr zu einem gesicherten Zustand	558
4.3.4	Den nächsten Snapshot im Gast setzen	559
4.3.5	Beispiele für die Verwendung von Snapshots	561
4.4	Multiple Snapshots von VMware Workstation und ESX Server 3	561
4.4.1	Der Nutzen mehrerer Snapshots an einigen Beispielen	562
4.4.2	Ein praktischer Workshop zum Umgang mit multiplen Snapshots	563
4.5	Tipps zur Arbeit mit Snapshots und einige wichtige Grundsätze	575
4.5.1	Allgemeine Hinweise zum Umgang mit den Snapshots zu allen VMware-Produkten	575
4.5.2	Zusammenfassende Hinweise zur Verwendung von multiplen Snapshots	576
4.5.3	Virtuelle Platten im Modus independent persistent oder nonpersistent	576
4.5.4	Einstellungen zu den Snapshots in jeder VM und global am Host	577
4.5.5	Verwendung von Snapshots in produktiven Umgebungen	578
4.6	Linked Clones und Full Clones unter VMware Workstation	578
4.6.1	Templates als geschützte Vorlagen für neue VMs	579

4.7	Multiple Snapshots und linked Clones unter VMware Server und VMware Player	580
4.7.1	Mehrere Redo-Logs erzeugen mittels Schreibschutz der zugrunde liegenden virtuellen Platte	580
4.7.2	VMSnap – das Tool von vmaschinen.de zur Verwaltung mehrerer Snapshots	583
4.7.3	Linked Clones unter VMware Server – mehrere VMs auf einer Basisinstallation betreiben	584
4.7.4	Erstellen einer eigenständigen VM ohne Snapshots aus einem der Redo-Logs	585
4.7.5	Entfernen des Snapshot-Status beim VMware Server	585
4.8	Snapshots per Skript mit vmrun.exe erstellen	586
5	Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs	587
5.1	Allgemeine Betrachtungen zur Datensicherung und Wiederherstellung	587
5.2	Datensicherung und Wiederherstellung von virtuellen Maschinen	588
5.2.1	Herkömmliche Datensicherung über das LAN mit Agenten in den Gästen	588
5.2.2	Datensicherung mit den speziellen Vorteilen virtueller Maschinen	589
5.2.3	Konzepte zur Sicherung virtueller Maschinen – Hot, Cold oder Agenten?	594
5.2.4	Beispiele zur Sicherung und Wiederherstellung unter VMware Server	596
5.2.5	Archivierung von Testsystemen oder Legacy-VMs als Teilaspekt der Datensicherung	602
5.2.6	Sicherung des Host-Systems	602
5.3	Verfügbarkeit virtueller Maschinen und der Host-Systeme	603
5.3.1	Allgemeine Betrachtungen zur Ausfallsicherheit	603
5.3.2	Redundanz – der Weg zum störungsfreien Betrieb	604
5.4	Rechteverwaltung auf dem Host	608
5.4.1	Eine Verzeichnisstruktur auf dem Host mit Berechtigungen versehen	608
5.4.2	Notwendige Rechte auf die Konfigurationsdatei unter VMware	609
5.4.3	Notwendige Rechte auf die Konfigurationsdatei unter Virtual Server 2003 R2610	
6	P2V – physische Rechner in virtuelle Maschinen übernehmen	611
6.1	Einleitung	611
6.1.1	Gründe für eine Virtualisierung	612
6.1.2	Cloning oder Neuinstallation einer VM?	612
6.1.3	Grundsätzliche Vorgehensweise einer 1:1-Virtualisierung	613
6.2	Vorüberlegungen zur Virtualisierung	614
6.2.1	Problematische Hardware in der virtuellen Maschine	614
6.2.2	Problematische Software in der virtuellen Maschine	616
6.2.3	Pilotmigration auf eine Testmaschine – unbedingt empfohlen!	616
6.2.4	Sicherheit während der Migration und die Möglichkeit zur Umkehr	616

6.3	Quellsystem auf den Umzug vorbereiten	617
6.3.1	Allgemeine Vorbereitungen des Quellsystems vor der Übertragung	618
6.3.2	Treiber für den virtuellen Festplattencontroller in der Quelle vorinstallieren	619
6.4	Image des Quellsystems erstellen und in eine VM klonen	621
6.4.1	Hilfs-VM zur Übertragung des Images und zur Problembehebung einrichten	621
6.4.2	Alternative Methoden zum Übertragen des Images in die VM	623
6.4.3	Schritt 1 der Übertragung – Image erstellen	625
6.4.4	Schritt 2 – Image auf die virtuelle Zielplatte zurückspielen	626
6.5	Vorbereiten des ersten Startvorganges der VM und Beheben von Boot-Fehlern	626
6.5.1	Keine aktive Partition auf der Zielplatte festgelegt	627
6.5.2	Fehlender MBR auf der virtuellen Platte	628
6.5.3	Ziel-VM bootet nicht durch eine falsche CHS-Geometrie	628
6.5.4	Boot.ini anpassen	629
6.5.5	Alte Treiber verursachen einen BlueScreen	629
6.5.6	Startprotokollierung und abgesicherter Modus zur Fehlersuche	630
6.5.7	Die Quelle ist ein Multiprozessorsystem	631
6.5.8	Probleme bei der Verwendung von Systemplatten größer als 8 GB	633
6.5.9	Keine Anmeldung am geklonten DC möglich durch verschobene Active Directory-Dateien	634
6.5.10	Registry des Zielsystems nachträglich ändern	634
6.5.11	Reparaturinstallation als letzter Notnagel	636
6.6	Nacharbeiten an der lauffähigen VM	637
6.6.1	Tools und Additions im Zielsystem installieren	637
6.6.2	Alte Treiber im Zielsystem entfernen	637
6.6.3	Netzwerkkarten in der Ziel-VM konfigurieren	637
6.6.4	Festplatten anlegen und Daten zurückspielen	638
6.7	V2P – Gast wieder zurück auf physische Hardware verschieben	639
6.8	Produkte und Tools zur automatisierten Virtualisierung	640
6.8.1	Kostenpflichtige P2V-Produkte	640
6.8.2	Kostenlose P2V-Tools	642
7	Nützliche Zusatzprodukte, Tools, Links und Tipps	645
7.1	Tools und Hilfsprogramme für die Arbeit mit virtuellen Maschinen	645
7.1.1	Klonen von Mustervorlagen mit NewSID oder Sysprep	645
7.1.2	Vorlagen und Templates (Master-Images) erstellen	647
7.1.3	Platz sparen beim Archivieren oder Weitergeben von VMs	648
7.1.4	Invirtus Virtual Machine Optimizer spart Platz in virtuellen Maschinen	649
7.1.5	TweakUI aus den Microsoft PowerToys	649
7.1.6	CD-Tools – ISO Images erstellen und mounten	650
7.1.7	Virtuelle Festplatten erstellen, verwalten und mounten	651
7.1.8	Sonstige Tools – Editoren, Fernsteuerung, kleine Helferlein	651
7.1.9	Imaging Tools und Notfall-CDs BartPE bzw. Knoppix	652

7.2	Scripting zur Fernsteuerung von VMs oder zur Automatisierung	653
7.2.1	Skripte für Microsoft Virtual Server	653
7.2.2	Skripte für VMware Server oder Workstation	654
7.2.3	psexec.exe – Tool zum Starten von Skripten in Windows-Gästen	656
7.2.4	DevCon – Windows-Geräte manager per Kommandozeile	656
7.2.5	AutoIT – kostenloses mächtiges Scripting Tool für alle Belange	656
7.3	Fremdherstellerprodukte zur Verwaltung virtueller Maschinen	657
7.3.1	Komfortable Oberfläche VSPlus für Microsoft Virtual Server	657
7.3.2	Dunes VS-O und VD-O – Workflow und Automatisierung (VMware und Microsoft)	657
7.3.3	Platespin PowerRecon – Überwachung und Inventarisierung zur P2V Vorbereitung	658
7.3.4	Vizioncore esxMigrator, esxRanger, esxReplicator, esxCharter für ESX Server	658
7.3.5	Datensicherung ESX Server	659
7.4	Links zu Downloads, weiteren Informationen und aktuellen Meldungen	659
7.4.1	Seiten mit Informationen zu VMware und Microsoft	659
7.4.2	Links VMware – alle Produkte	660
7.4.3	Links VMware – Schwerpunkt ESX Server	660
7.4.4	Links Microsoft Virtual PC	661
7.4.5	Links Microsoft Virtual Server	661
8	Aktualisierungen, Ergänzungen und Neuerungen zum Buch	663
8.1	VMware Virtual Lab Manager für virtuelle Test- und Schulungsumgebungen	663
8.1.1	Funktion und Komponenten des VMware Virtual Lab Manager	663
8.1.2	Arbeiten mit dem Lab Manager	665
8.1.3	Netzwerkisolation und weitere Besonderheiten	666
8.1.4	Alternativen zum VMware Lab Manager	667
8.2	VMware Workstation 6 – Neuerungen und Unterschiede zur Version 5.5	667
8.2.1	Wichtige Neuerungen von VMware Workstation 6 im Detail	668
8.2.2	Weitere Neuerungen und zukünftige Entwicklungen der Workstation 6	675
8.3	VMware Fusion für Apple Macintosh auf Intel-PC bringt VMs auf den Mac	677
8.3.1	Die Alternative Parallels Desktop for Mac	677
8.4	Microsoft Virtual PC 2007 – Neuerungen und Unterschiede	677
8.5	Windows Vista als Host und in VMs	680
8.5.1	Aero Glass auch in virtuellen Maschinen über den Umweg RDP	680
8.5.2	Lizenzierung von Windows Vista Enterprise in VMs	680
8.6	VMware Converter 3.0 – physische Maschinen und VMs konvertieren	681
	Stichwortverzeichnis	683

Einleitung

Eine Technologie revolutioniert die IT-Branche – Virtualisierung!

Virtuelle Maschinen erobern mehr und mehr die Server in Rechenzentren und die Testplätze von Entwicklern, Trainern, Admins oder Consultants. Sogar ambitionierte Privatpersonen können mit Programmen, wie dem kostenlosen VMware Player, in das Thema einsteigen und problemlos einen virtuellen Zweitrechner für Testzwecke betreiben.

Das Thema *Virtualisierung* umfasst eigentlich viele Bereiche – von Speichervirtualisierung im SAN bis zur Applikationsvirtualisierung mit Citrix Presentation Server, um nur zwei Beispiele zu nennen. Wer derzeit von Virtualisierung spricht, meint aber häufig die Produkte von VMware, Microsoft Virtual Server/PC, das OpenSource-Projekt XEN oder ähnliche Software, die auf einer einzigen Hardware mehrere Computer nachbildet, um darin jeweils unabhängige Betriebssysteme laufen zu lassen. Die Konzepte zur praktischen Anwendung und das Wissen zur Bedienung dieser virtuellen Maschinen unter VMware und Microsoft vermittelt Ihnen dieses Buch.

**VMware und
Microsoft**

Mich haben die Virtualisierungslösungen von VMware und Microsoft sofort begeistert. Zusammen mit meinen Kollegen eines Systemhauses erlebte ich eine regelrechte Offenbarung, als wir vor einigen Jahren unsere erste virtuelle Testumgebung auf einem einzigen Rechner unter VMware Workstation aufbauten, um damals die Migration einer NT4-Domäne nach Windows 2000 durchzuspielen. Der nervige Aufbau einer Testumgebung aus mehreren Rechnern, vielen Kabeln und Umschaltern war endlich Geschichte! Heute gehören virtuelle Maschinen für mich zum täglichen Handwerkszeug. Von Novell Netware über Linux bis zu Windows, von Microsoft Exchange bis zu Terminalserverfarmen – die unterschiedlichsten Szenarien werden vor dem Kundeneinsatz bereits virtuell getestet. Auch gestandene Produktionsserver tummeln sich mittlerweile sehr häufig als Gäste unter VMware oder Microsoft Virtual Server. Die Vorteile der neuen Technik sind z.B. Hardware-Unabhängigkeit beim Übertragen von Systemen auf andere Rechner, Kosten- und Platzersparnis, bessere Ressourcenauslastung im Produktivbetrieb, vereinfachte Disaster Recovery und nicht zuletzt sehr komfortable Testumgebungen.

**Testumgebung
oder Produktiv-
betrieb**

Virtuelle Maschinen in der Praxis

Viele Skeptiker musste ich erst vom Sinn und vom Nutzen virtueller Computer überzeugen, die meisten sind heute begeisterte Befürworter. Also lag der Gedanke nahe, diese Begeisterung weiterzugeben und einem breiten Publikum die fantastischen Möglichkeiten der Technologie nahe zu bringen – und zwar möglichst praxisbezogen.

Dieses Buch soll Unentschlossene überzeugen, Überzeugten den Einstieg erleichtern und den bereits Eingestiegenen alle fantastischen Möglichkeiten aufzeigen, die virtuelle Maschinen in der Praxis bieten.

Was sind virtuelle Maschinen?

Kennen Sie den Science-Fiction-Streifen *The Matrix*? Neo, der Held des Films, ist überzeugt davon, im realen New York der Jahrtausendwende zu leben. Irgendwann muss er aber schockiert feststellen, dass alles um ihn herum nur Schall und Rauch ist – eine virtuelle Welt, erzeugt von einem Computerprogramm in einem Superrechner.

Matrix für Betriebssysteme

Könnte ein Betriebssystem denken, so würde es vielleicht früher oder später auch einmal die Frage stellen, ob die Hardware wirklich existiert, auf der es läuft. Und tatsächlich hätten heutige Programme allen Grund, misstrauisch zu sein. Die zeitgemäße Matrix für Betriebssysteme und Anwendungen wird von Anbietern wie VMware und Microsoft geliefert. Sie nennt sich *virtuelle Maschine*, kurz *VM*.

Wie ein vollwertiger PC

Eine VM ist ein nachgebildeter Rechner, der in einer abgeschotteten Umgebung auf einer realen Maschine läuft. Jede VM verhält sich dabei wie ein vollwertiger Computer mit eigenen Komponenten, wie CPU, RAM, VGA-Adapter, Netzwerkkarten und Festplatten. Auf einige physikalisch vorhandene Bauteile, etwa die CPU oder den RAM, darf die VM kontrolliert zugreifen. Andere Geräte, z.B. Netzwerkkarten, können sogar komplett emuliert werden, ohne dass echte Hardware existiert. In einer VM lassen sich normale Betriebssysteme installieren, wobei die Software meint, sie würde auf einem richtigen PC laufen. Alle Anforderungen des Gastsystems, wie das Schreiben auf eine Festplatte oder die Kommunikation mit dem Netzwerk, werden vom Virtualisierungsprogramm unbemerkt abgefangen und auf die echte oder auf emulierte Hardware umgesetzt.

Wirt und Gäste

Eine virtuelle Maschine wird häufig als Gast bezeichnet. Den realen Rechner, auf dem die VMs ausgeführt werden, nennt man Wirt oder auch Host. Mehrere Gäste können gleichzeitig und völlig unabhängig auf ein und demselben Host gestartet werden, ohne sich gegenseitig zu beeinflussen. So läuft ein Linux-System parallel zum gewohnten Windows XP auf dem Desktop, und ein Techniker hat jederzeit zusätzliche Rechner für Probelaufe zur Verfügung. Der überquellende Serverschrank reduziert sich auf wenige leistungsfähige Maschinen, wobei der betagte NT4-Domänencontroller problemlos neben einem

aktuellen Windows 2003- oder Netware-Server zeitgleich auf derselben Hardware läuft. Weder ein Anwender noch ein Programm bemerken dabei einen Unterschied zu physischen Rechnern.

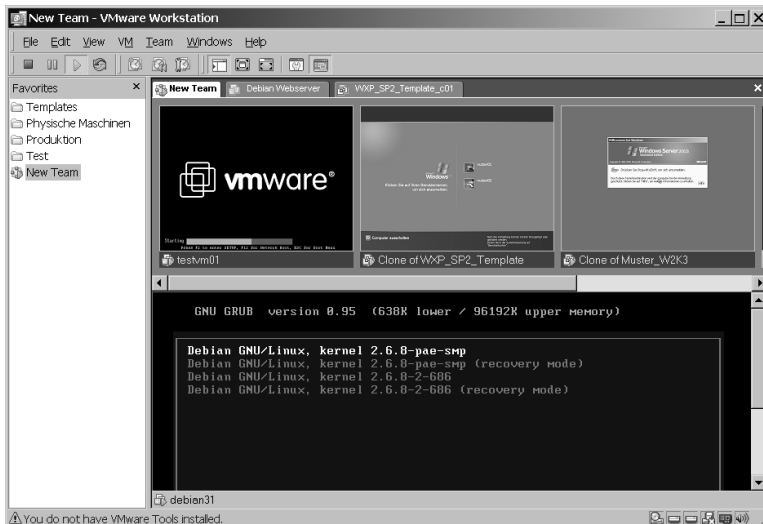


Abbildung 1:
Mehrere Betriebssysteme laufen unbeeindruckt parallel auf einem einzigen realen Rechner.

Ein bisschen grenzt es schon an Zauberei, wenn man das erste Mal ein voll funktionsfähiges Linux innerhalb seiner kleinen virtuellen Matrix auf dem Windows-Desktop laufen sieht. Lassen Sie sich auch verzaubern von den vielen neuen Möglichkeiten, ob im Serverraum oder am Testplatz!

Nützen Ihnen virtuelle Maschinen?

Erkennen Sie sich in folgenden Szenarien wieder, dann wird der Einsatz virtueller Maschinen Ihnen einen Nutzen bringen:

- ▶ **Als Techniker oder Consultant** müssen Sie komplexe Testumgebungen aufbauen? Mit mehreren Rechnern – Clients wie Servern –, die oft sogar untereinander zu vernetzen sind?
- ▶ **Als leitender Mitarbeiter** sind Sie dafür verantwortlich, die IT-Kosten im Rahmen zu halten? Sie ärgern sich über jeden neu angeschafften Server-Boliden, der dann wieder völlig unterfordert, strom- und platzfressend im 19-Zoll-Schrank hängt?
- ▶ **Im Support, im Helpdesk oder auch als Trainer** benötigen Sie ständig andere PCs mit unterschiedlichen Betriebssystemen und Konfigurationen? Diese Rechner müssen jederzeit bereitstehen und auf Abruf sofort laufen?
- ▶ **Als Administrator** wünschen Sie sich schon lange eine Pilotumgebung, in der Sie völlig entspannt neue Service-Packs, Patches und Migrationen ausprobieren können?

Brauchen Sie das?

- ▶ **Als Programmierer oder Webdesigner** würden Sie gerne eine lauffähige Entwicklungsumgebung aus Web- oder Datenbankserver inkl. passender Clients ständig mit dabei haben? Diese Rechner möchten Sie zusätzlich als Demo-Umgebung unkompliziert an Ihre Kunden weitergeben?
- ▶ **Sie sind ein ambitionierter Laie**, der schnell einmal ein neues Betriebssystem, etwa Linux, ausprobieren möchte, ohne gleich einen neuen Rechner zu kaufen oder das bestehende System durch parallele Installationen zu gefährden?

Mindestens eine dieser Fragen haben Sie mit „Ja“ beantwortet? Dann sollten Sie unbedingt weiterlesen. Ich zeige Ihnen, wie virtuelle Maschinen Ihren Arbeitsalltag erleichtern werden und wie Virtualisierung hilft, Kosten und Zeit zu sparen.

Welche Vorteile haben virtuelle Maschinen?

Vorteile für jede Anwendergruppe

Ich behaupte einfach, virtuelle Maschinen nützen jedem, der mit IT zu tun hat. Hier finden Sie kurz und knapp die wichtigsten Vorteile:

Größere Flexibilität gegenüber echter Hardware

- ▶ *Unterschiedliche Betriebssysteme auf der gleichen Hardware* – Linux läuft neben Windows oder Netware. Durch diese Flexibilität können Sie komplexe Testumgebungen auf einem einzigen Rechner aufbauen oder alte Systeme im Serverraum auf wenige Maschinen konsolidieren.
- ▶ *Verringerung der Anzahl physischer Server* – Das führt zu Ersparnissen bei Strom, Platz und Anschaffung. Die vorhandene physikalische Hardware wird durch mehrere virtuelle Maschinen besser ausgelastet – keine Verschwendung mehr von teuren Serverressourcen!
- ▶ *Flexible Verteilung von Ressourcen* – RAM, CPU, Netzwerkkarten und Plattenplatz werden genau den virtuellen Maschinen zugewiesen, die sie wirklich brauchen, ohne Umbau physischer Komponenten. Ein skalierbarer Ausbau der Kapazitäten und die Lastverteilung sind teilweise im laufenden Betrieb möglich.
- ▶ *Einfaches Kopieren virtueller Maschinen* – Damit geben Sie fertig installierte und konfigurierte Gäste an Kunden oder Mitarbeiter auf DVD, USB-Platte oder sogar per Internet-Download weiter. Sie verteilen sie auf eine komplette Demo-Umgebung zum sofortigen Starten und Evaluieren einer Anwendung. Genauso betreiben Sie Ihre Testumgebung aus der Firma problemlos auf dem Laptop im Hotel, unterwegs im Zug oder zu Hause.

Hardware-Unabhängigkeit der Gastsysteme in den VMs

- ▶ *Einfacher Hardwarewechsel oder Klonen von Systemen* – In den VMs ist immer die gleiche virtuelle Hardware vorhanden, unabhängig davon, welche physische Hardware darunter liegt. Gastsysteme werden ohne Treiberärger einfach kopiert.
- ▶ *Sehr schnelles Bereitstellen neuer virtueller Rechner* – Durch Kopieren von fertig installierten Mustervorlagen entfällt die komplette Neuinstallation des Betriebssystems in jeder weiteren Maschine. Die Notwendigkeit zur Hardware-Beschaffung wird verringert.
- ▶ *Schnelles Abzweigen einer Test- oder Pilotumgebung* – Wenn die Systeme bereits virtualisiert sind, ist eine Kopie der aktuellen virtuellen Produktionsserver möglich, um in Sicherheit Patches oder Einstellungen zu testen. Zusätzliche Hardware und aufwändiges Klonen ist nicht mehr notwendig.

Vorteile virtueller Maschinen im täglichen Einsatz

- ▶ *Schnelle und einfache Disaster Recovery* – Durch Sichern kompletter virtueller Systemplatten mit den darin enthaltenen Betriebssystemen und Applikationen, ähnlich einem Image, erfolgt das Zurückspielen der virtuellen Systeme innerhalb von Minuten durch einfaches Kopieren.
- ▶ *Testen ohne Reue* – Wiederanlaufpunkte mittels RedoLogs, Snapshot und Revert sind eine besondere Komfortfunktion virtueller Maschinen. Damit sichern Sie Systemzustände, z.B. vor anstehenden Installationen. Änderungen lassen sich jederzeit auf Knopfdruck wieder verwerfen. Ohne langwierig Festplattenimages zurückzuspielen, steht das System in der VM sofort wieder im sauberen Zustand vor der Änderung.
- ▶ *Isolation sich beeinflussender Applikationen* – Kritische Anwendungen bekommen in Minutenschnelle einen Server für sich allein, der von einer vorhandenen Mustervorlage geklont wird.
- ▶ *Laufende Server ohne Ausfallzeit auf andere Hardware verschieben* – Bei Wartung an der Hardware bemerken angemeldete Nutzer keinerlei Unterbrechung, das kann allerdings nicht jedes Virtualisierungsprodukt. Bei Hardware-Ausfall lassen sich virtuelle Server schnell wieder auf anderen Hosts starten.

Auf alle hier genannten Vorteile werde ich in den jeweiligen Kapiteln dieses Buches detailliert eingehen.

Die Hemmschwelle: Nachteile, Stabilität, Sicherheit virtueller Maschinen

**Funktioniert
denn das?**

Viele Neueinsteiger, die ich gerne vom Einsatz virtueller Maschinen überzeugen möchte, stellen sich immer wieder die Frage: „Funktioniert denn das?“ oder „Zieht man sich nicht zusätzliche Fehlerquellen hinzu?“ – kurz und knapp sechs Antworten dazu.

Erfahrungen mit dem Einsatz virtueller Maschinen

- ▶ VMs laufen stabil.
- ▶ Virtuelle Maschinen sind vielfach praxiserprobt.
- ▶ Der leichte Performance-Verlust durch die Virtualisierung kann in den meisten Fällen vernachlässigt werden, außer bei stark ausgelasteten Servern.
- ▶ Für Testumgebungen sind VMs fast uneingeschränkt zu empfehlen. Nur spezielle Hardware kann nicht immer problemlos verwendet werden, z.B. Messplätze oder Multimedia-Anwendungen.
- ▶ In Produktionsumgebungen gibt es seltene Anwendungsfälle, wo eine Virtualisierung nicht sinnvoll oder sogar unmöglich ist. Hier ist eine gute Vorbereitung notwendig. Hauptsächlich bereiten Performancefragen oder spezielle Hardware Probleme. Ein Großteil der Server sind aber potentielle Virtualisierungskandidaten.
- ▶ VMs bieten in den meisten Anwendungsfällen grundsätzlich viel mehr Vorteile als Nachteile.

Nachteile und Grenzen virtueller Maschinen

- ▶ *Nicht jede Hardware wird in virtuellen Maschinen unterstützt* – Viele Einschränkungen lassen sich zwar umgehen, z.B. kann als Ersatz für ISDN-Karten ein so genannter LAN-CAPI verwendet werden. Manche Einschränkungen sind aber unausweichlich, z.B. erkennt ein Gastsystem keine Hardware-Dongles im PCI-Slot.
- ▶ *Bestimmte Ressourcen stehen nur begrenzt zur Verfügung* – Die meisten Virtualisierer reichen beispielsweise nur 3.6 GB RAM (ESX Server 16 GB) oder nur eine CPU (VMware bis zu 2 CPUs, ESX Server bis zu 4 CPUs) in eine VM durch.
- ▶ *Performanceprobleme* – Die Leistung der physischen Hardware kann in einer VM nicht vollständig genutzt werden. Dieser Punkt spielt allerdings nur bei sehr hochlastigen Servern eine Rolle. Aktuelle Hardware wird nur in den wenigsten Fällen von einem Betriebssystem und den Applikationen voll ausgelastet.

- ▶ *Single Point of Failure* – Fällt der Virtualisierungshost aus, dann laufen gleich mehrere virtuelle Server und Dienste nicht mehr. Durch mehrere physische Server und Ausfallkonzepte wie Clustering muss dieser Punkt in kritischen Umgebungen besonders abgesichert werden.
- ▶ *Zusätzliches Know-how erforderlich* – Zur sicheren Bedienung und Verwaltung der vorhandenen Systeme und der Applikationen kommt zusätzlich der Umgang mit der virtuellen Infrastruktur hinzu.

Weitere Grenzen virtueller Maschinen und detaillierte Hinweise zur physischen und virtuellen Hardware finden Sie in *Teil 1, Kapitel 1, „Grundlagen virtueller Maschinen und Hinweise zur Hardware“*.



Was ist das Anliegen dieses Buches, und für wen habe ich es geschrieben?

In erster Linie möchte ich Ihnen mit diesem Buch meine eigene Begeisterung für virtuelle Maschinen weitergeben, Sie mit praktischen Beispielen vom Nutzen überzeugen und Ihnen einen schnellen Start mit der Technologie ermöglichen.

Neueinsteigern helfen

Die Hemmschwelle, vor der Sie als Neuanwender noch stehen, beseitigen nachvollziehbare praktische Workshops, zu finden in *Teil 2* des Buches. Sie vermitteln alle Grundlagen, um in der virtuellen Welt erfolgreich zu sein. Wenn Sie einen schnellen Einstieg mit einem überschaubaren Pilotversuch wagen wollen oder wenn Sie für Ihre Test- oder Schulungsumgebung Lösungen zur Vereinfachung suchen, dann sind Sie hier genau richtig.

**Überschaubarer
Einstieg**

Erfahrenen Anwendern weiteres Know-how vermitteln

Erfahrene Anwender werden beim Lesen neue Anregungen finden, wie sie ihr vorhandenes Virtualisierungsprodukt noch besser ausnutzen können. Tipps, die nicht immer im Handbuch zu finden sind, und Workshops, die tägliche Anforderungen bei der Arbeit mit VMs abdecken, z.B.:

**Vertiefende
Workshops**

Linked Clones, Templates und Multiple Snapshots der VMware Workstation sowie *mehrere Snapshots* und *Clones* auch mit VMware Server.

Differenzplatten der Microsoft-Produkte, *virtuelle Netzwerke* unter VMware und Microsoft.

VMs mit dem *VMware Player* weitergeben, physische Maschinen in virtuelle Maschinen ohne *Bluescreen* übernehmen, *Cluster* zwischen VMs auf unterschiedlichen Hosts aufbauen

Praxisbezogener Sofort-Einstieg mit Workshops

Nachvollziehbare Praxis-Workshops

Auf keinen Fall ist dieses Buch einfach nur ein deutsches Produkt-handbuch. Der Schwerpunkt liegt auf HowTos und Projekten zum sofortigen Nachvollziehen. Direkt bei der praktischen Arbeit mit virtuellen Maschinen erhalten Sie das notwendige Wissen. Keine akribische Aufzählung jedes einzelnen Menüpunktes, sondern grundlegende Konzepte und wichtige Tipps.

VMware Player, Workstation und Server sowie Microsoft Virtual PC und Server

Thema dieses Buches sind die etablierten Virtualisierungsprodukte von VMware und Microsoft:

VMware-Produkte in diesem Buch

- ▶ VMware Workstation 5.5 und der VMware Player
- ▶ VMware Workstation 6 – Neuerungen und Unterschiede
- ▶ VMware Server 1.0
- ▶ VMware ESX Server 3 und Virtual Center 2 (*Virtual Infrastructure 3*) werden in einem eigenen ausführlichen Kapitel behandelt.

Microsoft-Produkte in diesem Buch

- ▶ Microsoft Virtual PC 2004 SP1
- ▶ Microsoft Virtual PC 2007 – Neuerungen und Unterschiede
- ▶ Microsoft Virtual Server 2005 R2

Der Aufbau dieses Buches in drei Teilen

Drei unabhängige Teile

Das Buch gliedert sich in drei unabhängige Teile. Jeder ist in sich abgeschlossen und kann separat verwendet werden. Schauen Sie bitte auch ins Vorwort zu jedem Teil, um genauere Informationen zu erhalten, und in das Kapitel *Verwendung dieses Buches – wie kommen Sie schnell zum Ziel?*.

Teil 1 – Einstieg: allgemeine Einführung und Grundlagen

Den Teil 1 des Buches können Sie durchaus erst später lesen, wenn Sie lieber gleich mit einem praktischen Beispiel aus Teil 2 starten wollen oder wenn Ihnen viele Grundlagen schon bekannt sind. Teil 1 klärt wichtige Begriffe und erläutert die grundlegenden Prinzipien von der Installation bis zur Bedienung. Sie erhalten einen Überblick über die verschiedenen Produkte und ihre Vor- und Nachteile.

Teil 2 – Praxis: sofort nachvollziehbare Workshops

Teil 2 ist das Rückgrat des Buches – *sofort loslegen* lautet das Motto. An praxisbezogenen konkreten Beispielen erhalten Sie die wichtigsten Grundlagen und Tipps zum Umgang mit den einzelnen Produkten. Das nötige Basiswissen wird direkt am Beispiel vermittelt. Über Verweise auf die Technik-Kapitel in Teil 3 und auf die Grundlagen in Teil 1 finden Sie tiefere Erklärung zu bestimmten Themen.

**Sofort praktisch
loslegen**

Auch ohne Verweise zu den anderen Kapiteln können Sie jeden Workshop aus Teil 2 sofort nachvollziehen und haben damit einen Schnellstart zu Ihrem Virtualisierungsprodukt ohne Vorstudium und Querlesen!



Teil 3 – Technik: Hintergründe, Tipps und Tricks

Der Technikteil geht sehr detailliert auf bestimmte Themen ein. Hier erfahren Sie alles zu virtuellen Netzwerken, lernen Tricks für den Umgang mit den virtuellen Platten und deren RedoLogs oder erfahren wichtige Konzepte zur Datensicherung oder zur Übernahme von physischen Maschinen in eine VM (P2V).

Mit welchem Teil Sie beginnen, hängt von Ihrem Vorwissen und von Ihrer bevorzugten Herangehensweise ab. Egal wie Sie sich entscheiden – ich wünsche Ihnen bereits *jetzt viel Spaß beim Lesen dieses Buches!*

Viel Spaß!

Die Icons in diesem Buch

Sie finden an verschiedenen Stellen im Text Icons, die Sie auf Besonderheiten, Tipps, Gefahren und zusätzliches Material auf der CD aufmerksam machen sollen. Im Einzelnen handelt es sich hierbei um folgende Icons:



Hier finden Sie Hintergrundinformationen zum gerade behandelten Thema und Hinweise, wie Sie Ihr Wissen noch vertiefen können.



Hier erfahren Sie, welche Fehler und Probleme auftreten können, wie Sie diese am besten beseitigen und was Sie unbedingt vermeiden sollten.



Hier erhalten Sie Tipps und Tricks, die Ihnen bei Ihrer täglichen Arbeit weiterhelfen.



Hier wird auf zusätzliches Material verwiesen, das sich auf der beiliegenden CD-ROM befindet.

Verwendung dieses Buches – wie kommen Sie schnell zum Ziel?

Hier finden Sie einen Leitfaden, wie Sie die einzelnen Teile und Kapitel des Buchs anwenden können, um schnell mit virtuellen Maschinen vertraut zu werden.



Aktualisierungen und Linkliste und auf www.vmaschinen.de

Aktuelle Ergänzungen und alle Links in den Kapiteln dieses Buches finden Sie ständig aktualisiert auf meiner Webseite <http://www.vmaschinen.de>. Sie sparen sich damit beispielsweise das Abtippen der Links in den Browser, wenn Sie zu den aufgeführten Webseiten gelangen wollen.

Wie sollten Sie als Einsteiger die Kapitel durcharbeiten?

Wenn Sie gerade mit dem Einstieg beginnen, wird Sie folgende Vorgehensweise zügig zur ersten lauffähigen VM führen. Ohne Vorstudium beginnen Sie, schnellstmöglich mit Ihrem Virtualisierungsprodukt zu arbeiten:

**Grundlagen,
wichtige Begriffe
und erste
Schritte mit den
Produkten**

1. *Teil 1, Kapitel 1* – Erfahren Sie, wie virtuelle Maschinen funktionieren, und lernen Sie wichtige Begriffe, wie Host und Gast, kennen. Erfahren Sie alles zur Hardware einer virtuellen Umgebung, von Dual-CPU's über SATA bis zum Fibre-Channel SAN.
2. *Teil 1, Kapitel 2* – Wählen Sie für sich das Produkt, mit dem Sie praktisch beginnen wollen. Haben Sie sich schon für ein Virtualisierungsprodukt entschieden, müssen Sie Teil 1, Kapitel 2 nicht unbedingt durcharbeiten.
3. *Teil 1, Kapitel 3* – Installieren Sie das ausgewählte Virtualisierungsprodukt und konfigurieren Sie die notwendigsten Einstellungen als direkte Vorbereitung auf die Praxis-Workshops.
4. *Teil 2 des Buches* – Wählen Sie einen Einsteiger-Workshop aus dem Teil 2 des Buches, und beginnen Sie sofort mit der Anwendung virtueller Maschinen (siehe „Einsteigerworkshops aus Teil 2 des Buches“).
5. *als Ergänzung: Teil 1, Kapitel 4* – Sie können das Kapitel 4 nachträglich durcharbeiten, um weitere interessante Funktionen Ihres Produktes zu entdecken. Sie können sich aber auch bereits vor dem ersten Praxis-Workshop mit der Virtualisierungssoftware theoretisch vertraut machen.

Einsteigerworkshops aus Teil 2 des Buches

Die Einsteiger-Workshops sind auf ein bestimmtes Produkt zugeschnitten und erläutern den Umgang mit VMs von der Erstellung bis zum Betrieb direkt an einem praktisch nachvollziehbaren Beispiel. Folgende Produkte finden Sie in den jeweiligen Einsteiger-Workshops:

- ▶ VMware Player – *Teil 2, Kapitel 5*
- ▶ VMware Workstation und VMware Server – *Teil 2, Kapitel 1*
- ▶ VMware ESX Server 3 – *Teil 2, Kapitel 9*
- ▶ Microsoft Virtual PC 2004 – *Teil 2, Kapitel 2*
- ▶ Microsoft Virtual Server 2003 R2 – *Teil 2, Kapitel 7*

Wie sollten Sie als erfahrener Anwender die Kapitel durcharbeiten?

Details zu Netzwerken, Snapshots oder virtuelle Platten

Als erfahrener Anwender können Sie sofort die Praxis-Workshops durcharbeiten oder sich im Teil 1 einen Überblick über die konkurrierenden Produkte holen. Zusätzlich erhalten Sie tiefergehende Informationen zu bestimmten Themen, wie Netzwerke, Snapshots oder virtuelle Platten, im Teil 3 des Buches.

- ▶ *Teil 2* – Wählen Sie einen fortgeschrittenen Praxis-Workshop, um komplexere Umgebungen mit virtuellen Maschinen aufzubauen, wie Cluster oder eine DMZ (siehe „Erweiterte Workshops aus Teil 2 des Buches“).
- ▶ *Teil 3* – Befassen Sie sich intensiver mit einem bestimmten Thema, z.B. den virtuellen Netzwerken, virtuellen Platten oder mit den Snapshots von VMware. Erfahren Sie erweiterte Konzepte, z.B. zu Datensicherung und Ausfallsicherheit.
- ▶ *Teil 1, Kapitel 4* – Um einen Überblick über interessante Funktionen Ihres Virtualisierungsproduktes zu erhalten, die Ihnen vielleicht noch unbekannt sind, können Sie zusätzlich das Kapitel 4 von Teil 1 durcharbeiten.

Erweiterte Workshops aus Teil 2 des Buches

Die erweiterten Workshops sind nicht ausschließlich auf ein Produkt zugeschnitten, sondern lassen sich mit verschiedenen Virtualisierern umsetzen. Die Kapitel setzen bereits Basiskenntnisse zu virtuellen Maschinen voraus und behandeln ein komplexeres Thema:

- ▶ Aufbau einer virtuellen DMZ – *Teil 2, Kapitel 3*
- ▶ Aufbau eines Clusters aus VMs mit iSCSI – *Teil 2, Kapitel 8*
- ▶ Kostenloses virtuelles Klassenzimmer einrichten – *Teil 2, Kapitel 6*

Danke!

Viele Menschen wirken am Entstehen eines Buches mit: Freunde und Kollegen, Lektoren und Supportmitarbeiter, nette Vertriebsbeauftragte und engagierte Consultants – all die vielen Leute, die täglich unter großem Einsatz das Rad der IT am Laufen halten und trotzdem Zeit für Antworten und Hilfestellungen finden. Ihnen allen möchte ich für die Unterstützung danken!

Ganz besondere Anerkennung gebührt aber meiner Familie – Manuela, Elena und Tabea. Nur durch Euer großes Verständnis konnte dieses Buch in endlosen Abenden und Nächten, vor allem an vielen Wochenenden, entstehen. Es wird Zeit, dass ich meiner Matrix entsteige, um ganz real wieder teilzuhaben an Ausflügen ins Bad in den Wald oder ins Kino. Dafür, dass Ihr mich nicht in meiner virtuellen Welt vergessen habt, verdient Ihr meinen allergrößten Dank – ich bin wieder da!

Teil 1

Allgemeine Einführung und Grundlagen

Sie machen gerade Ihre ersten Schritte mit virtuellen Maschinen und möchten gerne die wichtigsten Grundlagen und Begriffe kennen lernen? Sie haben sich noch nicht für ein bestimmtes Produkt entschieden und hätten gerne einen Überblick, was für Ihren Einsatzzweck die richtige Virtualisierungslösung ist? Sie wollen wissen, wie eine VM überhaupt funktioniert?

Wichtige Grundlagen

Dann sind Sie hier in Teil 1 des Buches richtig!

Was lernen Sie im ersten Teil?

Teil 1 dient als Einstieg und vermittelt Basiswissen, was später nicht in jedem einzelnen Praxis-Workshop vom zweiten Teil des Buches ausführlich besprochen werden soll. Sie erfahren, was ein Wirt, ein Host und ein Gast ist und wie die Komponenten einer VM zusammenspielen.

Begriffe und Funktionen

Weiterhin werden alle Produkte mit ihren wichtigsten Vor- und Nachteilen vorgestellt, und Sie können sich ein Bild machen, was Sie für Ihre Arbeit benötigen und welche Hardware-Voraussetzungen ein Host erfüllen sollte.

Produkte

Können Sie Teil 1 überspringen?

Sie zählen zu den Verfechtern des *Learning by Doing* und Ihr Motto lautet *Erst klicken, dann fragen*? Sie kennen sich bereits etwas mit virtuellen Maschinen aus und haben sich schon für ein Produkt entschieden?

Dann beginnen Sie in *Teil 2* mit einem für Sie interessanten Praxis-Workshop. Wenn Sie dabei merken, dass Ihnen doch einige grundlegende Begriffe fehlen, kommen Sie einfach hierher zurück.

Praxis in Teil 2

Die meisten Workshops in *Teil 2* enthalten ebenfalls die wichtigsten Grundlagen in Kurzform und können Ihnen damit als praxisnaher Schnelleinstieg ohne langes Vorstudium dienen.



1 Grundlagen virtueller Maschinen und Hinweise zur Hardware

Um sich in der virtuellen Welt zurechtzufinden, sollten Sie einige Begriffe kennen und die ungefähre Funktionsweise einer virtuellen Maschine verstehen. Was ist ein Wirt bzw. ein Gastsystem? Wozu dient der Virtualisierungslayer?

Eine weitere wichtige vorbereitende Frage ist, welche Geräte in einer VM unterstützt werden und über welche Hardware der Host verfügen sollte. Legen Sie die virtuellen Platten am besten auf lokalen Datenträgern oder in einem externen SAN ab? Benötigen Sie mehrere CPUs oder genügt bereits eine, und was ist mit dem Hauptspeicher? Auf diese Fragen finden Sie in *Kapitel 1* eine Antwort.

1.1 Wichtige Begriffe bei der Arbeit mit virtuellen Maschinen

Gleich zu Beginn muss ich zum besseren Verständnis zwei Begriffe genauer erklären, die in der Einleitung schon einige Male vorkamen und die Ihnen im gesamten Buch immer wieder begegnen werden. Was ist ein Host, und was ist ein Gast?

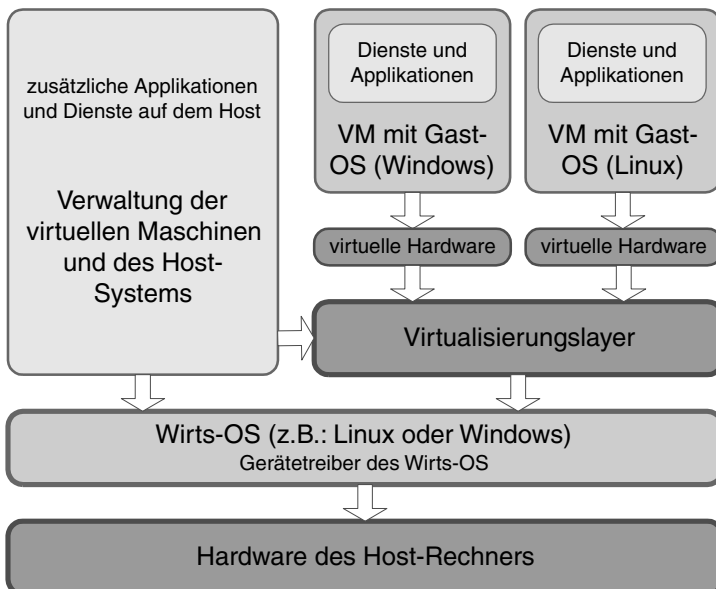


Abbildung 1.1:
Der Virtualisierungslayer stellt virtuelle Hardware bereit. Er setzt auf einem Wirts-OS auf oder spricht die Hardware direkt an

1.1.1 Was ist der Host bzw. der Wirt?

**Der Host ist
der physische
Rechner**

Der *Host*, oder auch *Wirt* genannt, ist der reale Rechner, auf dem die virtuellen Maschinen laufen. Auf dem Host kann ein Betriebssystem wie Windows oder Linux seinen Dienst tun, unter dem die Virtualisierungssoftware installiert wird. Der Host ist in diesem Falle ein PC oder ein Server mit gewohnter Arbeitsoberfläche, auf dem als Anwendung einige virtuelle Maschinen laufen. VMware Server, VMware Workstation und der Player sowie Microsoft Virtual PC/Server arbeiten nach diesem Prinzip.

Der VMware ESX Server läuft dagegen direkt auf der Hardware (*Bare Metal* – deutsch: bloßes Metall) und benötigt kein Wirtsbetriebssystem. Dazu bringt er selbst die notwendigen Treiber, ein eigenes Dateisystem, einen schlanken Kernel und eine Service-Konsole zur Verwaltung von Kernel und virtuellen Maschinen mit, er ist sozusagen selbst das Wirtssystem.

1.1.2 Was ist eine VM bzw. ein Gast?

**Der Gast ist
die virtuelle
Maschine**

Die so genannten *virtuellen Maschinen* (kurz: *VM*) laufen in einer abgekapselten Umgebung auf dem Wirtsrechner unter der Kontrolle des Virtualisierungsprogramms, wie z.B. VMware Workstation oder Microsoft Virtual PC. Eine virtuelle Maschine bezeichnet man auch als *Gast*. Das Gastsystem, also das Betriebssystem innerhalb der virtuellen Maschine, meint, auf einem realen Rechner zu laufen, es bemerkt keinen Unterschied zu einem echten Computer. Jede VM verfügt über eine Ausstattung mit virtualisierter Hardware, etwa VGA, Festplatten, RAM und CPU.

1.1.3 Was macht der Virtualisierungslayer?

Die Software-Schicht, die sich zwischen das Gastbetriebssystem und die reale Hardware schiebt, wird als *Virtualisierungslayer* bzw. als *Hypervisor* oder *Virtual Machine Monitor* bezeichnet. Dieser Virtualisierungslayer emuliert für die Gäste die virtuelle Hardware, teilt ihnen CPU-Zeit zu oder ermöglicht den kontrollierten Zugriff auf bestimmte physische Geräte des Wirts.

Bei Produkten, wie VMware Server, VMware Workstation oder Microsoft Virtual Server/PC, läuft der Virtualisierungslayer auf dem Wirtsbetriebssystem. Erst dieses Wirtsbetriebssystem steuert mit seinen Treibern die eingebauten physischen Geräte an (Abbildung 1.1). Beim VMware ESX Server greift der Virtualisierungslayer dagegen mit eigenen Treibern direkt auf die physische Hardware zu, die zusätzliche Schicht des Wirtssystems entfällt.

Dem Gast macht es nichts aus, ob ein Betriebssystem dazwischen liegt oder ob die Virtualisierungssoftware ohne Umwege mit der physischen Maschine spricht. Das Betriebssystem in der VM sieht immer nur die Geräte, die vom Virtualisierungslayer bereitgestellt werden.

Virtuelle Hardware bereitstellen

Der Virtualisierungslayer bestimmt, über welche Hardware ein Gast verfügt. Diese virtuelle Hardware ist innerhalb der Produkte des jeweiligen Herstellers (VMware bzw. Microsoft) immer vom gleichen Typ, unabhängig davon, welche physische Hardware eingebaut ist.



1.2 So funktioniert eine virtuelle Maschine

Ein gewisses Grundverständnis der internen Funktion virtueller Maschinen ist für den Umgang mit den Gästen nützlich, obwohl Sie die Virtualisierungsprodukte auch ohne dieses Wissen verwenden können.

1.2.1 Die wichtigsten Eigenschaften einer VM

Hier finden Sie auf einen Blick die wichtigsten Eigenschaften, die eine VM charakterisieren.

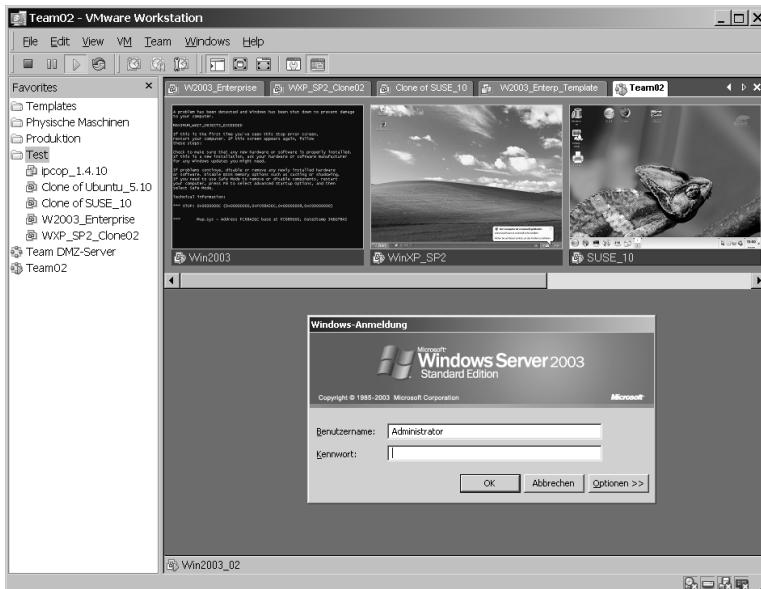


Abbildung 1.2: Unterschiedliche Betriebssysteme auf einem Rechner, und selbst ein Bluescreen bleibt isoliert innerhalb der virtuellen Maschine

- ▶ *Eine VM wirkt wie ein vollwertiger Computer.* Weder das Gastbetriebssystem, noch Anwendungen oder Benutzer merken einen Unterschied zu einem echten Rechner. Auch im LAN kann eine VM wie ein vollwertiger PC mit eigener IP- und MAC-Adresse auftreten.
- ▶ *Ein Gast ist komplett abgeschottet.* Das Gastsystem in einer VM kann auf andere Gäste oder auf den Wirt nur so zugreifen, wie das auch zwischen separaten Rechnern der Fall wäre, z.B. über das Netzwerk. Ansonsten sind die Systeme voneinander isoliert. Selbst ein Bluescreen in einer VM lässt den Host und andere Gäste unbeeinträchtigt weiterlaufen (Abbildung 1.2 – am gezeigten Bluescreen war übrigens nicht VMware, sondern ein Treiber im Gastsystem schuld).
- ▶ *Verschiedene Betriebssysteme.* Sie können in den Gästen durch die gegenseitige Abschottung parallel und unabhängig auf der gleichen Hardware laufen. So betreiben Sie Linux neben Windows oder Netware zeitgleich auf ein und demselben Host-Rechner.
- ▶ *Für das Gastsystem existiert immer die gleiche Hardware-Ausstattung.* Egal auf welchem physischen System die VM läuft, innerhalb eines Gastes werden immer dieselben Komponenten emuliert. Bis auf CPU und RAM, auf diese Komponenten greift jeder Gast unter Kontrolle der Virtualisierungssoftware direkt zu.

1.2.2 Der Unterschied von Virtualisierung und Emulation

Vollständige Emulation der Hardware samt CPU

Oft wird im Bezug auf die Virtualisierungsprodukte von VMware oder Microsoft von Emulatoren gesprochen, was aber nicht ganz stimmt. Richtige Emulatoren sind z.B. die OpenSource-Projekte Qemu und Bochs oder auch Amiga-Emulatoren. Diese Programme bilden alle Komponenten eines Rechners, selbst die CPU, komplett mit Software nach. Unter dem Emulator Bochs würde eine Windows-VM sogar auf einem IBM-Großrechner laufen, Hauptsache, dort existiert ein C-Compiler, der den Quellcode des Emulationsprogramms übersetzen kann.

Ein richtiger Emulator ist auch die Microsoft Virtual PC-Version für den Apple Macintosh auf PowerPC-Basis. Da ein Macintosh-Rechner mit PowerPC-CPU auf einer völlig anderen Hardware-Architektur von IBM und Motorola aufsetzt, muss dort eine vollständige Intel-kompatible i386-Umgebung emuliert werden, um Betriebssysteme wie Windows ausführen zu können. Durch die vollständige Emulation der kompletten Hardware sind solche Lösungen aber sehr langsam, weil für jeden Befehl der nachgebildeten CPU mehrere Befehle des Emulationsprogramms auf der realen CPU ablaufen müssen.

Virtualisierung versucht dagegen, dem Gast so weit wie möglich den kontrollierten Zugriff auf die vorhandenen Ressourcen zu ermöglichen. So laufen z.B. alle Befehle in einer VM direkt auf der CPU des Hosts. Nur einige Ausnahmen müssen abgefangen und nachgebildet werden (siehe weiter unten bei „Kontrolle über die CPU in einer VM“). Wenn Sie einmal im Gastsystem in den Gerätemanager schauen, finden Sie dort immer die gleiche CPU wie auf dem Host vor.

Virtualisierung ermöglicht kontrollierten Zugriff

Trotzdem werden auch bei der Virtualisierung einige Komponenten vollständig emuliert. So ist es möglich, mehrere Gäste mit virtuellen Netzwerkkarten an virtuellen Switches zu vernetzen, etwa für Testumgebungen, ohne dass ein einziger realer Netzwerkadapter im Host eingebaut ist.

1.2.3 Was passiert intern in einer VM?

Ein einfaches Beispiel verdeutlicht die Zusammenhänge und Funktionsweisen in einer virtuellen Maschine.

Beispiel: Zugriff auf einen virtuellen IDE-Controller

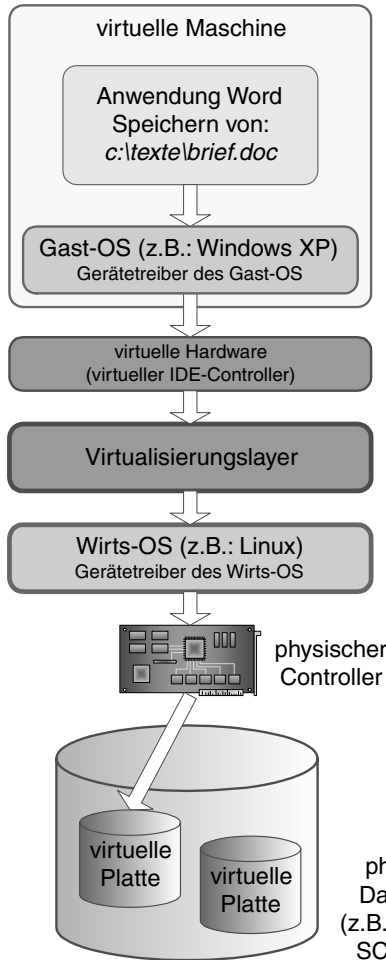
Ich muss hier zum besseren Verständnis etwas vorgreifen. Eine virtuelle Platte meist ist eine große Datei auf einem physischen Datenträger des Wirts. So eine Datei ist sozusagen der Container oder Behälter, in dem die Daten landen, die der Gast schreibt, man nennt sie auch *Image-Dateien*. Um eine Verwechslung mit Sicherungs- oder ISO-Images auszuschließen, werde ich sie im Folgenden einfach als *Behälterdatei* bezeichnen. Innerhalb der VM taucht eine Behälterdatei immer als vollwertige Festplatte auf. Der Gast merkt keinen Unterschied. Er greift, ohne es zu wissen, nur auf die Behälterdatei zu und nicht direkt auf den physischen Datenträger im Host.



Nehmen wir an, Sie haben eine virtuelle Maschine unter VMware Workstation oder Microsoft Virtual PC mit einer virtuellen IDE-Festplatte konfiguriert. Sie haben in Ihrer VM als Gastsystem Windows XP installiert und zusätzlich das Anwendungsprogramm Word. Sie haben in der VM mit Word einen Brief geschrieben und wollen ihn auf der Platte im Gast `C:\texte\brief.doc` abspeichern. Das ist ein sehr einfaches Beispiel, die VM könnte auch ein Terminalserver sein oder ein Fileserver, auf dem über das Netzwerk mehrere Anwender arbeiten.

Abspeichern einer Datei im Gastsystem

Abbildung 1.3:
Der Zugriff von
einer virtuellen
Maschine auf die
Hardware am Bei-
spiel des Abspei-
cherns eines
Dokuments



Word will ein Dokument abspeichern. Die Daten werden über das Betriebssystem zum Gerätetreiber übermittelt.

Der Treiber in der VM greift auf einen virtuellen IDE-Controller zu und meint die Daten auf eine Festplatte zu schreiben.

Die Zugriffe auf die virtuelle Hardware werden vom Virtualisierungslayer weitergeleitet.

Erst das Wirts-OS greift mit seinen Treibern direkt auf die physische Hardware zu.

Der Brief *brief.doc* liegt in einer Behälterdatei auf einem physischen Datenträger.

Wie läuft in unserem Beispiel das Speichern des Dokuments auf die virtuelle IDE-Platte im Gastsystem ab (Abbildung 1.3)?

Der Gerätetreiber des Gastsystems

1. Das Programm Word muss in der VM, genau wie auf einem normalen PC, den Text in eine Datei speichern. Dazu übergibt Word die Daten an eine Routine des Betriebssystems (im Beispiel Windows XP in der VM), die den Datenträgerzugriff regelt. Windows XP weiß, dass mit dem Laufwerk C: eine Festplatte gemeint ist, und reicht die Daten weiter an den zuständigen Gerätetreiber für diese IDE-Platte im Gast.
2. Der Gerätetreiber kommuniziert mit dem virtuellen IDE-Controller des Gastes, an dem die virtuelle IDE-Platte angeschlossen ist, wie mit einem physischen Controller. Der IDE-Controller würde im Normalfall als letztes Glied der Kette über ein angestecktes Flachbandkabel die Festplattenelektronik ansprechen und den Brief auf der Festplatte speichern ...

3. In einer VM gibt es aber keine Flachbandkabel! Die vermeintliche IDE-Festplatte in der VM existiert nur als Behälterdatei auf irgendeinem physischen Datenträger des Host-Rechners. Auch der IDE-Controller im Gast existiert nicht als Hardware, sondern er wird dem Gerätetreiber vom Virtualisierungslayer nur vorgegaukelt.

**Traum und
Wirklichkeit**

4. Der Treiber im Gastsystem meint aber, dass er direkt mit richtiger Hardware kommuniziert, welche die Schreiboperation bestätigt hat. Der Treiber meldet das erfolgreiche Schreiben ans Betriebssystem in der VM. Damit ist vom Gerätetreiber über das Betriebssystem bis hoch zur Textverarbeitung jeder überzeugt, gerade einen Brief auf einer IDE-Platte abgespeichert zu haben.

Die Sache ist im Gast erledigt, allerdings wurde bis zu dieser Stelle noch kein einziges Byte an irgendeine Hardware übertragen.

5. In Wirklichkeit hat die Virtualisierungssoftware die Daten abgefangen und muss sich nun darum kümmern, wo sie gespeichert werden. Die geschriebenen Sektoren des Gastsystems, die den Brief darstellen, müssen in der Behälterdatei der virtuellen Platte abgelegt werden. Die Datei kann im Netzwerk oder auf einer SCSI-Platte liegen, nur die emulierte Hardware erscheint dem Gast als IDE-Gerät.

**Der Virtualisie-
rungslayer**

6. Um die Daten in der Behälterdatei auf dem Host abzulegen, reicht sie der Virtualisierer mit einer Schreib Anforderung an das Wirtssystem weiter. Der Treiber des Wirtssystems spricht schließlich mit dem echten Controller und dem physischen Datenträger. Erst jetzt liegt der Brief auf einer Festplatte.

Der eigentliche Vorgang des Abspeicherns eines Briefes funktioniert innerhalb der VM also wie gewohnt. Das Gastbetriebssystem muss in keiner Weise modifiziert oder angepasst werden, um in einer virtuellen Maschine zu funktionieren. Entscheidend ist der „Betrug“ am Gerätetreiber in der VM, also auf der untersten Ebene der Architektur.

Der gesamte Vorgang der Hardware-Virtualisierung funktioniert so perfekt, dass selbst die Treiber der Gerätehersteller darauf hereinfallen. VMware emuliert beispielsweise einen LSI-Logic SCSI-Controller, der auch wirklich von der Firma LSI-Logic als Hardware gebaut und vertrieben wird. Die offiziellen Treiber von der Herstellerwebseite, die für den physischen Controller programmiert wurden, funktionieren genauso in einer virtuellen Maschine mit dem virtuellen SCSI-Controller, den VMware emuliert.

**Perfekte
Täuschung**

Auf die hier beschriebene Art und Weise funktionieren letztendlich fast alle Geräte, die das Gastsystem in einer VM anspricht. Von der Netzwerkkarte über den Grafikadapter bis zum Sound – alles eine perfekte Täuschung!

Kontrolle über die CPU in einer VM

Der Geschwindigkeitsverlust durch den Umweg über den emulierten Controller beim Zugriff auf eine virtuelle Platte lässt sich verschmerzen. Bei der Virtualisierung von RAM und CPU wird es dagegen komplizierter. Würden die Befehle des Betriebssystems oder der Applikationen nicht direkt auf der CPU laufen, sondern erst emuliert werden, dann wäre eine virtuelle Maschine viel zu langsam. Auch Hauptspeicher könnte mit einer Auslagerungsdatei emuliert werden, das System würde dadurch aber ebenfalls massiv ausgebremst. Auf beide Ressourcen, CPU und RAM, muss der Gast ohne große Umwege zugreifen, um eine akzeptable Geschwindigkeit zu erreichen. Das ist der Unterschied zwischen Emulation und Virtualisierung.

Gefahr von Abstürzen

Wenn aber alle Gäste uneingeschränkt auf RAM und CPU zugreifen, ist eine Abschottung nicht mehr gegeben. Eine VM könnte die Kontrolle übernehmen und den Host mit allen Gästen zum Absturz bringen. Das gleiche Problem hat auch ein Betriebssystem wie Windows oder Linux. Es muss die Kontrolle über alle laufenden Programme behalten und darf nicht von jeder schlecht programmierten Software immer wieder mit in den Abgrund gerissen werden (wie das bei Windows 95 gang und gäbe war). Deshalb muss ein modernes Betriebssystem eine höhere Priorität haben als die Anwendungen.

Prioritäten in Ring 0 und Ring 3

Dazu unterstützen i386-CPU's im so genannten *Protected Mode* (geschützter Modus) verschiedene Prioritätsstufen, die sich Ring 0 bis Ring 3 nennen. Im Ring 0 laufende Prozesse haben die höchste Priorität und die volle Kontrolle über den Rechner. Anwendungen aus höheren Ringen können auf darunter liegende Ringe und auf die Hardware dagegen nicht direkt zugreifen, sondern nur über Schnittstellen (*APIs*), die wiederum von Anwendungen im Ring 0 kontrolliert werden. Windows und Linux verwenden nur Ring 0 (so genannter *Kernel-Modus*), in dem das Betriebssystem läuft, und Ring 3 (so genannter *Benutzermodus*), wo alle Anwendungen laufen (Abbildung 1.4).

Gastsystem ohne direkten Zugriff

Um immer die Oberhand zu behalten und alle VMs kontrollieren zu können, muss die Virtualisierungsschicht die Gäste also im Benutzermodus von Ring 3 laufen lassen, als wären die Gastbetriebssysteme normale Applikationen. Natürlich erwarten die Systeme in der VM eine solche Einschränkung ihrer Allmacht nicht und versuchen wie gewohnt, als Chef im Kernel-Modus die Kontrolle über die Hardware zu erhalten.

An dieser Stelle greift der Virtualisierungslayer ein. Er fängt so genannte *privilegierte Operationen* der Gastbetriebssysteme ab, mit denen diese versuchen, Hardware direkt anzusprechen. Diese Operationen werden dann mit anderen ungefährlichen Befehlssequenzen nachgebildet, ohne dass der Gast das bemerkt.

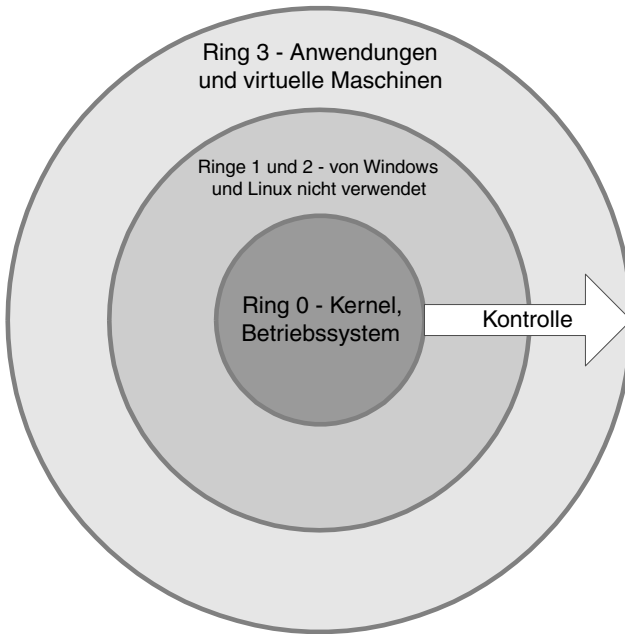


Abbildung 1.4:
Im Protected Mode
werden anhand
einer Ringstruktur
bestimmten Pro-
grammen Prioritä-
ten zugewiesen

Leider lassen sich nicht alle gefährlichen Befehle einfach abfangen, weil die Architektur von i386-Prozessoren niemals für Virtualisierung vorgesehen war und dadurch unzureichend implementiert ist. Normalerweise erzeugt jede privilegierte Operation eine so genannte *Exception* (Ausnahme), die sich vom Virtualisierer recht gut überwachen und bearbeiten lässt. Allerdings erzeugen nicht alle gefährlichen Operationen eine solche Ausnahme. Um diesen gefährlichen Befehlen auf die Spur zu kommen, muss der Virtualisierer den Code von Betriebssystem und Programmen im Gast während der Laufzeit aufwändig analysieren und solche Befehle ersetzen. Zum Teil erfolgt das dadurch, dass im ersten Durchlauf jede Befehlsfolge im Gast vom Virtualisierungslayer im Einzelschrittmodus (*Debug-Modus*) abgearbeitet wird, in dem jede Anweisung einzeln betrachtet werden kann. Zum Glück sind der überwiegende Teil ungefährliche Operationen, die ohne Modifikation direkt auf der CPU ausgeführt werden können, so dass es letztendlich nur zu einem geringen Virtualisierungs-Overhead kommt.

Das hört sich alles sehr aufwändig an? Zuerst wollte auch niemand so recht daran glauben, dass so etwas auf normaler i386-Hardware überhaupt funktionieren kann – bis zu dem Zeitpunkt, als VMware und Connectix (später von Microsoft gekauft) vor ein paar Jahren ihre ersten Programmversionen vorstellten! Seit 2006 bieten moderne CPUs mit Intels VT (*Virtualization Technology*, auch *Vanderpool* genannt) oder AMDs *Pacifica* als eingebaute Unterstützung zur Hardware-Virtualisierung weitere Prioritätsschichten, die noch unterhalb von Ring 0 angesiedelt sind. In der Priorität liegen diese also am höchsten. Ein dort laufender Virtualisierungslayer kann alle anderen Betriebsys-

Hardware-Unterstützung macht Virtualisierung einfacher

teme kontrollieren, während diese wie gewohnt im Ring 0 laufen. Damit wird die Programmierung von Virtualisierungssoftware vereinfacht und die Geschwindigkeit optimiert.



Übrigens ist Virtualisierung bei Großrechnern oder im Mainframe-Lager schon seit Jahrzehnten gang und gäbe und wird direkt von der Hardware und von den Betriebssystemen unterstützt. So neu ist die Idee also nicht.

1.3 Das Wichtigste zur Hardware auf dem Host und in den VMs

Mit diesem kurzen Ausflug in die Tiefe richtet der folgende Abschnitt das Augenmerk auf Themen, die Sie als Anwender direkt betreffen:

- ▶ Und über welche Hardware sollte der Host verfügen, und welche Komponenten sind besonders wichtig?
- ▶ Welche Hardware wird dem Betriebssystem in einer VM vom Virtualisierungslayer geboten?
- ▶ Was für Geräte werden dagegen in den Gästen nicht unterstützt?

1.3.1 Die Prozessoren auf dem Host und im Gast

Wie Sie bereits erfahren haben, werden CPUs nicht emuliert. In der VM tauchen immer die CPU-Typen des Hosts auf, z.B. AMD oder Intel.

Die physischen CPUs auf dem Host

Ein Host kann im Minimalfall über nur eine einzige CPU verfügen, dann teilen sich alle Gäste diesen Prozessor. Wenn der Host über zwei oder mehr CPUs verfügt, dann können die Gäste zur Lastverteilung auf verschiedenen Prozessoren laufen. Virtualisierung nutzt mehrere Prozessoren besonders gut aus. Es existieren verschiedene Arten von Multiprozessoren, die auf dem Host zum Einsatz kommen können:

- ▶ *Echte Multiprozessoren* sind mehrere physische CPUs, die als getrennte Einheiten in einzelnen Sockeln auf dem Board stecken. Das ist die klassische *Dual-CPU*, *Quad-CPU* usw. Durch eigene Busanbindung und eigene Recheneinheit verdoppelt sich durch zwei CPUs die Leistung, vorausgesetzt, die Anwendungen nutzen die Architektur.
- ▶ *Dual-Core-CPU*s haben zwei physische Kerne (Hauptprozessoren) in einem Gehäuse und verhalten sich fast wie zwei separate CPUs in getrennten Sockeln. Dual-Core-CPU sind von der Leistung her mit echten Dual-CPU vergleichbar.

**Hyperthreading
und Dual Core**

- ▶ Beim *Hyperthreading* sind Teile der physischen CPU, z.B. die Register, doppelt vorhanden, und die CPU ist in zwei logische interne Einheiten unterteilt. Dadurch wird zwar die parallele Abarbeitung verschiedener interner Prozesse möglich, was einen Performancegewinn bringen kann. Die eigentliche Recheneinheit ist auf dem Chip aber trotzdem nur einmal vorhanden. Maschinenbefehle laufen immer sequenziell hintereinander ab, wodurch nie die Leistung echter Multi-CPU's erreicht wird.
- ▶ Es sind auch Kombinationen möglich, zwei Dualcore-CPU's in physisch getrennten Sockeln mit eingeschaltetem Hyperthreading ergeben insgesamt acht logische CPU's (2*2*2).

Es ist wichtig zu wissen, dass Software oft auf die Anzahl physischer CPU's lizenziert wird. Z.B. ist es beim ESX Server 3 wesentlich preiswerter, zwei Dual-Core-CPU's einzusetzen als vier physische CPU's, obwohl die Leistung ähnlich ist (zur Lizenzierung des ESX Servers siehe Teil 2, Kapitel 9, „VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2“).



Mehrere VMs können problemlos auf ein und demselben Prozessor im Host laufen und sich dessen Leistung teilen. Die Gäste lassen sich aber auch auf verschiedene Prozessoren verteilen. So kann eine einzige VM mit viel Last die erste CPU für sich allein beanspruchen, während sich alle anderen Gäste die zweite CPU teilen müssen. Der Gast merkt nicht, ob er eine physische CPU exklusiv zur Verfügung hat oder ob er sich mit vielen anderen Gästen einen Prozessor teilt.

Lastverteilung

Der Virtualisierungslayer, bzw. Hypervisor oder Virtual Machine Monitor, teilt den Gästen per Zeitscheibe einen Teil der Prozessorleistung zu. Beispielsweise darf zuerst die VM01 einige Befehle abarbeiten, danach die VM02 usw. Bei jedem Umschalten erfolgt das Sichern des gesamten CPU-Status (Registerinhalte usw.) eines Gastes.

Beim ESX Server funktioniert die Verteilung von CPU-Leistung an die Gäste sehr fein bis hinunter auf MHz-Ebene.

Unter Microsoft Virtual Server lassen sich die CPU-Ressourcen für einen Gast begrenzen oder prozentual über alle Gäste verteilen.

VMware Workstation und VMware Server verteilen die laufenden VMs automatisch auf verschiedene CPU's im Host. Bestimmte VMs lassen sich aber auch manuell bestimmten CPU's zuweisen.

Unter Virtual PC laufen alle Gäste immer auf ein und derselben CPU, so dass die übrigen Prozessoren im Host weitestgehend ungenutzt bleiben.

Die virtuellen CPUs in den Gästen

Virtuelle Multi-prozessoren

Im Gast laufen alle Maschinenbefehle der Programme und des Betriebssystems direkt auf einer physischen CPU des Hosts. Alle vorgestellten Virtualisierungsprodukte unterstützen nur eine eingeschränkte Anzahl virtueller CPUs in den VMs.

Microsoft reicht grundsätzlich immer nur eine einzige CPU durch, egal wie viele im Host stecken.

VMware Workstation und Server können jeweils zwei CPUs virtualisieren, der Player nur eine. Der ESX Server 3 kann maximal vier Prozessoren an einen Gast weitergeben. Dabei lassen sich auch Dual-Core- oder Hyperthreading-Prozessoren als zwei virtuelle CPUs durchreichen. Letzteres ist aber aus Performancegründen nur zu Testzwecken sinnvoll, etwa um in einer VM den Umgang einer Software mit zwei CPUs zu testen.

Unterstützung der Betriebssysteme für mehrere CPUs

Mehrere Prozessoren müssen vom Gastsystem und auch vom Hostsystem unterstützt werden. Dazu wird z.B. von Windows die Unterstützung für *SMP* (*symmetrisches Multiprocessing*) gleich beim Setup des Systems eingerichtet, sobald zwei CPUs erkannt werden.

Beim nachträglichen Wechsel von Dual-CPU zu Single-CPU müssen Anpassungen am Betriebssystem in der VM vorgenommen werden, eine automatische Erkennung erfolgt dann nicht mehr. Ohne Anpassung kann es je nach Betriebssystem beim Bootvorgang zu Abstürzen oder zu Effekten, wie permanenter hoher CPU-Last, kommen.

Wenn dagegen umgekehrt beim Wechsel von Single-CPU zu Dual-CPU keine Anpassung am Betriebssystem im Gast erfolgt, dann wird die zweite CPU einfach nicht verwendet. Der Vorgang des nachträglichen Anpassens der Gastsysteme an die CPU-Architektur wird in *Teil 3, Kapitel 6, „P2V – physische Server in virtuelle Maschinen übernehmen“*, ausführlich beschrieben.



Für die meisten Anwendungsfälle, auch im produktiven Einsatz, genügt in den Gästen eine virtuelle CPU. Verwenden Sie in einer VM nur dann mehrere virtuelle CPUs, wenn Sie im Gast Anwendungen benutzen, die einen echten Vorteil daraus ziehen, z.B. Datenbanken. Ansonsten verbraucht schon der Virtualisierungslayer für die Verwaltung der virtuellen Prozessoren unnötig viele Ressourcen, und diese Verschwendung bringt keinerlei Nutzen für Sie.

1.3.2 Der Hauptspeicher auf dem Host und in den Gästen

Hauptspeicher ist das Lebenselixier virtueller Maschinen – es gilt hier: *Viel hilft viel!* Grundsätzlich sollte im Host so viel RAM stecken, wie alle laufenden VMs benötigen. Zusätzlich muss auch für den Host noch genügend übrig bleiben, sonst entstehen Performanceprobleme.

Während die Microsoft-Produkte bei der Zuweisung des Hauptspeichers an die Gäste in der Summe nicht den wirklich vorhandenen RAM überschreiten können, ermöglicht es VMware, allen laufenden VMs in der Summe mehr RAM zuzuweisen, als wirklich physisch vorhanden ist (*Memory over-commitment*). Das liegt daran, dass der zugewiesene RAM nicht immer auch wirklich vom Gastsystem verwendet wird.

Mehr Speicher zuweisen als physisch vorhanden ist

VMware verwaltet den Hauptspeicher sehr intelligent und kann unbenutzten Speicher eines Gastes anderen Gästen zur Verfügung stellen (*Memory Page Trimming*). Weiterhin werden gleiche Speicherseiten, die von verschiedenen laufenden Anwendungen mehrfach benötigt werden, immer wieder mitverwendet, ohne jedes Mal zusätzlich in den RAM geladen zu werden (*Memory Sharing*).

Diese Funktionen sparen teilweise viel Hauptspeicher, man kann sich aber nicht darauf verlassen. Wenn doch einmal alle Gäste auf ihrem versprochenen Speicher bestehen, dann bleibt VMware nichts anderes übrig, als virtuellen Speicher über eine Auslagerungsdatei auf der Festplatte zu erzeugen. Dabei geht die Performance des gesamten Systems teilweise rapide in die Knie. Für Testumgebungen kann es allerdings sehr nützlich sein, ein paar VMs mehr starten zu können, als der physische RAM es eigentlich zulassen würde (mehr zu den Einstellungen der Speicherverwaltung unter VMware lesen Sie in *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*).

Der ESX Server unterstützt zusätzlich das so genannte *Memory Ballooning*. Dabei zwingt ein spezieller Treiber der VMware Tools (*vmmemctl-Treiber*) durch Speicheranforderungen das Gastsystem, andere Speicherseiten in die Auslagerungsdatei auszulagern. Der dabei frei werdende physische RAM kann anderen aktiven Gästen mit höherer Priorität zugeteilt werden.

Jeder Gast unter allen Produkten benötigt zur reinen Verwaltung immer etwas mehr Hauptspeicher, als ihm zugewiesen wurde. Je nach zugeteiltem Speicher können das 5–10% zusätzlich sein. Bei mehreren parallel laufenden Gästen kann es deshalb vorkommen, dass der verfügbare RAM ausgeht, obwohl rein rechnerisch für alle VMs gar nicht so viel reserviert wurde. In der Praxis merkt man das nur, wenn viele VMs gleichzeitig laufen und der verfügbare Speicher voll ausgeschöpft wird.

Verwaltungs-Overhead



Maximal 3,6 GB

Für die Virtualisierung großer Serversysteme ist es wichtig, die folgende Begrenzung zu kennen: Egal wie viel RAM im Host vorhanden ist, von fast allen Produkten können jedem Gast maximal 3,6 GB davon zugewiesen werden. Nur der ESX-Server 3 bietet jedem Gast bis zu 16 GB Hauptspeicher. Auch auf dem Host selbst können Sie nicht ohne weiteres mehr als 4 GB RAM verwenden.

Mehr als 4 GB physischen Hauptspeicher im Host verwenden

4-GB-Grenze bei 32-Bit-Systemen

Noch vor der CPU-Leistung und vor den Festplatten spielt die RAM-Ausstattung des Hosts die entscheidende Rolle, ob Sie an Ihrer virtuellen Welt Freude haben oder nicht. Je mehr VMs parallel laufen sollen, umso mehr Hauptspeicher benötigt Ihr Host. Unter den noch häufig vorhandenen 32-Bit-Systemen ist aber spätestens ab 4 GB RAM Schluss mit der Adressierung, das kann im produktiven Betrieb und in großen Testumgebungen knapp werden. Sie können in Ihren Host so viel Speicherriegel stecken, wie Sie wollen, das Betriebssystem wird maximal 4 GB anzeigen, der Rest liegt auch für die VMs ungenutzt brach. Um mehr als 4 GB RAM nutzen zu können, gibt es drei Möglichkeiten:

PAE – Physical Address Extension

► *PAE (Physical Address Extension) auf 32-Bit-Hardware* – Um die Einschränkung der begrenzten Adressierungsbreite auf einem 32-Bit-System zu umgehen, wurde die so genannte *Physical Address Extension*, kurz *PAE* entwickelt, die es ermöglicht, bis zu 64 GB Hauptspeicher zu benutzen. Unter Windows müssen Sie den Windows Server 2003 Enterprise Edition als Hostsystem anschaffen, die Standard-Edition adressiert maximal 4 GB. In der *Boot.ini* ist dann einfach die Option */PAE* an den Booteintrag anzuhängen (siehe dazu auch den entsprechenden Artikel in der Microsoft Knowledge Base <http://support.microsoft.com/kb/283037/en-us>):

```
multi(0)disk(0)rdisk(0)partition(1)\
WINDOWS="Windows Server 2003 Enterprise"
/fastdetect /PAE
```

Wollen Sie diese Funktion unter Linux einschalten, muss der Kernel mit einer speziellen Option kompiliert werden (siehe *Teil 2, Kapitel 4, „Linux-Host mit VMware Server und Integration ins Windows-Netz“*).

64-Bit-Hardware

► *64-Bit-Hardware mit 64-Bit-Betriebssystem* – Auf 64-Bit-Hardware mit 64-Bit-Betriebssystem kann Speicher auch ohne zusätzliche Optionen voll genutzt werden. Unter Windows reicht es, wenn Sie eine 64-Bit-Version anschaffen. Hier genügt dann auch wieder der Windows 2003 Server Standard Edition oder sogar Windows XP, um mehr als 4 GB RAM zu verwenden. Eine PAE-Unterstützung ist nicht mehr notwendig. Wenn Sie dagegen ein 32-Bit-Betriebssystem auf einem 64-Bit-Rechner installieren, benötigen Sie wieder PAE.

Unter Linux ist die Installation von VMware auf einem 64-Bit-System ebenfalls problemlos möglich, wenn Sie eine unterstützte Distribution (z.B. SUSE) verwenden. Da VMware keine native 64-Bit-Anwendung ist, sondern 32-Bit-Kompatibilität benötigt, ist der Betrieb auf puren 64-Bit-Distributionen (z.B. Debian) schwieriger einzurichten (siehe Teil 2, Kapitel 4).

- *ESX Server* – VMware ESX Server hat einen eigenen Kernel, der von sich aus automatisch den vorhandenen Hauptspeicher im Host auf 32-Bit- und auf 64-Bit-Hardware erkennt und verwaltet.

1.3.3 Platten, CD und Floppy in den virtuellen Maschinen

Die virtuellen Festplatten sind das Rückgrat einer VM, schließlich sind dort die Gastbetriebssysteme installiert. Ich widme diesem Thema einen eigenen ausführlichen Workshop in Teil 3, Kapitel 3, „Die Virtuellen Platten als Herzstück der Gastsysteme“. Dort werden der Aufbau und der praktische Umgang mit den virtuellen Datenträgern detailliert beschrieben. Hier finden Sie vor allem eine ausführliche Besprechung der möglichen physischen Datenträger als Grundlage für die virtuellen Maschinen.

Virtuelle Festplatten der Gäste als Dateien auf dem Host

Sie können physische Festplatten des Host-Systems in eine VM einbinden und direkt verwenden. Das ist aber in der Praxis eher unüblich. Stattdessen wird für eine virtuelle Platte meist eine eigene Datei auf dem physischen Host-Datenträger erstellt, in der die Sektoren einer virtuellen Platte liegen. Im Beispiel zur Funktion einer VM haben Sie bereits kennen gelernt, wie eine virtuelle Platte arbeitet (siehe auch Abschnitt 1.2, „So funktioniert eine virtuelle Maschine“).

Mehrere virtuelle Platten können je nach verfügbarem Platz auf einem physischen Datenträger liegen. Die Behälterdateien können Sie auf dem Host einfach kopieren und in eine andere VM einbinden. Das entspricht dem Umbauen einer echten Festplatte von einem PC in einen anderen. Durch die Kopie einer virtuellen Platte erhalten Sie einen 1:1-Klon des enthaltenen Betriebssystems, ähnlich einem Image eines physischen Rechners. Virtuelle Platten lassen sich auf DVD archivieren oder auf dem Laptop mitnehmen.

Der ESX Server verwendet ein spezielles optimiertes Dateisystem, *VMFS (VMware Filesystem)* auf den physischen Datenträgern. Nur dort können die virtuellen Platten abgelegt werden. Beim Austausch von VMs des ESX Servers mit anderen Produkten, wie dem VMware Server, müssen die virtuellen Platten erst konvertiert werden. Näheres dazu finden Sie in Teil 2, Kapitel 9.



Virtuelle SCSI- oder IDE-Controller in den Gästen

Fast alle im Buch vorgestellten Produkte emulieren wahlweise virtuelle SCSI-Controller und virtuelle IDE-Controller in den Gästen, an denen die virtuellen Platten angeschlossen sind. Mit folgenden beiden Einschränkungen:

- ▶ Der ESX Server kennt in den Gästen nur virtuelle SCSI-Platten. Virtuelle IDE-Platten von VMware Server oder von VMware Workstation müssen erst umgewandelt werden, bevor sie auf einem ESX Server verwendet werden können.
- ▶ Virtual PC kennt nur virtuelle IDE-Platten. SCSI-Platten vom großen Bruder Virtual Server können aber einfach als IDE-Platten verwendet werden.

Welcher Typ von Controller im Gast emuliert wird, ist völlig unabhängig von der wirklichen physischen Ausstattung. Eine virtuelle IDE-Platte kann auf einer SCSI-Platte oder einem SAN untergebracht sein. Umgekehrt kann ein Gast durchaus virtuelle SCSI-Platten verwenden, obwohl der Host nur über eine IDE-Platte verfügt. Virtuelle SCSI-Platten sind meist etwas schneller, IDE-Platten unproblematischer mit den Treibern.

CD und Floppy in den Gästen

ISO-Images verwenden

Disketten und CDs, die im realen Laufwerk des Hosts liegen, können auch vom Gast verwendet werden. Die Laufwerke werden einfach durchgereicht. Zusätzlich lassen sich ISO-Images direkt als virtuelle CD in eine VM einbinden, das funktioniert auch mit Disketten. Das Gastsystem sieht dann eine echte CD oder DVD. Damit können Sie Software direkt von einem ISO-Image installieren, ohne erst eine CD zu brennen. Von häufig benötigten Installations-CDs können Sie ein Image-Archiv erstellen. Tools zum Erstellen von ISO-Images finden Sie in *Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“*.



Virtual PC hat ein Problem mit DVDs, die mehr als 2,2 GB Daten enthalten. Als Lösung können Sie diese DVD im LAN freigeben und dann über diese Netzwerkfreigabe vom Gast aus darauf zugreifen.

1.3.4 Arten von physischen Host-Datenträgern als Speicherplatz für virtuelle Platten und ISO-Images

Die virtuellen Platten und ISO-Images benötigen letztendlich einen physischen Datenträger als Speicherplatz. Neben Hauptspeicherausstattung und CPUs im Host ist der Massenspeicher eine der wichtigsten Komponenten für die virtuelle Infrastruktur. Grundsätzlich lassen sich virtuelle Platten auf allen Datenträgern ablegen, die vom Host angesprochen werden können.

USB-Platten als Sicherungs- oder Transportmedium

Externe USB-Platten sind wegen Ihrer vergleichsweise geringen Geschwindigkeit eher als Sicherungslösung zum Kopieren der virtuellen Maschinen oder als temporäre Notlösung zum Betrieb in Testumgebung bzw. bei einer Kunden-Demo geeignet. Zum Transport virtueller Maschinen sind sie ideal.

Lokale Festplatten IDE, SATA, SCSI und RAID-Controller

Eine lokale Festplatte (*DAS – Direct Attached Storage*) ist der verbreitetste Datenträger in Computern. Je nach Anforderungen kommen im einfachsten Falle IDE- oder SATA-Platten zum Einsatz. SCSI-Platten sind meist teurer und verlangen einen zusätzlichen Controller, bieten aber oft höhere Geschwindigkeiten und haben vor allem eine längere Lebensdauer, da sie für den Serverbetrieb ausgelegt sind.

RAID-Controller (Redundant Array of Independent Disks), die es für SCSI-Platten und auch für SATA-Platten gibt, spiegeln die Daten über mehrere Festplatten (z.B. RAID1) oder bilden Prüfsummen über alle Festplatten eines RAID-Verbandes (z.B. RAID5). Damit kann eine Festplatte auch ausfallen, ohne dass es zu Datenverlust kommt, und man hat Gelegenheit, die defekte Platte, meist sogar im laufenden Betrieb, auszutauschen. In produktiven Servern und in zentralen Speicherlösungen sind RAID-Controller Pflicht.

Ausfallsicherheit durch Raid

Eine neuere Variante ist RAID6, die besonders für die anfälligeren SATA-Platten empfehlenswert ist. Während bei einem RAID5-Verband eine Platte ausfallen kann, ohne dass Daten verloren gehen, verfügt eine RAID6-Konfiguration über eine zusätzliche Redundanz, so dass auch bei zwei gleichzeitig ausgefallenen Platten alle Daten erhalten bleiben.

RAID6

Externer Speicher in einem SAN mit Fibre-Channel

Der Nachteil an lokalen Platten ist, dass der Speicher oft auf Servern zur Verfügung steht, wo er gar nicht gebraucht wird, wogegen andere Maschinen gerade keinen Platz mehr zur Verfügung haben. Weiterhin muss jeder einzelne Server über Ausfallsicherungen wie RAID-Systeme verfügen. Und wenn ein Server gegen einen neuen ausgetauscht wird, müssen die Daten erst übernommen werden. Aus diesem Grunde setzen vor allem Anwender in größeren Umgebungen auf externe Speicherlösungen, die den Plattenplatz für mehrere Server zentral vorhalten und diesen wesentlich flexibler verwalten. Der Zugriff erfolgt über spezielle Netzwerke, die nur für die Speicheranbindung reserviert sind.

Die Profilösung für große Umgebungen ist ein *SAN (Storage Area Network)*. Das sind dedizierte Geräte, die für die Massenspeicherverwaltung optimiert sind und die über Ausfallsicherungen verfügen. Dabei kommen RAID-Konfigurationen oder sogar Spiegelung über mehrere

Geräte an räumlich getrennten Standorten zum Einsatz. In einem SAN können Dutzende Festplatten eingebaut sein.

HBA – Host Bus Adapter

Für den Datentransport im Speichernetzwerk wird meist das optimierte Protokoll *Fibre Channel* mit 2 bzw. 4 GBit/s über Glasfaserleitungen verwendet. Dazu sind in den angeschlossenen Rechnern spezielle Steckkarten eingebaut, so genannte *HBA (Host Bus Adapter)*, die nach außen die Verbindung zum zentralen Speicher über Glasfaser halten und nach innen für das Betriebssystem Teilbereiche des zentralen Speichers wie lokal eingebaute Festplatten bereitstellen, ähnlich einem lokalen SCSI- oder RAID-Controller.

LUN – ein Bereich auf dem SAN

Die Bereiche, in die der verfügbare Platz im SAN unterteilt ist, werden als *LUN (Logical Unit)* bezeichnet. Ein SAN verfügt über mehrere solcher LUNs, um seinen Speicherplatz verschiedenen angeschlossenen Rechnern zur Verfügung zu stellen. Jeder Rechner kann als Client mit seinem HBA auf jeweils eigene LUNs zugreifen. Eine LUN erscheint im zugreifenden Betriebssystem als Festplatte, die formatiert werden muss, das ist der Unterschied zu einer Dateifreigabe im LAN (siehe auch „Blockorientierter oder dateiorientierter Zugriff bei SAN oder NAS“ weiter unten). In den meisten Fällen ist eine LUN einem bestimmten Rechner fest zugeordnet. Wird der Rechner ausgetauscht, kann der Nachfolger sofort die LUN mit den enthaltenen Daten weiterverwenden.



Mehrere ESX Server können, dank ihres speziellen Dateisystems VMFS, auf eine gemeinsame LUN gleichzeitig zugreifen, das ist mit den meisten anderen Dateisystemen, wie NTFS, nicht möglich (siehe Teil 2, Kapitel 9). Erst externer Speicher ermöglicht die vielen Zusatzfunktionen virtueller Umgebungen, z.B. Cluster oder das Verschieben laufender VMs von einem Host auf einen anderen.

Externer Speicher (SAN) mit Anbindung über iSCSI

Speicheranbindung über Ethernet

Preiswerter als Fibre-Channel ist die Anbindung des externen Speichers über das Protokoll *iSCSI (Internet Small Computer System Interface)*. Prinzipiell übermittelt iSCSI die Kommunikation der SCSI-Schnittstelle über das TCP/IP-Protokoll auf einer normalen Netzwerkverbindung, es verlängert sozusagen das Kabel für die lokalen Festplatten über das LAN. Dadurch wird es möglich, über eine vorhandene Ethernet-Verkabelung und die üblichen Netzwerkkarten und Switches einen externen Speicher an einen Server anzubinden. Bereits mit dem üblichen Gigabit-Ethernet lassen sich in der Praxis gute Ergebnisse für kleine und mittlere Umgebungen erzielen.

Vor allem mit der Verfügbarkeit von 10 GBit Ethernet wird iSCSI als preiswerte Speicheranbindung noch interessanter. Die Clients können weiterhin über preiswertes Gigabit-Ethernet an den Switch angeschlossen sein. Eine 10-GBit-Verbindung vom Switch zum Speichergerät verhindert dann den bisherigen Flaschenhals.

Grundsätzlich spielen bei iSCSI zwei Komponenten die Hauptrolle, das *Target* und der *Initiator*. Ein iSCSI-Target ist der Ort, an dem die Daten liegen, auf die alle angebundenen Rechner zugreifen wollen. Ein iSCSI-Target kann ein dediziertes SAN mit iSCSI-Schnittstelle sein. Diese Hardware von spezialisierten Herstellern ist meist recht teuer, was die Ersparnis der preiswerten Anbindung teilweise schmälert. **iSCSI-Target**

Als Alternative bietet sich als Target eine Software-Lösung auf einem normalen Linux- oder Windows-Server an. Diese Software läuft als Anwendung und gibt einen Teil der Plattenkapazität des Servers als LUNs im Netzwerk frei. Dadurch können Sie auf erschwingliche Standardhardware für den Server zurückgreifen. Als Software für ein iSCSI-Target kommen z.B. folgende Lösungen in Frage:

SANmelody von DataCore:

<http://www.datacore.com/>

WinTarget von String Bean:

<http://www.stringbeansoftware.com/products.asp>

StarWind von Rocket Division Software:

<http://www.rocketdivision.com/>

Für die Linux-Welt existieren ebenfalls einige Alternativen:

iscsitarget.sourceforge.net/

<http://www.ardistech.com/iscsi/>

Eine weitere sehr interessante Möglichkeit, aus Standardservern iSCSI-Targets zu machen, sind Steckmodule mit eigenem Betriebssystem auf einem Flash-Speicher, wie z.B. *Open-E iSCSI*. Von diesen Modulen bootet der Rechner gleich als Speichergerät, ohne dass Sie überhaupt erst Windows oder Linux installieren zu müssen:

<http://www.open-e.com/>

Beim Preis der Hardware und der Software sollten Sie niemals die zentrale Rolle und die Wichtigkeit eines externen Speichersystems vergessen. Ausfallsicherheit, Zuverlässigkeit und guter Support sind wichtiger als ein niedriges Angebot. In Fragen der Performance sollten Sie sich speziell für Ihre Anwendungen im produktiven Einsatz unbedingt beraten lassen.



Neben der zentralen Komponenten, dem Target, ist der *iSCSI-Initiator* die Client-Komponente, über die der Zugriff auf das Target erfolgt. Über den Initiator benutzt der Rechner den vom Target bereitgestellten externen Speicher genauso wie eine lokal eingebaute Festplatte. Ein Initiator kann entweder ein so genannter *HBA (Host Bus Adapter)* sein, wie er auch bei Fibre-Channel zum Einsatz kommt. Ein Hardware-Initiator verfügt über einen eigenen Prozessor, der das gesamte Protokollhandling übernimmt. Das entlastet vor allem die CPU des Servers und kommt der Performance zugute. **iSCSI-Initiator**

Software-Initiator

Eine weitere Möglichkeit ist ein so genannter *Software-Initiator*. Dieser wird als Treiber im Betriebssystem eines Clients installiert und verwendet eine verfügbare Netzwerkkarte, um darüber mit dem iSCSI-Target zu kommunizieren. Das hat den Vorteil, dass recht preiswerte Hardware zum Einsatz kommt, ein teurer HBA wird nicht benötigt. Gerade für den Einstieg ist ein Software-Initiator interessant.

Der Nachteil liegt in der schlechteren Leistung einer Software-Lösung, da die CPU des Rechners belastet wird, um den Protokollverkehr zu verwalten. Bei aktuellen Rechnermodellen, die meist nie richtig ausgelastet sind, muss das aber nicht unbedingt ein Nachteil sein. Als Software bietet sich z.B. der Microsoft iSCSI Software Initiator an, auch viele Linux-Distributionen liefern einen Initiator bereits mit.

<http://www.microsoft.com/windowsserver2003/technologies/storage/iscsi/>



Weniger Interrupts und Overhead

Jumbo Frames zur Verbesserung der Leistung bei iSCSI und NAS

Versuchen Sie, beim Einsatz von iSCSI auf Ihrem Speichernetzwerk so genannte *Jumbo-Frames* zu verwenden. Das sind wesentlich größere Pakete (MTU ab 9000 Bytes), als bei Ethernet standardmäßig verwendet werden. Dadurch lassen sich in einem Paket im Verhältnis zu den Steuerungsdaten des Protokolls mehr reine Nutzdaten transportieren, wodurch der Protokoll-Overhead stark reduziert wird. Weiterhin sind für die Verarbeitung insgesamt weniger Pakete, und damit weniger Interrupts auf den beteiligten Stationen, notwendig, wodurch die CPU stark entlastet wird. In knappen Worten: Größere Pakete verbessern die Performance!

Schauen Sie in der Dokumentation Ihrer LAN-Switches und der Netzwerkkarten (bei Software-Initiator), ob und wie diese Paketgrößen unterstützt werden.

Ein weiteres Kriterium ist die Anbindung des Speichers. Greifen mehrere Clients mit Gigabit-Anbindung auf ein SAN zu, das selbst nur über einen einzigen Gigabit-Adapter verfügt, dann liegt an dieser Stelle der Flaschenhals, und die Leistung kann durch so genannte *Dropped Packets* (*verlorene Pakete*) stark einbrechen. Mehrere Adapter oder ein 10-GBit-Adapter sind bei vielen zugreifenden Clients für das Target durchaus angebracht.

Dateifreigaben im LAN auf einem Server oder NAS

Eine interessante Alternative zu lokalen Datenträgern und zu teuren SAN-Lösungen sind Dateifreigaben in einem LAN mit Gigabit-Ethernet-Anbindung. Vorausgesetzt, ein schneller Dateiserver kommt zum Einsatz, können damit manchmal sogar bessere Geschwindigkeiten erzielt werden als mit langsamen lokalen Platten. Vor allem entlastet diese Auslagerung die Systemplatte des Hosts von den Zugriffen der VMs, wenn nur eine lokale Festplatte zur Verfügung steht.

Sinnvoll ist dabei ein separates physisches Netzwerk mit eigenem Switch oder VLAN, über das nur der Verkehr vom Host zu den Freigaben läuft, auf denen die Platten der VMs liegen. Mischen Sie LAN und Speicherzugriff, kann es schnell zu Leistungseinbußen kommen.

Vor allem in Testumgebungen mit den Hosted Produkten bietet die Verwendung von LAN-Freigaben einige Vorteile:

- ▶ Komponenten für die Ausfallsicherheit (RAID-Controller) müssen nur einmal zentral im Server bereitgestellt werden.
- ▶ Die gesamte Anbindung mit den üblichen Netzwerkkarten, Switches und Kupferkabeln ist sehr preiswert.
- ▶ Alle VMs (vor allem Vorlagen) liegen zentral erreichbar auf einem Server und können von verschiedenen Arbeitsplätzen verwendet werden.
- ▶ Eine Konfiguration spezieller Protokolle (iSCSI, Fibre-Channel) ist nicht notwendig. Es kann die gewohnte LAN-Infrastruktur zum Einsatz kommen.
- ▶ Vor allem wird auch für die Hosted Produkte der gemeinsame Zugriff von unterschiedlichen Hosts auf die Dateien einer VM möglich. Das kann eigentlich nur der ESX Server. Dadurch können Sie z.B. eine VM auf einem Host in den Suspend-Modus versetzen und auf dem anderen Host wieder zum Leben erwecken, was einem Verschieben der laufenden Maschine fast in Echtzeit entspricht.

Diese Funktionen werden sonst nur bei der Verwendung von teurem externen Speicher (SAN) und dazu passender komplizierter Konfiguration von Cluster-Lösungen möglich (siehe Teil 2, Kapitel 8, „Cluster mit VMs und einem iSCSI Target als externem Speicher“).

Als zentraler Fileserver kommt alles in Frage, was eine Dateifreigabe bereitstellt, auf die der Host als Client zugreifen kann. Unter Windows ist SMB (*Server Message Block*) bzw. CIFS (*Common Internet File System*) üblich, dazu müssen Sie am Server nur eine Freigabe einrichten und sich vom Host aus als LAN-Client darauf verbinden.

**Dateiserver
im LAN**

Unter Linux ist NFS (*Network File System*) der Standard. NFS ist im Allgemeinen auch schneller als SMB. Unter Windows kann NFS mit den kostenlosen Microsoft Windows Services für Unix bereitgestellt werden (<http://www.microsoft.com/windows/sfu>), die seit Windows Server 2003 R2 bereits dabei sind.

Ein dediziertes Gerät, das nur Dateifreigaben bereitstellt, wird als NAS (*Network Attached Storage*) bezeichnet. Das sind meist kompakte Gehäuse mit optimiertem Betriebssystem und Web-Interface zur Remote-Verwaltung. Dazu kommen eigene Ausfallsicherheit, wie RAID5, und viel Einbauplatz für Festplatten. Ein NAS unterstützt, genau wie ein Fileserver, Protokolle, wie SMB oder NFS.

Dedizierter NAS



Zwar ist die Verwendung von Dateifreigaben die langsamste Anbindung von externem Speicher, aber in Test- und Schulungsumgebungen sicherlich eine gute Alternative. Seitdem der ESX Server 3 ebenfalls eine NAS-Anbindung erlaubt, ist diese ehemals verpönte Methode sozusagen geadelt worden. In produktiven Umgebungen mit hohen Leistungsanforderungen sollten Sie allerdings auf ein SAN mit Fibre-Channel oder wenigstens iSCSI-Anbindung oder auf schnelle lokale SCSI-Festplatten an einem oder mehreren RAID-Controllern setzen.

Blockorientierter oder dateiorientierter Zugriff bei SAN oder NAS

Der Unterschied eines SAN zu einem NAS bzw. einer LAN-Freigabe ist die Art des Zugriffs, er erfolgt bei einem NAS *dateiorientiert*, bei einem SAN *blockorientiert*.

Dateiorientierter Zugriff

Beim dateiorientierten Zugriff übernimmt der zentrale Dateiserver die Verwaltung von Datenblöcken des Dateisystems und auch von Dateirechten. Der Client (in unserem Falle also der Host) greift auf die Dateien zu, ohne zu wissen, auf welchem Dateisystem in welchem Format sie gespeichert sind. Das entspricht dem normalen Zugriff auf einen Fileserver. Am Client ist nur eine Verbindung mit der Freigabe einzurichten, die gesamte Verwaltung von Datenblöcken und Sektoren bzw. das Anlegen und Formatieren von Partitionen erfolgt am Dateiserver.

Blockorientierter Zugriff

Beim blockorientierten Zugriff wird der externe Speicher, die LUN, dem Client (in unserem Falle wieder dem Host) wie eine leere Festplatte präsentiert. Der Client muss sich um die Verwaltung des Dateisystems dieser Festplatte selbst kümmern. Gegebenenfalls muss er auch selbst eine Partition anlegen und diese formatieren. In vielen Fällen ist der blockorientierte Zugriff durch optimierte Protokolle schneller als der Zugriff auf Dateifreigaben.

1.3.5 Physische und virtuelle Netzwerkkarten

Damit eine virtuelle Maschine auch mit dem Rest der Welt kommunizieren kann, können Sie Ihr bis zu vier virtuelle Netzwerkkarten zuweisen. Jede virtuelle Netzwerkkarte wird von VMware hardwaremäßig emuliert. Das Betriebssystem in der VM denkt dabei, es ist ein echter Netzwerkkartenadapter eingebaut. In der Netzwerkumgebung des virtuellen Systems sehen Sie die Treiber zum emulierten Netzwerkkartentyp, unter VMware z.B. ein AMD-PCNET-Adapter, unter Microsoft eine Intel-Karte. An die Netzwerkkarten können Sie innerhalb der VM alle Protokolle binden, die im Gastsystem unterstützt werden, also auch IPX/SPX oder NetBEUI.

Die Netzwerkfunktionalität einer VM ist völlig unabhängig von den im Host eingebauten physischen Adaptern. Das geht so weit, dass im Host überhaupt keine physische Netzwerkkarte notwendig ist, wenn sich die Kommunikation der VMs auf die internen virtuellen Netzwerke bzw. auf den Datenaustausch mit dem Host beschränkt.

Im LAN oder abgeschottet

Virtuelle Netzwerke an physische Netzwerkkarten binden

Nur wenn Sie wollen, gelangt der Verkehr eines virtuellen Adapters über eine physische Netzwerkkarte vom Host ins LAN. Dann wirkt der Gast wie ein vollwertiger unabhängiger PC mit eigener MAC-Adresse und IP. Die Gäste treten parallel zum Host als eigenständige Clients auf. Alle Gäste können sich einen einzigen physischen Adapter teilen und trotzdem als separate Maschinen auftreten. Es lassen sich aber auch verschiedene VMs auf mehrere physische Adapter im Host verteilen, etwa zur besseren Auslastung. Bestimmte Protokolle verbinden die virtuellen Netzwerke transparent über die physischen Adapter des Hosts mit dem LAN-Switch.

Dem recht komplexen Thema Netzwerke habe ich gleich mehrere Workshops gewidmet:

- ▶ Wenn Sie einen schnellen Einstieg suchen, finden Sie ihn in *Teil 3, Kapitel 1, „Virtuelle Netzwerke Teil 1 – Schnellstart“*.
- ▶ In die Tiefen der Netzwerkkonfiguration gelangen Sie in *Teil 3, Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“*.
- ▶ Wenn Sie lieber die Theorie direkt an einem praktischen Beispiel nachvollziehen wollen, dann empfehle ich Ihnen *Teil 2, Kapitel 3, „Virtuelle DMZ mit Firewall und Webserver im Internet“*.

1.3.6 USB, Sound und Schnittstellen

Die Schnittstellen des Host-Rechners werden von den Produkten unterschiedlich gehandhabt. Dabei steht nicht immer die volle Funktionalität zur Verfügung, manche Schnittstellen werden gar nicht durchgereicht.

USB wird nur eingeschränkt unterstützt

Microsoft-Gäste können keine USB-Geräte verwenden, nur Tastatur und Maus am USB-Anschluss des Hosts werden in die VM durchgereicht. VMware bietet eine virtuelle USB1.1-Schnittstelle an, die allerdings auch nicht immer die volle Funktionalität bietet. Schauen Sie bitte unter „USB-Geräte im Gast verwenden“ nach, um Alternativen zu finden.

Sound funktioniert nicht immer ganz sauber

Die Desktop-Versionen haben eine virtuelle Soundkarte in den Gästen. Erwarten Sie aber keinen lupenreinen Klang, je nach Hardware und Leistung kann es zu Aussetzern und Rucklern kommen. Die Server verfügen, bis auf den VMware Server, über keine Sound-Ausgabe.

Parallele Schnittstelle und serielle Schnittstelle

Parallele und serielle Schnittstellen werden in die Gäste durchgereicht, wenn sie im Host physisch vorhanden sind. Ausgaben der seriellen Schnittstelle können sogar in eine Datei oder eine Named Pipe (nur Windows) umgeleitet werden. Microsoft kann nur die serielle, nicht die parallele Schnittstelle umleiten.

1.3.7 Physische SCSI-Geräte aus den Gästen ansprechen

Neben virtuellen SCSI-Platten können Sie unter VMware in einem Gast auch andere SCSI-Geräte direkt verwenden. So kann z.B. ein Streamer, ein Scanner oder ein MO-Laufwerk als so genanntes *Legacy-SCSI-Gerät* direkt aus einem Gast heraus angesprochen werden. Mehr dazu erfahren Sie im Platten-Workshop von Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“.

1.3.8 VGA, Tastatur und Maus zwischen Gast und Host teilen

Bei der Verwendung von Tastatur, Maus und Bildschirm gibt es ein paar Besonderheiten zu beachten, da sich alle Gäste die gleichen Eingabegeräte teilen müssen.

Tastatur und Maus im Gast verwenden

**Fokuswechsel
zwischen Gast
und Host**

Tastatur und Maus bereiten in einer VM keine Probleme. Die angeschlossenen Geräte des Host werden einfach durchgeschleift und können in der VM verwendet werden. Damit die Gäste aber wissen, wann Tastenanschläge und Mausbewegungen für Sie gelten und wann der Anwender auf dem Host oder in einem anderen Gast arbeitet, muss die VM erst den Fokus bekommen. Das kann automatisch erfolgen, sobald der Mauszeiger in ein Gastfenster geschoben wird. Je nach Einstellung ist manchmal auch erst ein Mausklick in das Fenster notwendig. Heraus aus einer VM kommt man oft nur mit einer bestimmten Tastenkombination. Unter VMware ist das **Strg** + **Alt**, unter Microsoft die rechte Taste **⇧** oder die rechte Taste **AltGr**.

Entscheidend für die Funktion von Maus und Tastatur sind die so genannten *VMware Tools* bzw. *Virtual Machine Additions*. Diese Tools können Sie in den Gästen installieren. Neben anderen Funktionen ermöglichen sie einen nahtlosen Übergang der Maus vom Host in die VM und umgekehrt (siehe Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“).



VGA-Adapter in einer VM

Als Grafikkarte erkennen die VMs unterschiedliche Adapter. VMware emuliert grundsätzlich erst einmal nur einen Standard-VGA-Adapter, wodurch anfangs nur eine geringe Auflösung und Farbtiefe in den Gästen zustande kommt. Erst mit der Installation der VMware Tools wird ein optimierter VMware VGA-Treiber eingerichtet, der dann volle Farbtiefe und beliebige Auflösungen ermöglicht. Virtual PC/Server emuliert gleich einen S3-Trio-Adapter, für den die meisten Betriebssysteme schon eigene Treiber mitbringen.

Hardware-Features, wie Grafikbeschleunigung, stehen in einer VM nur sehr eingeschränkt zur Verfügung. Aus diesem Grunde ist eine virtuelle Maschine zum Spielen oder zum Videoschauen, vor allem auf langsamen Wirten, eher schlecht geeignet. Hier kommt es je nach Anwendung und Hardware-Ausstattung immer auf einen Versuch an.

1.3.9 Nicht unterstützte Hardware in den Gästen

Alles, was bis jetzt nicht aufgezählt wurde, kann in einer VM auch nicht verwendet werden. Die Liste ist damit eigentlich lang, aber Sie haben Glück. Bei genauerer Betrachtung sind nur ganz wenige fehlende Komponenten wirklich problematisch.

PCI-Steckkarten sind im Gast nicht sichtbar

Fernsehkarten, schnelle Grafikkarten, Steuerungen, Messgeräte – egal was es ist –, Hardware, die in einem PCI-Slot steckt und nicht über USB oder seriell/parallel angeschlossen werden kann, ist in einer VM nicht sichtbar. Daran lässt sich auch nichts ändern. Einzige Ausnahme ist die *legacy SCSI*-Unterstützung von VMware, die es ermöglicht, auf Geräte zuzugreifen, die an einem SCSI-Controller des Hosts angeschlossen sind, etwa einen Streamer.

ISDN im Gast verwenden

Der Zugriff auf ISDN-Karten im PCI-Slot ist aus einer VM heraus ebenfalls nicht möglich. Mit USB-Adaptern funktioniert es oft, aber auch nicht immer. Die beste Lösung ist ein so genannter *LAN-CAPI* (auch als *virtual CAPI* bezeichnet). Dabei steckt die ISDN-Karte in einem physischen PC im LAN, oder ein Router ist direkt am ISDN

LAN-CAPI

angeschlossen. Die Kommunikation des ISDN-Anschlusses wird über das LAN an einen Treiber im Gast übermittelt, der dann die CAPI-Schnittstelle bereitstellt. Als Beispiel können die Router der Firma LANCOM oder auch Software, wie z.B. *AVM KEN!* der Firma AVM, zum Einsatz kommen.

<http://www.lancom.de>

<http://www.avm.de>

USB-Geräte im Gast verwenden

USB über LAN USB 2.0 wird ebenfalls in keinem Gast unterstützt. Und selbst unter dem von VMware angebotenen USB1.1 funktionieren lange nicht alle Geräte. Hier hilft nur Testen. Microsoft unterstützt überhaupt keine USB-Geräte in seinen Gästen. Als Ausweg bietet sich ebenfalls eine Lösung über das Netzwerk an, z.B. AnywhereUSB der Firma Digi, oder USB Server von Keyspan, womit mehrere USB-Schnittstellen über das LAN bereitgestellt werden können.

<http://www.digi.com>

<http://www.keyspan.com>

Dongles für die Lizenzierung von Software im Gast

Lizenzserver Dongles machen immer wieder Ärger in virtuellen Maschinen. Im PCI-Slot können sie nicht angesprochen werden, und auch manche USB-Dongles funktionieren nicht in einer VM. Hier können Sie bei negativen Tests nur beim Hersteller nach anderen Lösungen, etwa einem Lizenzserver, nachfragen. Ein Kopierschutz an der parallelen Schnittstelle bereitet erfahrungsgemäß die wenigsten Probleme.

Firewire wird in den Gästen nicht unterstützt

Der Vollständigkeit halber muss ich hier noch die fehlende Firewire-Unterstützung aller Produkte nennen. Hier hilft nur der Umweg über den Host und das Kopieren der Dateien (von externen Platten oder Videokameras) auf eine im LAN verfügbare Dateifreigabe.

1.3.10 Wie geht es jetzt weiter?

Sie kennen jetzt die grundsätzlichen Funktionen und wichtigen Begriffe virtueller Maschinen. Weiterhin können Sie die Hardware für Ihren Host auswählen. Im folgenden *Kapitel 2* erhalten Sie eine Entscheidungshilfe, welches der im Buch vorgestellten Produkte für Ihren Einsatzzweck in Frage kommt und welche Merkmale die Virtualisierer unterscheiden.

2 Das richtige Virtualisierungsprodukt für Sie

Welches der vorgestellten Virtualisierungsprodukte sollten Sie für Ihren Einsatzzweck wählen – Microsoft Virtual PC, den VMware Player oder VMware Workstation? Genügt Ihnen der kostenlose VMware Server für einen Einstieg als Testumgebung und auch längerfristig für produktive VMs, oder benötigen Sie den teuren VMware ESX Server? Was kann Microsoft Virtual Server besser als VMware? Ich werde Ihnen bei der Entscheidung helfen.

Den ESX Server mit allen Funktionen komplett zu beschreiben, könnte ein eigenes Buch problemlos füllen. Ich habe ihn deshalb in ein separates Kapitel ausgelagert (siehe *Teil 2, Kapitel 9, „VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2“*). Ich gehe hier nur auf die wichtigsten Funktionen von ESX Server 3 im Vergleich zu den anderen Produkten ein, als Entscheidungshilfe, ob Sie auf seine Features verzichten können oder nicht.

Mit den kostenlosen und unkompliziert einzurichtenden Produkten, wie dem VMware Server oder dem Microsoft Virtual Server, gelingt Ihnen ohne große Investition und ohne Hemmschwelle schon heute der Einstieg in die virtuelle Welt. Ein Wechsel auf den ESX Server ist später jederzeit möglich.

2.1 Anforderungen an virtuelle Maschinen für Testumgebungen oder Produktion

Jeder Anwenderkreis hat ganz spezielle Anforderungen an eine virtuelle Maschine. Ein Entwickler oder Techniker legt Wert auf größtmögliche Flexibilität in der Netzwerkkonfiguration und weiß z.B. die Möglichkeit von Wiederanlaufpunkten durch schnelle Sicherungen eines Gastes mittels Snapshots zu schätzen. Auch schnelles Klonen von Vorlagen und Zusammenfassen von VMs zu Teams können sehr nützliche Funktionen sein, etwa um ganze Testumgebungen gemeinsam zu starten oder mittels Suspend einzufrieren. Viele dieser Features werden aber von dem einen gefeiert und vom Nächsten als übertrieben abgetan, hier spielt sicher die Komplexität der Testszenarien und die Häufigkeit des Einsatzes eine große Rolle. Und eine Privatperson wird vor allem auf den Preis oder eine möglichst einfache Bedienung des Produktes achten.

Entwickler, Techniker oder Privatperson

Produktiver Einsatz

In einer Produktionsumgebung spielen dagegen vor allem solche Funktionen wie automatisches Herunterfahren und Starten der Gäste, Scripting zur Steuerung der VMs, Ressourcenkontrolle und eine zentrale Verwaltung die Hauptrolle. Je nach Größe der Umgebung entstehen dabei sehr unterschiedliche Anforderungen. Beispielsweise ist in einem hochverfügbaren Rechenzentrum die Fähigkeit des ESX Servers Gold wert, laufende Gäste für Wartungszwecke ohne Unterbrechung von einer Hardware auf die andere zu verschieben. In einem mittelständischen Betrieb mit eher knappen IT-Budget können dagegen zehn Minuten Ausfallzeit vielleicht verschmerzt werden, um einen virtuellen Server auf einem anderen Host manuell neu zu starten. Genauso muss man sich entscheiden, ob Clustering zur Ausfallsicherheit unbedingt benötigt wird oder ob nur unkritische Dienste virtualisiert werden sollen.

Sie sehen – es gibt keine uneingeschränkt empfehlenswerte Lösung. Dieses Kapitel legt das Augenmerk auf die herausragendsten Eigenschaften sowie Vorteile und Nachteile der Produkte, um Ihnen die Auswahl zu erleichtern. Letztendlich kommt es darauf an, was Sie mit virtuellen Maschinen erreichen wollen.



Viele Anregungen, was Sie mit virtuellen Maschinen realisieren können, erhalten Sie in den Praxis-Workshops von *Teil 2* des Buches.

Zum Ausprobieren und Vergleichen der verschiedenen Produkte können Sie manche davon nebeneinander auf dem gleichen Host betreiben. MS Virtual PC läuft parallel zur VMware Workstation und selbst den VMware Server können Sie parallel zum MS Virtual Server auf ein und demselben Wirt laufen lassen, um Features und Bedienung direkt nebeneinander zu vergleichen, was in der Entscheidungsphase sehr praktisch sein kann.

Aufteilung der Produkte in Gruppen für einen besseren Überblick

Es hat keinen Sinn, die Leistung von Virtual PC mit dem VMware Server oder gar mit den Funktionen des ESX Servers zu vergleichen. Die Zielgruppen und die Möglichkeiten der Produkte unterscheiden sich zu stark. Also ist mindestens eine Gruppierung der Produkte in Desktop-Produkte und Serverprodukte sinnvoll.

Desktop-Produkt oder Serverlösung

Beispielsweise spielen Microsoft Virtual Server und VMware Server als zentrale Testumgebung oder als Einstiegslösung in den produktiven Betrieb in der gleichen Liga. Microsoft Virtual PC eignet sich dagegen als Desktop-Produkt hauptsächlich für Test-, Demo- und Schulungsumgebungen, genau wie VMware Player und VMware Workstation.

Innerhalb der Serverprodukte existieren weitere Klassen. Der ESX Server tummelt sich in der Oberliga, keine der anderen Lösungen hält einem Vergleich stand. Aber bei einigen tausend Euro für einen ESX Server 3 mit allen lizenzierten Funktionen sollten Sie einfach wissen,

ob für fünf bis zehn Gäste nicht auch der kostenlose VMware Server oder Microsoft Virtual Server genügen. Selbst in der Produktion reicht der VMware Server lange aus, bevor der ESX Server notwendig wird.

2.2 Die Desktop-Produkte VMware Workstation, Player und MS Virtual PC

Die Desktop-Lösungen sind für den Einsatz auf einem PC gedacht, auf dem Sie auch die normale tägliche Arbeit verrichten. Sie arbeiten hauptsächlich in Testumgebungen oder um ein alternatives Betriebssystem, wie Linux, nebenbei laufen zu lassen. Man könnte sogar kleinere produktive Server, etwa für eine Webseite, unter diesen Virtualisierungen betreiben. Von der Stabilität und der Leistung geben sie das allemal her.

**Testumgebungen
und Schulungs-
räume**

Es fehlen aber einige sehr wichtige Funktionen, wie Scripting, Fernverwaltung, automatisches Starten und Herunterfahren der VMs oder die Möglichkeit, Gäste als Dienst laufen zu lassen. Natürlich gibt es bei Problemen keinen Support für einen produktiven Einsatz, und durch die kostenlosen Serverprodukte beider Hersteller ist diese Art der Verwendung der Desktop-Lösungen auch nicht zu begründen.

Im Gegensatz zu den weiter unten vorgestellten Serverprodukten sind die Desktop-Produkte vor allem schlanker. VMware Workstation hat zusätzlich einige besondere Funktionen, die vor allem in Testumgebungen sehr wertvoll sind und die der VMware Server nicht zu bieten hat.

2.2.1 VMware Player

Der VMware Player ist ein schlankes kostenloses Programm, um vorbereitete VMs laufen zu lassen, die mit den Vollprodukten erstellt wurden. Sie können weder neue VMs erstellen noch die Konfiguration vorhandener Gäste ändern. Trotzdem hat der Player ausreichendes Potenzial für einfache Einsätze, z.B. um ein oder zwei Linux-Instanzen als paralleles System unter Windows zu betreiben.

Mit dem Gastbetriebssystem in der VM können Sie unter dem Player uneingeschränkt arbeiten, es lässt sich nur keine neue Hardware hinzufügen. Auch für Software-Demos oder Produktschulungen ist der Player durchaus brauchbar und vor allem kostenlos. Mit etwas Willen zum Basteln sind viele weitere Möglichkeiten offen.

Workshops zum Player finden Sie hier:

- ▶ Teil 2, Kapitel 5, „*Virtuelle Umgebungen mit dem VMware-Player weitergeben*“
- ▶ Teil 2, Kapitel 6, „*Schulungs- oder Demo-Umgebung schnell aufgebaut*“.

Einsatzzweck von VMware Player

Virtuelle Maschinen weitergeben

- ▶ Vorbereitete VMs können kostenlos an Kunden und Mitarbeiter als Produktvorstellung oder als Entwicklungsumgebung weitergegeben werden.
- ▶ Einfache Testumgebungen für Software-Test, Demo und Schulung lassen sich mit dem Player aufbauen. Ein Webserver als Entwicklungs- oder Demo-Umgebung ist auf DVD oder auf dem Laptop immer mit dabei, ohne VMware Workstation-Lizenz.
- ▶ Linux lässt sich zum Ausprobieren auf Knopfdruck parallel auf dem Windows-PC betreiben, ohne extra Hardware anzuschaffen oder eine Dualboot-Konfiguration einzurichten.

Vorteile von VMware Player

- ▶ Der Player ist kostenlos ohne Registrierung im Internet verfügbar.
- ▶ Durch die extrem simple Installation, Oberfläche und Bedienung können Anwender mit einer vorbereiteten VM sofort loslegen, völlig ohne Einarbeitung, z.B. Kunden beim Evaluieren einer Software.
- ▶ Viele vorbereitete, sofort lauffähige VMs sind als Download auf der Webseite von VMware verfügbar, z.B. vorinstallierte Linux Distributionen. Diese VMs laufen auch unter allen anderen VMware-Produkten. Sie sparen sich damit die Installation eines neuen Gastsystems, wenn Sie nur einmal schnell die Funktionen testen wollen. (<http://www.vmware.com/vmtn/appliances/>)
- ▶ Der Player ist auf Linux und Windows-Hosts lauffähig.
- ▶ Mit dem kostenlosen Server oder der Evaluierungsversion der Workstation können Sie sehr komfortabel eine Anzahl Muster-VMs für den Player vorbereiten und später unbegrenzt weiterverwenden.

Nachteile von VMware Player

- ▶ Der Player hat eine sehr eingeschränkte Oberfläche mit minimalen Funktionen. Das kann aber auch ein Vorteil sein – z.B. in Schulungsumgebungen.
- ▶ Beim Player ist eine Neuerstellung oder Konfigurationsänderung von VMs nur über umständliches Editieren der textbasierten Konfigurationsdatei möglich. Mittlerweise gibt es aber bereits kostenlose Zusatztools zur Verwaltung der Konfiguration (siehe Teil 3, Kapitel 7, „*Nützliche Zusatzprodukte, Tools, Links und Tipps*“). Sie können auch den kostenlosen Server zum Erstellen von Mustervorlagen verwenden.

2.2.2 VMware Workstation 5.5/6

VMware Workstation ist ein reichhaltig ausgestattetes Produkt für Testumgebungen von der einfachen Probier-VM bis zu komplexen virtuellen Netzwerken. Dem professionellen Anwender werden viele Komfortfunktionen und viele wertvolle Features geboten. Für einen einfachen Linux-Gast als Zweit-PC zum Ausprobieren ist VMware Workstation allerdings überdimensioniert, dazu genügt bereits der Player.

Die Folgeversion Workstation 6 unterscheidet sich nur in Details von der Version 5.5, bietet aber einige interessante Neuerungen. Mehr Informationen finden Sie im Teil 3, Kapitel 8 - Aktualisierungen, Ergänzungen und Neuerungen.



Eines der besonderen Highlights ist beispielsweise die komfortable Snapshot-Funktion zur Sicherung und Wiederherstellung verschiedener Zustände einer VM auf Mausklick. Damit können Sie eine zerschossene Testumgebung mit einem Klick reparieren, indem Sie alle Änderungen seit dem letzten Snapshot einfach verwerfen. Bei der VMware Workstation können mehrere Zustandssicherungen hintereinander aufgehoben werden (*multiple Snapshots*). Sie können beispielsweise kurz zum Stand eines Gastes vor einem bestimmten Service-Pack zurückkehren, dort eine Software testen und wieder zum Stand mit dem installierten Service-Pack zurückwechseln, wo Sie sofort einen Vergleichstest anstellen können.

Workshops zur VMware Workstation finden Sie hier:

- ▶ Teil 2, Kapitel 1, „Eine Testumgebung mit VMware Workstation oder Server aufbauen“
- ▶ Teil 2, Kapitel 3, „Virtuelle DMZ mit Firewall und Webserver im Internet“.

Einsatzzweck der VMware Workstation

- ▶ Komplexe virtuelle Testnetzwerke lassen sich auf einem einzigen Host betreiben; bis hin zur Simulation langsamer Verbindungen und schlechter Leitungsqualität zwischen einzelnen VMs.
- ▶ Ein Client-Rollout kann mit vielen Wiederanlaufpunkten während der Software-Einrichtung vorbereitet werden. Geht ein Schritt schief, wird er einfach verworfen oder zu weiter zurückliegenden Zuständen gewechselt. Erst am Ende wird der endgültige Stand auf die Clients im LAN geklont.
- ▶ Software-Test-, Entwicklungs-, Demo- und Schulungsumgebungen lassen sich sehr komfortabel aufbauen und verwalten. Und der Helpdesk-Mitarbeiter hat unterschiedliche Systeme in verschiedenen Konfigurationen innerhalb von Sekunden laufen.

Umfangreiche virtuelle Netzwerke

Vorteile der VMware Workstation

- ▶ VMware ist auf Linux und Windows-Hosts lauffähig.
- ▶ VMs laufen auf mehreren CPUs oder Kernen (wenn vorhanden) zur Lastverteilung. VMware kann virtuelle Dualprozessoren zum Testen von entsprechender Software innerhalb einer VM bereitstellen. Als Gäste laufen auch 64-Bit-Betriebssysteme. Der Zugriff auf USB- und SCSI-Geräte aus den Gästen heraus ist möglich.
- ▶ Eine übersichtliche Verwaltung vieler VMs, Klone und Vorlagen ist in einer Favoritenliste mit Ordnern möglich.
- ▶ Mehrere Snapshots zur Sicherung mehrerer Wiederanlaufpunkte.
- ▶ Mit Linked Clones (Gäste basierend auf derselben Basis-VM) und Templates (Vorlagen) können Sie innerhalb von Sekunden mehrere Klone der gleichen Maschine anfertigen.
- ▶ Zusammenfassen von Maschinen zu Teams zum gemeinsamen Starten, Beenden und Suspend/Resume ist möglich.
- ▶ In den virtuellen Netzwerken der Teams können Geschwindigkeit und verlorene Pakete konfiguriert werden, um schlechte Leistungsqualitäten zu simulieren.
- ▶ Der Mitschnitt von Videos (auch Screenshots) innerhalb der VM ist möglich, auch das ist ein Alleinstellungsmerkmal der VMware Workstation.

Nachteile der VMware Workstation

- ▶ Die Vorteile sind manchmal auch Nachteile – gerade Einsteiger werden oft überfordert von der Funktionsvielfalt der VMware Workstation. Da wirkt Virtual PC eher aufgeräumt. Aber man muss ja nicht gleich alle Funktionen von VMware ausprobieren.
- ▶ VMware Workstation ist ein kostenpflichtiges Produkt. Über 150 Euro sind zu viel, wenn Sie einfach nur ein Linux in einer VM ausprobieren wollen. Für Profis ist die Workstation aber jeden Cent wert!
- ▶ Keine Unterstützung von OS/2 als Gastsystem.

2.2.3 Microsoft Virtual PC 2004 SP1 und 2007

Microsoft Virtual PC 2004 SP1 ist ein ausreichendes und schlankes Produkt für Test und Demo. Es bietet nicht den großen Funktionsumfang wie VMware Workstation 5.5, ist dadurch aber übersichtlicher. Die wichtigsten Funktionen für Testumgebungen sind vorhanden. Mehrere Wiederanlaufpunkte zum Verwerfen von Änderungen und fehlgeschlagenen Tests müssen etwas umständlich mit so genannten Differenzplatten nachgebildet werden, platz- und zeitsparendes Klonen ist ebenfalls mit Differenzplatten möglich.

Die Folgeversion Virtual PC 2007 unterscheidet sich nur in Details von der Version 2004, mehr Informationen finden Sie im Teil 3, Kapitel 8 - Aktualisierungen, Ergänzungen und Neuerungen.



Auf dem Macintosh mit PowerPC oder für OS/2-Gäste bleibt unter den vorgestellten Produkten keine andere Wahl, da es nur von Virtual PC eine Version für PowerPC gibt. Einen Workshop zu Virtual PC finden Sie hier:

Teil 2, Kapitel 2, „Mobile virtuelle Entwicklungs- und Demo-Umgebung mit Virtual PC“

Einsatzzweck von Microsoft Virtual PC

- ▶ Software-Test, Entwicklung, Demo- und Schulungsumgebungen, Helpdesk usw.
- ▶ Linux oder auch OS/2 parallel zu Windows oder MAC OS betreiben.

Vorteile von Microsoft Virtual PC

- ▶ Virtual PC SP1 ist seit Juli 2006 kostenlos verfügbar.
- ▶ Die Oberfläche ist durch eher wenige, aber ausreichende Features recht übersichtlich.
- ▶ OS/2 ist als Gastsystem möglich, und für MAC OS als Host-System ist eine spezielle Version von Virtual PC verfügbar.

Testumgebungen oder Produkt-Demos

Nachteile von Microsoft Virtual PC

- ▶ Alle VMs laufen parallel auf der gleichen CPU, Multiprozessoren bleiben ungenutzt.
- ▶ Die Verwaltung von mehreren Wiederanlaufpunkten nur mit manuell einzurichtenden Differenzplatten ist möglich, was bei häufiger Nutzung etwas umständlich ist.
- ▶ Die Gäste verfügen über kein USB, kein SCSI, keine 64-Bit-Unterstützung und keine virtuellen Dual-CPU's.
- ▶ Gegenüber VMware bietet Virtual PC nur relativ einfache Netzwerkfunktionen, z.B. nur ein einziges internes abgeschottetes Netzwerk. Das ist für kleine Netze aber noch ausreichend.
- ▶ Ein Linux-Host wird nicht unterstützt (Linux-Gäste laufen aber unter Virtual PC).

2.3 Die Hosted Server-Produkte VMware Server und Microsoft Virtual Server

Hosted bedeutet, die Virtualisierer benötigen ein Wirtsbetriebssystem, auf dem sie installiert sind. Die Desktop-Produkte sind natürlich auch *Hosted*, aber ich zähle sie nicht zu den Servern, deshalb die Trennung. Nur der ESX Server läuft als einziges im Buch vorgestelltes Produkt direkt auf der Hardware und gehört deshalb nicht in die Kategorie *Hosted-Produkte*.

Alle Serverprodukte verfügen, im Gegensatz zu den Desktop-Produkten, über eine Remote Console, mit der sie vom LAN aus vollständig bedient werden können. Weitere Funktionen kommen hinzu, z.B. automatisches Starten und Herunterfahren der Gäste zusammen mit dem Wirtssystem sowie Scripting-APIs zum Steuern der Gäste aus eigenen Programmen und Skripten. Die virtuellen Maschinen laufen unter den Servern als Dienste im Wirtssystem. Im Gegensatz zu den Desktop-Produkten laufen die Gäste dadurch auch, wenn kein Benutzer an der Konsole des Host-Servers angemeldet ist. Und die Rechte zum Zugriff auf die VMs lassen sich feiner verwalten als unter den Desktop-Lösungen.

Als kostenlose Desktop-Lösung

Für Testumgebungen auf dem Desktop-PC sind die Serverprodukte etwas voluminös, wobei das bei einem modernen Rechner heute kein Problem mehr sein sollte. So kann der kostenlose VMware Server durchaus auch als Ersatz für die kostenpflichtige Workstation dienen, wenn Sie auf Komfortfunktionen wie multiple Snapshots verzichten können. Die VMs des Servers sind kompatibel zur Workstation und laufen genauso im Player.

Auch der Microsoft Virtual Server kann zu Testzwecken unter Windows XP Professional betrieben werden und dort als Ersatz für Virtual PC dienen. Allerdings ist die Bedienung von Virtual Server teilweise etwas umständlich, vor allem für häufig umzukonfigurierende Testumgebungen.

2.3.1 VMware Server 1.0

Der VMware Server ist der direkte Nachfolger des ehemals kostenpflichtigen GSX Servers. Er ist eine sehr gute Virtualisierungslösung für alle Einsatzzwecke von Test bis Produktion. Der Server wird als Einstiegslösung vermarktet, kann aber in kleineren bis mittleren Umgebungen lange alle Ansprüche erfüllen. Zusammen mit Linux als Host ergibt sich eine softwareseitig komplett kostenlose Virtualisierungslösung.

Workshops zum VMware Server finden Sie in folgenden Kapiteln:

- ▶ Teil 2, Kapitel 1, „Eine Testumgebung mit VMware Workstation oder Server aufbauen“
- ▶ Teil 2, Kapitel 3, „Virtuelle DMZ mit Firewall und Webserver im Internet“
- ▶ Teil 2, Kapitel 4, „Linux-Host mit VMware Server und Integration ins Windows-Netz“
- ▶ Teil 2, Kapitel 8, „Cluster mit VMs und einem iSCSI Target als externem Speicher“.

Einsatzzweck von VMware Server

- ▶ Kleinere Produktivumgebungen.
- ▶ Testumgebungen auf einem zentralem Host mit Remote-Zugriff von den Testplätzen. Das entlastet den einfachen Arbeitsplatz-PC des Mitarbeiters, da die VMs auf einem anderem leistungsfähigen Rechner laufen. Außerdem werden die Gäste zentral für alle Mitarbeiter bereitgestellt.
- ▶ Der Server bietet sich teilweise als Ersatz für die VMware Workstation auf dem Desktop an, hat aber weniger Komfortfunktionen (keine linked Clones, keine Templates und Teams, keine Videoaufzeichnung, nur einen Snapshot).
- ▶ VMs lassen sich mit dem Server komfortabel für den Einsatz im Player erstellen und vorbereiten.

Produktion oder zentrale Testumgebung

Vorteile von VMware Server

- ▶ Kostenlos verfügbar.
- ▶ Zwei virtuelle CPUs können an die Gäste durchgereicht werden, und eine Unterstützung für 64-Bit-Gäste ist vorhanden, das bietet unter den vorgestellten Produkten nur VMware.
- ▶ Die komfortable durchdachte Remote-Konsole aus einem Guss ähnelt stark der Oberfläche der VMware Workstation. Das erleichtert den Umstieg oder die Parallelnutzung.
- ▶ Eine Anbindung an das hostübergreifende zentrale Managementprodukt von VMware, das Virtual Center, ist möglich, zurzeit aber nur in der Virtual Center-Version 1.4 und noch nicht in der Version 2, die für den ESX Server 3 notwendig ist (siehe auch Teil 2, Kapitel 9 und <http://www.vmware.com/products/server/vc14.html>). Virtual Center kann Hosts und VMs übersichtlich unter einer einheitlichen Oberfläche verwalten, überwachen und steuern. Sie benötigen dazu einen kostenpflichtigen *Virtual Center Management Server* und eine ebenfalls kostenpflichtige Lizenz für den *Virtual Center Agent* für jeden einzubindenden VMware Server.

VMware Virtual Center

- Einmal installierte Gäste von VMware Server lassen sich ohne weiteres auf den ESX Server und damit auf Datacenter-Niveau migrieren. Das ist ein sehr wichtiger Punkt. Dadurch können Sie beruhigt mit dem kostenlosen Server einsteigen. Wenn er nicht mehr genügt, lässt er sich auf den ESX Server erweitern.

Nachteile von VMware Server

- Es existiert keine automatische Failover-Funktion (automatisches Übernehmen von Gästen auf andere Hardware) für den Host. Fällt er aus, können VMs nur manuell wieder auf einem anderen Server gestartet werden. Als Alternative lassen sich Cluster-Anwendungen direkt in jedem Gast einrichten, z.B. die Microsoft Cluster-Dienste mit Windows Server 2003 Enterprise Edition. Damit ist eine Ausfallsicherung zwischen virtuellen Maschinen über verschiedene Hosts möglich, siehe *Teil 2, Kapitel 8, „Cluster mit VMs und einem iSCSI Target als externem Speicher“*).

2.3.2 Microsoft Virtual Server 2005 R2

Der Virtual Server ähnelt vom Einsatzzweck und von der Zielgruppe sehr stark dem VMware Server, im Prinzip gilt alles dort Gesagte auch hier. Von Testumgebungen bis zur Produktion deckt Virtual Server ein breites Spektrum ab. Virtual PC und Virtual Server sind zwar vom selben Hersteller, aber von der Oberfläche und vom Konzept her grundverschieden, so dass ein Umstieg etwas Einarbeitung erfordert.

Einbindung in Microsoft Cluster-Dienste

Eine Besonderheit von Virtual Server ist die Möglichkeit, alle VMs eines Hosts in die Microsoft Cluster-Dienste einzubinden. Damit ist ein Failover von einem Host auf einen anderen möglich, ein so genannter *Hostcluster*. Das kann der VMware Server nur mit Fremdanbieterlösungen oder durch selbst konfigurierte Skripte, offiziell wird diese Funktion von VMware nur für den ESX Server angeboten.

Weiterhin kann Virtual Server zur Laufzeit die CPU-Auslastung der Gäste steuern, um z.B. einer VM mehr Performance bereitzustellen oder um einen leistungshungrigen Gast etwas zu begrenzen. Workshops zum Microsoft Virtual Server 2003 R2 finden Sie hier:

- *Teil 2, Kapitel 7, „Eine virtuelle Pilotumgebung als Testfeld für produktive Einsätze“*
- *Teil 2, Kapitel 8, „Cluster mit VMs und einem iSCSI Target als externem Speicher“*.
- *Teil 2, Kapitel 3, „Virtuelle DMZ mit Firewall und Webserver im Internet“* (die Umsetzung von VMware auf Virtual Server wird beschrieben)

Einsatzzweck von Microsoft Virtual Server

- ▶ Kleinere und mittlere Produktivumgebungen.
- ▶ Der Server kann auch in Testumgebungen als zentraler Host mit Remote-Zugriff von den Testplätzen eingerichtet werden. Das entlastet die Arbeitsplätze, da diese nur noch den Bildschirm der VMs bedienen und selbst keine Gäste laufen lassen.

Vorteile von Microsoft Virtual Server

- ▶ Kostenlos verfügbar.
- ▶ Die CPU-Leistung kann für einzelne Gäste prozentual oder mit Maximalwerten während der Laufzeit zugeteilt werden, das kann VMware erst ab dem teuren ESX Server.
- ▶ Anbindung an Active Directory (Nutzerverwaltung) und Microsoft Operations Manager (Monitoring) ist möglich.
- ▶ Die Host-Cluster-Funktion ermöglicht die Einbindung aller VMs eines Hosts in die Microsoft Cluster-Dienste (erfordert einen Windows Server 2003 Enterprise Edition als Host und iSCSI als externen Speicher). Bei Host-Ausfall werden die Gäste auf dem anderen Knoten neu gestartet (*Failover*). Bei geplanten Wartungsarbeiten können Gäste ohne Ausfall oder Absturz fast in Echtzeit auf den anderen Cluster-Knoten verschoben werden, dazu wird mittels Suspend der Status des Gastes gesichert und auf dem anderen Host wiederhergestellt. Das minimiert die Ausfallzeit.

Zusätzlich zur Host-Cluster-Funktion sind Cluster zwischen VMs auf unterschiedlichen Hosts genauso wie beim VMware Server möglich (siehe Workshop im *Teil 2, Kapitel 8*).



Nachteile von Microsoft Virtual Server

- ▶ Die Installation ist nicht auf einem Linux-Host möglich (Linux-Gäste sind aber möglich).
- ▶ VMware Server unterstützt keine 64-Bit-Gäste und reicht immer nur eine virtuelle CPU durch.
- ▶ Es ist kein Nachfolgeprodukt auf Datacenter-Niveau für eine spätere Erweiterung verfügbar (Migration der Gäste auf VMware ESX Server ist aber möglich).
- ▶ Teilweise etwas umständliche Bedienung, vor allem beim Zugriff auf das Dateisystem des Hosts zur Auswahl von VMs, virtuellen Platten oder ISO-Images (siehe auch *Teil 1, Kapitel 4*, zur Bedienung der Produkte).

System Center Virtual Machine Manager

Derzeitig bereits als Beta verfügbar, hat Microsoft eine zentrale Komponente zur Bereitstellung virtueller Maschinen und auch zur Übernahme physischer Maschinen angekündigt, den *System Center Virtual Machine Manager*:

<http://www.microsoft.com/systemcenter/scvmm/>

2.4 Das Data Center-Produkt VMware ESX Server 3

Der VMware ESX Server ist das einzige Produkt im Buch, das kein Wirts-OS benötigt. Der ESX bringt einen eigenen optimierten Kernel, eigene Treiber und eine eigene Konsole zur Verwaltung mit. Durch das fehlende Host-Betriebssystem muss sich der Administrator unbedingt auf dem ESX Server einarbeiten und kann nicht auf Erfahrungen mit Windows zurückgreifen. Teilweise ist Linux-Know-how notwendig. Im praktischen Einsatz wird der ESX Server fast immer zusammen mit Virtual Center installiert, zusammen die so genannte *Virtual Infrastructure*.



Trotz immer wieder auftauchender Behauptungen und Diskussionen – der ESX Server läuft nicht auf Linux! Das RedHat-Linux in der so genannten Service-Konsole dient lediglich als Verwaltungssystem und Boothilfe. Die Konsole läuft nach dem Start als eine Art virtueller Maschine mit Schnittstellen zum eigentlichen Kernel. Sie ist ebenfalls nur ein Gast unter der Kontrolle des VMware Kernels.

Eine detaillierte Einführung und eine ausführliche Beschreibung der weiter unten nur kurz angerissenen Begriffe und Funktionen sowie einen Workshop zum schnellen Einstieg mit dem aktuellen ESX Server 3 finden Sie im *Teil 2, Kapitel 9, „VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2“*.

Der VMware ESX Server ist derzeitig eine der besten Virtualisierungslösungen für den Produktiveinsatz. Für einfache Testumgebungen ist er allerdings Overkill und auch etwas unhandlich in der Bedienung für Einsteiger. Ich stelle Ihnen zusätzlich zu den anderen Produkten die wichtigsten Funktionen des ESX Servers vor, um einen Überblick zu schaffen, ob Sie den ESX für Ihre Ansprüche unbedingt brauchen oder ob die kostenlosen Alternativen noch ausreichen.

Einsatzzweck von VMware ESX Server

ESX 3 als High-End-Produkt bis zum großen Rechenzentrum

- Für Produktivumgebungen mit vielen Hosts und wenn nötig Hunderten VMs im unternehmenskritischen Einsatz ist der ESX Server erste Wahl.

- ▶ Für große zentrale Testumgebungen mit Hunderten VMs für Dutzende Mitarbeiter können mehrere ESX Server unter der Verwaltung von Virtual Center oder VMware Lab Manager ebenfalls interessant werden.
- ▶ Ein weitere Einsatzzweck ist das zentrale Hosten von Desktops, auf welche die Nutzer mittels Thin Clients über Remote-Desktop-Sitzungen zugreifen (*Abschnitt 2.6.3, „VMware Virtual Desktop Infrastructure (VDI)“*).

Vorteile von VMware ESX Server

- ▶ Ein optimierter Kernel läuft direkt auf der Hardware, das ergibt eine bessere Performance. Ein weiterer wichtiger Aspekt ist die direkte Hardware-Kontrolle durch spezielle VMware-Treiber und damit viele erweiterte Funktionen, z.B. Adapter-Teaming.
- ▶ In den Gästen können bis zu vier Prozessoren und bis zu 16 GB RAM zugewiesen werden.
- ▶ Fein abgestufte Ressourcenkontrolle zur Laufzeit für RAM, CPU, I/O, Netzwerkkarten ist möglich.
- ▶ Die zentrale Verwaltung und Überwachung aller Hosts und Gäste mit VMware Virtual Center ist für ganze Farmen von Hosts möglich.
- ▶ Es ist möglich, laufende Gäste ohne Unterbrechung von einem Host auf einen anderen mit der Erweiterung *VMotion* zu verschieben (benötigt externen Speicher im SAN oder NAS und Virtual Center). *VMotion* kann mit dem ESX Server 3 und Virtual Center 2 auch automatisiert zur Lastverteilung und für Failover genutzt werden (neue Funktionen *DAS* und *DRS* der Virtual Infrastructure 3 – siehe auch *Teil 2, Kapitel 9*).
- ▶ Cluster sind in allen Konstellationen zwischen physischen Maschinen und VMs, zwischen VMs auf dem gleichen Host und auch über Servergrenzen hinweg sowie zwischen ganzen Hosts durch den gemeinsamen Zugriff auf LUNs in einem SAN möglich. Diese Flexibilität im Clustering bietet nur der ESX Server.

Nachteile von VMware ESX Server

- ▶ Hoher Preis. Auch die versteckten Folgekosten sollten Sie nicht übersehen, denn viele der besonderen Funktionen, wie das Verschieben laufender VMs, funktionieren nur mit externem Speicher. Der ESX 2 ließ für die SAN-Anbindung bisher nur Fibre-Channel zu, mittlerweile wird vom ESX 3 aber auch das preiswertere iSCSI oder ein NAS unterstützt.
- ▶ Der ESX Server läuft nur auf Hardware, für die VMware Treiber liefert. Die meisten üblichen Serverkomponenten werden zwar unterstützt, mit preiswerten IDE- oder SATA-Platten kann im Host aber beispielsweise nicht gearbeitet werden; wobei das in Produktionsumgebungen auch nicht empfehlenswert ist.

- Zusätzliches Know-how für eine sichere Administration des ESX Servers und seiner Komponenten ist unbedingt notwendig. Für die Hosted-Produkte genügen gute Kenntnisse des Wirtsbetriebssystems.

Eines sollte natürlich klar sein: Alle genannten Nachteile sind für die Zielgruppe des ESX völlig irrelevant. Firmen, die viele produktive unternehmenskritische Server virtualisieren wollen, kommen um eine Virtualisierungslösung in der Klasse des ESX Servers nicht herum.

2.5 Vorteile und Nachteile eines Host-Betriebssystems als Zwischenschicht

Wir sollten zum Abschluss noch einen kurzen Blick darauf werfen, welche Vorteile ein Produkt hat, das auf einem Wirts-OS aufsetzt (z.B. Microsoft Virtual Server oder VMware Server), bzw. welche Vorteile sich ergeben, wenn der Virtualisierungslayer direkt auf der Hardware angesiedelt ist, wie beim VMware ESX Server.

2.5.1 Direkter Hardware-Zugriff ohne Wirts-OS

Optimale Ausnutzung der Hardware

Ein Vorteil des ESX Servers liegt in der besseren Performance, durch den optimierten und direkten Hardware-Zugriff. Ein weiterer Aspekt wird erst auf den zweiten Blick deutlich: Durch die speziellen eigenen Treiber, welche die Hardware direkt kontrollieren, können Funktionen realisiert werden, für die auf jedem Host-Betriebssystem zusätzlicher Aufwand notwendig wäre. *Netzwerkarten-Teaming* (Bündelung von Adaptern zur Ausfallsicherheit oder Performancesteigerung), Unterstützung von *VLANs* (virtuelle separate Netzwerke auf dem gleichen physischen Netzwerk) oder *Multipathing* (mehrere redundante Wege zum externen Speicher zwecks Ausfallsicherheit) sind nur einige Funktionen, die beim ESX Server bereits als Grundfunktionen integriert sind, ohne dass Sie auf zusätzliche Software angewiesen sind.

Sie können beispielsweise zwei physische Netzwerkkarten auf dem ESX Server einem virtuellen Netzwerk zuweisen. Fällt ein Adapter oder der Link aus, kommunizieren alle Gäste weiterhin ohne Unterbrechung über den zweiten Adapter. Die Verwaltung übernimmt VMware ESX Server, die Gäste müssen dazu keinerlei Teaming unterstützen. Die eigenen Treiber des ESX verlangen aber nach zertifizierter Hardware, da VMware nicht für alle Hersteller und Komponenten Treiber liefert. So laufen nicht jeder SCSI-Controller und nicht jede Netzwerkkarte unter dem ESX Server.

2.5.2 Umweg über ein Wirts-OS

Der Vorteil der Hosted-Produkte ist dagegen die sehr gute Hardware-Unterstützung, da prinzipiell jede Hardware verwendet werden kann, für die das Host-System, also Windows oder Linux, Treiber hat. Beahlt wird das mit etwas schlechterer Performance, weil jede Aktion eines Gastes neben dem Virtualisierungslayer zusätzlich noch das Host-System passieren muss. Bei aktueller Hardware spielt dieser Nachteil aber eine immer geringere Rolle, VMs laufen auch unter dem VMware Server oder Microsoft Virtual Server ausreichend schnell. Für Funktionen wie Adapterteaming müssen allerdings extra Lösungen gesucht werden, die meist abhängig von der verwendeten Hardware sind, z.B. spezielle Netzwerkkartentreiber.

**Einfacher
Umgang und
gute Hardware-
Unterstützung**

2.5.3 Aspekte der Bedienung

Ein weiterer Aspekt ist der Umgang mit den Produkten. Zur Bedienung von VMware Server oder MS Virtual Server genügen, neben Kenntnissen zum Virtualisierungsprodukt, gute Kenntnisse des Wirtsbetriebssystems. So ist z.B. das Kopieren einer virtuellen Platte unter Windows kein Problem, oder die gewohnte Sicherungslösung kann weiterverwendet werden.

Beim ESX Server muss man sich erst tiefer in alle Funktionen und in die Bedienung einarbeiten. Für unerfahrene Nutzer ist das ein deutlicher Mehraufwand, hier kann bereits das Kopieren einer Datei von einer Windows-Maschine auf den ESX Host zum ersten größeren Problem werden. Schon allein deshalb kann für den Einstieg in die Virtualisierung in kleineren bis mittleren Umgebungen der VMware Server oder der Microsoft Virtual Server die bessere Lösung sein. Ein Umstieg ist später jederzeit möglich.

2.6 Die weiteren VMware-Produkte im Überblick

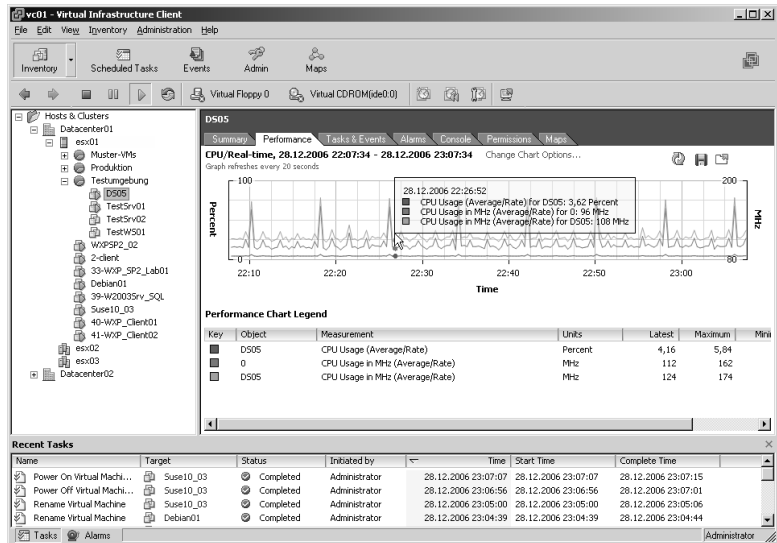
VMware bietet weitere spezielle Produkte und Lösungen, die ich Ihnen hier zusätzlich vorstelle, die aber im Buch, bis auf *Virtual Center 2*, nicht weiter behandelt werden.

2.6.1 VMware Virtual Center

VMware Virtual Center ist die übergreifende Managementlösung von VMware. Ein *Virtual Center Management Server* integriert einzelne Hosts und fasst sie zu einem *Datacenter* zusammen. Er überwacht und verwaltet alle Hosts und die virtuellen Maschinen zentral in einer Datenbank, der Administrator greift über eine grafische Oberfläche, den *Virtual Infrastructure Client*-Zugriff, darauf zu. Auf jedem Host wird ein *Virtual Center Agent* zur Anbindung an den Management-Server benötigt.

Zentrale Verwaltung und Überwachung

Abbildung 2.1:
VirtualCenter
verwaltet mehrere
Hosts und VMs
unter einer einheit-
lichen Oberfläche.



Virtual Center existiert in zwei Versionen:

- *VMware Virtual Center 1.4* unterstützt den VMware Server und den noch häufig eingesetzten ESX Server 2.x, die Vorgängerversion von ESX Server 3.
- *VMware Virtual Center 2* unterstützt dagegen den aktuellen ESX Server 3, aber noch keinen VMware Server. Ein Mischbetrieb beider Versionen ist nicht möglich.

Der ESX Server kann erst zusammen mit Virtual Center seine vollen Möglichkeiten entfalten, wie das Verschieben laufender VMs (*VMotion*) oder Cluster-Funktionen. Die meisten ESX Server-Installationen existieren unter der Verwaltung von Virtual Center. Virtual Center 2 und ESX Server 3 werden zusammen als *VMware Infrastructure 3* bezeichnet.

Der VMware Server kommt dagegen lange Zeit auch sehr gut ohne Virtual Center aus. Die herausragenden Funktionen der Kombination ESX Server und Virtual Center, wie *VMotion* und Host-Cluster, funktionieren beim VMware Server sowieso nicht. Und die zentrale Verwaltung aller virtuellen Maschinen mitsamt schneller Bereitstellung mittels Templates (Vorlagen-VMs) sowie das übersichtliche Verschieben von VMs zwischen einzelnen Hosts (allerdings nur im abgeschalteten Zustand) wird erst bei mehreren VMware Servern interessant.

Die Frage ist, ob der hohe Preis eines Virtual Center Management Servers und die zusätzlichen Kosten der benötigten Agenten für jeden einzelnen eingebundenen VMware Server so richtig mit dem kostenlosen Angebot des VMware Servers zusammenpassen. Wer bereit ist, Virtual Center zu kaufen, überlegt sich eher, ob er nicht auch gleich den ESX Server einsetzt, der die Möglichkeiten von Virtual Center wesentlich besser nutzt und den Agenten bereits kostenlos integriert hat.

Dagegen kann für Nutzer mit vorhandenem ESX Server 2.5 und Virtual Center 1.3 (Upgrade auf 1.4 möglich) die Einbindung zusätzlicher VMware Server interessant sein, z.B. für Testzwecke oder als preiswerte Kapazitätserweiterung. Es fallen dann nur die Kosten für die Agenten an.

Mehr zur Kombination von ESX Server 3 und Virtual Center 2 erfahren Sie in Teil 2, Kapitel 9, „*VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2*“.

2.6.2 VMware ACE (Assured Computing Environment)

Mit *VMware ACE* ist es möglich, virtuelle Maschinen als MSI-kompatible Pakete zu verpacken und samt Laufzeitumgebung an Desktop-PCs über das LAN oder auf DVD zu verteilen. Sie übertragen auf die Clients vorgefertigte und verwaltete virtuelle Systeme, mit denen der Endanwender arbeitet, als wären sie direkt auf dem lokalen PC installiert. Beispielsweise kann auf einem Laptop eine vorkonfigurierte und abgeschottete VM mit einem eingerichteten VPN-Client für einen sicheren Zugriff auf das Firmennetzwerk dienen.

VMs als fertige Pakete verteilen

Das Prinzip von *VMware ACE* ist ähnlich dem *VMware Player*, Sie verteilen also keine Software-Pakete, wie beispielsweise mit Novell ZEN-Works oder Microsoft SMS, sondern gleich komplette virtuelle Maschinen samt Betriebssystem. Im Gegensatz zum einfachen *VMware Player* bietet *VMware ACE* wesentlich mehr Verwaltungs- und Konfigurationsoptionen. Virtuelle Umgebungen lassen sich damit ganz individuell für jeden Benutzer konfigurieren. Weiterhin können diese Umgebungen jederzeit wieder zurückgesetzt und auf einen sauberen Grundzustand gebracht werden. Es existiert eine Rechteverwaltung, und der Zugriff auf den Host oder auf Geräte, wie USB, lässt sich einschränken.

Der Nachteil ist, dass für jede verteilte VM eine Betriebssystemlizenz benötigt wird, zusätzlich zur Lizenz des Rechners, auf dem der Gast läuft und dass der lokale PC über genügend Leistung verfügen sollte.

<http://www.vmware.com/products/ace/>

<http://www.vmware.com/products/ace/faqs.html>

2.6.3 VMware Virtual Desktop Infrastructure (VDI)

VMware Virtual Desktop Infrastructure verfolgt einen recht neuen Ansatz. Während mittels *VMware ACE* komplette Umgebungen als Gäste auf den lokalen PCs laufen, werden beim *Virtual Desktop* virtuelle Maschinen auf einem zentralen Host vorgehalten. Beispielsweise laufen mehrere Windows XP-Gäste auf einem zentralen ESX Server. Der Anwender verbindet sich auf einen dieser Gäste mittels Remote-Desktop-Protokoll (RDP) und hat das virtuelle System für

Virtuelle Bürocomputer mit Remote-Zugriff

sich allein zur Verfügung. Als Clients können normale Desktop-PCs oder schlanke Terminals, so genannte Thin Clients, dienen. Das sind kleine lüfterlose Geräte mit schlankem Betriebssystem, oft Linux oder Windows CE, die nur zum Remote-Zugriff dienen.

Der Vorteil gegenüber normalen Desktop-PCs ist die zentrale Verarbeitung auf einem leistungsstarken Host, wodurch auch leistungsschwache Client-PCs mit aktuellen Anwendungen arbeiten können. Neue virtuelle Maschinen für weitere Benutzer können in Sekunden von Vorlagen erzeugt werden, und die individuellen VMs der Anwender lassen sich einfach sichern oder auf einen definierten Grundzustand zurücksetzen.

Konkurrenz zum Terminalserver

VMware dringt damit ins angestammte Gebiet der Terminalserver vor. So interessant wie sich dieser Ansatz der *Virtual Desktop Infrastructure* auch anhört, so hat er doch einige Nachteile. Zum einen muss neben den teuren zentralen Hosts trotzdem für jeden Anwender ein Client-Gerät angeschafft werden. Leider liegen die Preise dieser Geräte oft nahe denen preiswerter Bürocomputer.

Weiterhin entsteht, im Gegensatz zu einem Terminalserver, ein großer Overhead, da für jeden Anwender ein eigener Gast mit vollständigem Windows XP laufen muss, auch wenn der Anwender nur eine Textverarbeitung benötigt. Ein Terminalserver, benötigt dagegen nur eine Betriebssysteminstanz für viele Anwender und Applikationen.

Ob sich der Ansatz der *VMware Virtual Desktop Infrastructure* gegen etablierte Lösungen, wie Terminalserver mit Citrix Metaframe, durchsetzen kann, bleibt abzuwarten. Ein Vorteil der VMware-Lösung ist die gegenseitige Abschottung der einzelnen Gäste, jeder Nutzer hat damit seine eigene Umgebung und eigene Applikationen. Auf Terminalservern machen die vielen parallel installierten Programme dem Admin oft zu schaffen. Auch die Ausnutzung von Snapshots und Klonen zum schnellen Zurücksetzen und Vervielfältigen von Gästen stellen weitere Vorteile der VMware-Lösung dar.

<http://www.vmware.com/solutions/desktop/vdi.html>

2.6.4 VMware Technology Network (VMTN) als Jahresabo aller Produkte für Entwickler

Die so genannte VMware Technology Network (VMTN) Subscription soll es vor allem Entwicklern ermöglichen, alle Produkte von VMware zu evaluieren oder für Produktentwicklungen zur Verfügung zu haben. Für einen jährlichen Preis pro Benutzer (etwa 250 Euro) erhalten Sie Versionen der aktuellen Produkte, auch VMware ESX Server 3 mit Infrastructure 3, P2V-Assistent und VMware Workstation, zum nichtproduktiven Gebrauch für Entwicklung und Test.

<http://www.vmware.com/products/vmtn/>

2.6.5 VMware Virtual Appliance Marketplace – vorkonfigurierte lauffähige VMs zum Herunterladen

VMware bietet auf seiner Webseite eine Börse, wo es mittlerweile einen großen Pool kostenloser Virtual Appliances gibt. Das sind virtuelle Maschinen samt Software wie Firewalls, Webserver oder Demoverversionen kommerzieller Produkte. Die VMs laufen sofort unter den VMware-Produkten. Sie bieten fertige Lösungen ohne Installationsaufwand zum schnellen Ausprobieren.

<http://www.vmware.com/vmtn/appliances>

2.6.6 VMware Virtual Lab Manager 2.4 – Verwaltung von Testumgebungen

Das neueste VMware-Produkt Virtual Lab Manager dient zur komfortablen Verwaltung von Test-, Demo- und Schulungsumgebungen. Detaillierte Informationen finden Sie im Teil 3, Kapitel 8 – Aktualisierungen, Ergänzungen und Neuerungen.

2.6.7 VMware-Hilfsprogramme wie P2V, Converter oder Importer

Weiterhin liefert VMware einige Hilfsprogramme, etwa zum Übernehmen physischer Maschinen in eine VM. Auf diese Programme gehe ich im Buch in den entsprechenden Kapiteln ein.

<http://www.vmware.com/products/accelerator.html>

2.6.8 Wie geht es jetzt weiter?

Damit Sie sich nun selbst ein Bild machen können, wie virtuelle Maschinen funktionieren, geht es im folgenden *Kapitel 3* um die Installation der Produkte, von VMware Workstation bis Microsoft Virtual Server, als Vorbereitung auf die Praxis-Workshops im *Teil 2* des Buches.

3 Installation und Konfiguration der einzelnen Produkte

Mit Hilfe dieses Kapitels erhalten Sie schnell ein lauffähiges System für die weitere Arbeit mit den Praxis-Workshops in *Teil 2*. Hinweise zur grundsätzlichen Bedienung finden Sie gleich im Anschluss in *Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*.

Das Setup der Produkte ist völlig unkompliziert. Einzig und allein die Installation von VMware unter Linux ist, je nach Distribution, nicht ganz simpel. Dafür existiert zusätzlich ein separater detaillierter Workshop in *Teil 2, Kapitel 4, „Linux-Host mit VMware Server und Integration ins Windows-Netz“*, der auch für Linux-Neulinge geeignet ist.

3.1 Allgemeine Voraussetzungen und Vorbereitung für die Installation

Am wichtigsten ist es, sich vor der Installation ein paar Gedanken um die Vorbereitung des Host-Systems oder um die Hardware-Voraussetzungen zu machen und nach dem Setup noch einige Handgriffe an der Konfiguration der Umgebung zu erledigen, z.B. eine Ordnerstruktur für die Dateien der VMs zu erstellen. Das eigentliche Setup bereitet keine Probleme.

**Vorbereitung
und Konfiguration**

3.1.1 Hardware-Voraussetzungen auf dem Host

Bauen Sie möglichst vor der Installation des Host-Betriebssystems bereits alle Hardware ein, die Sie später verwenden wollen. So sparen Sie sich später Ärger mit nicht funktionierenden Komponenten und nicht erkannten Geräten. Manchmal werden z.B. nachträglich eingebaute parallele Schnittstellen von VMware nicht richtig erkannt, und unter Virtual PC/Server sind nachträglich eingebaute Netzwerkkarten nicht immer sofort sichtbar. Das sind alles leicht behebbare Fehler, die aber den ersten Eindruck trüben können.

Im Anschluss bekommen Sie kurz und knapp die wichtigsten Hinweise für die Ausstattung des Host-Rechners als Überblick, eine detaillierte Diskussion zur Hardware finden Sie in *Teil 1, Kapitel 1, „Grundlagen virtueller Maschinen und Hinweise zur Hardware“*. Dort werden auch grundlegende Begriffe erklärt, wie SAN, NAS oder iSCSI.

RAM-Ausstattung des Host-Rechners

Mindestens 512 MB RAM

Der Host sollte mindestens über 512 MB RAM verfügen. Aber erst ab 1–2 GB macht die Arbeit mit virtuellen Maschinen wirklich Spaß. Optimal ist eine Bestückung mit 2–4 GB. Damit haben Sie genügend Luft für mehrere parallel laufende VMs. *Viel hilft viel!* In Produktivumgebungen kann es auch mit 4 GB eng werden. Hinweise für die Verwendung von mehr als 4 GB RAM mittels PAE oder 64-Bit-Systemen schauen Sie bitte in *Teil 1, Kapitel 1* nach.

Anforderung an die Prozessoren im Host

CPU-Leistung spielt nicht die entscheidende Rolle, die meisten Gäste begnügen sich mit wenigen Prozent Auslastung. Aktuelle Prozessoren ab 2,5 GHz können problemlos mehrere Gäste bedienen. Selbst mit einer CPU ab 1 GHz können Sie in Testumgebungen schon mit virtuellen Maschinen arbeiten, je nachdem, welche Applikationen und Dienste im Gast laufen. Nur das Starten und Beenden mehrerer Gäste dauert dann entsprechend länger.

Dual CPU oder Dual Core

Produktiv sollten Sie für den Host Maschinen mit mindestens zwei oder mehr schnellen CPUs einplanen. Bedenken Sie dabei, dass ein Host mit vier CPUs zwar insgesamt preiswerter ist als zwei komplette Maschine mit Dual-CPU. Aber dafür bieten zwei Maschinen Redundanz und damit bessere Ausfallsicherheit. Eine gute Alternative sind Dual-Core-CPU, die zwei separate CPUs ersetzen können, die Mother Boards dafür sind meist preiswerter als Boards mit zwei Sockeln. Mit der Kombination eines Dual-CPU-Boards, bestückt mit Dual-Core-CPU, haben Sie insgesamt vier CPU-Kernel auf einem Board. Das genügt für viele virtuelle Umgebungen in einem Host vollauf.



Wenn Sie bei der Anschaffung eines neuen Desktop-PC bisher noch nicht wussten, ob sich der Aufpreis für einen Dual-Core gegenüber einer normalen CPU für Sie lohnt, dann haben Sie schon einen Kaufgrund mehr, sobald Sie mit virtuellen Maschinen Testumgebungen auf Ihrem PC aufbauen wollen!

Blade-Center

In großen Umgebungen sollten Sie über den Einsatz von so genannten Blade-Servern nachdenken. Das sind Platinen, welche die wichtigsten Komponenten wie RAM und CPU eines normalen Servers enthalten. Mehrere solcher Platinen werden in einem Gehäuse, dem so genannten Blade-Center, untergebracht und teilen sich dort Stromversorgung, Maus-, Tastatur- und VGA-Controller sowie weitere Peripherie. Dadurch können mit hoher Packungsdichte auf kleinstem Raum viele Server untergebracht werden. Weitere Server lassen sich durch Stecken zusätzlicher Platinen einfach hinzufügen. Blade-Server sind allerdings eher eine Domäne des ESX Servers.

Lastmessungen vor der Virtualisierung

Vor der Anschaffung der Hardware zum produktiven Einsatz ist zu prüfen, welche Last die schon vorhandenen Server und Dienste im laufenden Betrieb bereits erzeugen. Die Summe der Durchschnittswerte der einzelnen Maschinen muss dann der Host auf Dauer verkraften. Planen Sie auch genügend Ressourcen für Lastspitzen ein, z.B. für größere monatliche Datenbankläufe.

Zur Lastmessung können Sie beispielsweise den Microsoft Systemmonitor verwenden, zu finden bei den Serverprodukten unter SYSTEMSTEUERUNG/VERWALTUNG/SYSTEMMONITOR. Damit überwachen Sie verschiedene Leistungsindikatoren und zeichnen die Werte über einen gewissen Zeitraum in Protokolldateien auf. Interessante Parameter sind CPU-Leistung, Plattenzugriffe, Hauptspeichernutzung und Netzwerkverkehr.

Ein professionelles Tool zur Vorbereitung und Durchführung größerer Virtualisierungsvorhaben ist *PlateSpin PowerRecon* (<http://www.platespin.com/products/PowerRecon.aspx>).

Datenträger im Wirt für das Host-System und für die VMs

Sehr wichtig sind die Leistung und die Aufteilung der physischen Datenträger im Host. Ausführliche Hinweise zu Festplatten und zu externem Speicher finden Sie in *Teil 1, Kapitel 1, „Grundlagen virtueller Maschinen und Hinweise zur Hardware“*. Idealerweise sollte der Host über mehrere unabhängige Datenträger verfügen, mindestens zwei. Einer enthält das Wirtsbetriebssystem, auf den anderen liegen die VMs. Mehrere kleinere Datenträger sind besser als ein großer.

**Mehrere
Datenträger**

Mit separaten Datenträgern sind übrigens nicht nur einfach gesonderte Partitionen gemeint. Für die VMs eine extra Partition auf dem gleichen Datenträger anzulegen ist zwar übersichtlicher, bringt aber keinen Performancevorteil. Verwenden Sie besser zwei physische Platten oder zwei RAID-Systeme usw.



Bereits in einer Testumgebung mit VMware Workstation oder Virtual PC lohnen sich zwei getrennte Festplatten. Schon alleine weil dadurch Kopiervorgänge von Muster-VMs oder eine schnelle Sicherungskopie über verschiedene Platten wesentlicher zügiger vonstatten gehen als auf ein und derselben Platte. Sie werden bei der Verwendung von virtuellen Maschinen mit relativ großen Dateien umzugehen haben.

Zügiger kopieren

Für Gäste mit sehr intensiver I/O-Arbeit können Sie mehrere virtuelle Platten auf unterschiedlichen physischen Datenträgern erstellen. In diesen virtuellen Platten lassen sich Exchange-Datenbanken oder Fileserver-Bereiche der Gastsysteme aufteilen. Dadurch liegen sie dann auf separaten physischen Platten und werden durch unter-

schiedliche physische Controller angesprochen, was dem Durchsatz zugute kommt. In Produktionsumgebungen ist es selbstverständlich, Spiegelungen oder RAID-Konfigurationen zur Ausfallsicherheit einzusetzen. Für die Testumgebung genügen dagegen oft schon ein bis zwei einzelne SATA-Platten.

SAN, iSCSI, NAS, LAN

Virtuelle Maschinen und die Dateien der virtuellen Platten können auch auf einem externen Speicherplatz, wie einem SAN, liegen. Jeder Datenträger, der vom Host-System unterstützt wird, lässt sich auch als Ablageplatz für virtuelle Platten verwenden (siehe *Teil 1, Kapitel 1*). Mit Gigabit-Ethernet ist es sogar möglich, Gäste direkt über das LAN auf einer Dateifreigabe abzulegen und zu betreiben, z.B. in Test- oder Schulungsumgebungen.

Dateisysteme auf dem Host

Das Dateisystem der Wahl ist auf einem Host unter Windows unbedingt NTFS und unter Linux Ext3 oder ReiserFS. Diese Journaling-Systeme bieten eine wesentlich bessere Ausfallsicherheit und unterstützen große Dateien. Der ESX Server verwendet ein eigenes Dateisystem VMFS (*Virtual Machine File System*) als Ablage für die virtuellen Maschinen.

Rechte und Ordnung im Dateisystem auf dem Host

Ordnung im Dateisystem halten

Auf den Datenträgern sollten Sie unbedingt für die VMs eine sinnvolle Ordnerstruktur anlegen. In den Workshops von *Teil 2* des Buches empfehle ich einen Ordner *vmachines* mit Unterordnern *testumgebung*, *produktion* und *mustermachines*. Sie werden es am Anfang kaum glauben, wie schnell man den Überblick bei vielen VMs verliert, die sich mit der Zeit ansammeln. Ein Vorteil dieser Struktur ist es, dass Sie später z.B. dem Ordner *Produktion* sehr restriktive Dateirechte geben können und nur speziellen Nutzern den Zugriff gestatten. So verhindern Sie versehentliches oder mutwilliges Löschen bzw. Verändern der virtuellen Maschinen. In der Testumgebung dürfen die Rechte dagegen etwas lockerer gehandhabt werden, um den Anwendern das Benutzen von eigenen VMs zu ermöglichen. Zur Rechteverwaltung lesen Sie bitte *Teil 3, Kapitel 5, „Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs“*.

Physische Netzwerkkarten auf dem Host

Gemeinsame physische Adapter nutzen

Im einfachsten Falle benötigen Sie gar keine Netzwerkkarte im Host, wenn die VMs nur in virtuellen Testnetzen kommunizieren, z.B. unterwegs auf dem Laptop. Alle VMs und der Host gleichzeitig können sich auch ein und dieselbe Netzwerkkarte teilen und trotzdem als separate Rechner im LAN auftreten. In Produktivumgebungen ist eine Aufteilung der VMs über verschiedene Netzwerkkarten und damit eine Lastverteilung empfehlenswert. Eine zusätzliche Netzwerkkarte kann nur für die Bedienung des Hosts oder für Kopiervorgänge reserviert werden. Mehr Details und tiefgreifende Konzepte zu virtuellen Netzwerken finden Sie in den Netzwerk-Workshops *Teil 3, Kapitel 1*, und *Teil 3, Kapitel 2*.

3.1.2 Voraussetzungen an das Host-Betriebssystem

Das Host-Betriebssystem richten Sie vor der Produktinstallation fertig ein, nur der ESX Server wird direkt auf der Hardware installiert. Alle Treiber, der Zugriff auf die Datenträger und der Netzwerkzugriff müssen bereits funktionieren. So sparen Sie sich die spätere Fehlersuche.

Unterstützte Host-Betriebssysteme für die VMware-Produkte

Ich spare mir hier die komplette Liste der unterstützten Host-Systeme für alle VMware-Produkte. Grundsätzlich laufen die VMware-Produkte auf Systemen ab Windows 2000 und auch auf den aktuellen 64-Bit-Versionen der Windows-Betriebssysteme. Obwohl für den VMware Server nur die Windows Server offiziell unterstützt werden, läuft er auch problemlos auf einer Workstation mit Windows XP Professional. So müssen Sie für eine Evaluierung nicht unbedingt einen Server aufsetzen. Mit der Home-Version von XP verzichten Sie allerdings auf das Web-Interface des VMware Servers, weil es unter Windows XP Home offiziell keinen IIS (*Internet Information Server*) gibt.

Auf Linux-Basis unterstützt VMware offiziell vor allem RedHat und SUSE Linux, aber auch unter vielen anderen Distributionen, etwa Debian, funktionieren die Produkte. Manchmal ist ein wenig zusätzlicher Aufwand erforderlich. Als exemplarisches Beispiel dient der Workshop in Teil 2, Kapitel 4, „Linux-Host mit VMware Server und Integration ins Windows-Netz“. Dort beschreibe ich die komplette Installation und Einrichtung eines Linux-Hosts mit Debian für eine nicht unterstützte Distribution und SUSE für eine unterstützte.

VMware unter Linux

Wenn Sie die Wahl haben, dann entscheiden Sie sich aber möglichst für eine von VMware offiziell unterstützte Distribution. Vor allem als Linux-Neuling kann Ihnen das manche Google-Stunde ersparen!



Unterstützte Host-Betriebssysteme für die Microsoft-Produkte

Virtual Server kann unter Windows Server 2003 oder zum Testen auch unter Windows XP Professional installiert werden. Virtual Server benötigte zur Verwaltung zwingend den IIS (*Internet Information Server*)!

Für Virtual PC werden die Workstation-Versionen Windows 2000 Professional und Windows XP offiziell unterstützt. Trotz einer kleinen Warnung lässt sich die Software aber auch auf anderen Systemen, wie dem Windows Server 2003, installieren.

3.1.3 Vereinfachte Lizenzierung von Microsoft Windows Server 2003 R2 Enterprise Edition in VMs

Fünf Windows Server mit einer Lizenz!

Interessant ist in diesem Zusammenhang das Lizenzierungsmodell von Microsoft Windows Server 2003 R2 Enterprise Edition. Es wurde an die Anforderungen der Virtualisierung angepasst und erlaubt jetzt die Ausführung von zusätzlich bis zu vier virtuellen Maschinen auf ein und demselben Host mit nur einer erworbenen Lizenz. Das bedeutet im Klartext:

- ▶ Sie kaufen eine Lizenz Windows Server 2003 R2 Enterprise Edition.
- ▶ Sie installieren das Produkt einmal auf dem Host als Wirtsbetriebssystem.
- ▶ Sie können zusätzlich vier virtuelle Maschinen mit derselben Lizenz auf diesem Host laufen lassen.
- ▶ Sie betreiben damit fünf Windows Server-Instanzen mit einer Lizenz, vier davon virtuell.
- ▶ Eine Lizenz wird nur noch pro *laufender* Instanz benötigt. Das bedeutet, Sie dürfen unbegrenzt viele Kopien (Sicherungen, Templates usw.) erstellen, wovon aber immer nur vier in virtuellen Maschinen gleichzeitig laufen dürfen.
- ▶ Haben Sie Windows Server 2003 R2 Enterprise Edition gekauft, dürfen Sie in den VMs auch Windows Server 2003 R2 Standard Edition betreiben und kommen trotzdem in den Genuss des erweiterten Lizenzmodells.
- ▶ Die Lizenzierung gilt unabhängig von der verwendeten Virtualisierungssoftware.
- ▶ **Die Einschränkung:** Alle Maschinen müssen auf demselben Host laufen. Sollen zwei VMs auf Host A und eine VM auf Host B laufen, etwa zur Lastverteilung oder zum Clustering, benötigen Sie zwei Lizenzen!

Detaillierte Informationen finden Sie hier:

http://www.microsoft.com/germany/serverlizenzierung/produkte/windowsserver2003/neuerungen_r2.mspx

<http://www.microsoft.com/germany/serverlizenzierung/allgemein/virtualisierung.mspx>

3.2 Installation der Produkte

Folgen Sie einfach der Setup-Routine der Produkte, es ist ganz einfach – nur einige wenige zusätzliche Hinweise genügen, um Ihnen den Blick ins Handbuch ersparen. Zur Installation der Produkte benötigen Sie Administratoren- bzw. Root-Rechte auf dem Host.

Ich habe bereits im vorangehenden Kapitel darauf aufmerksam gemacht, dass Sie zum Ausprobieren der verschiedenen Produkte manche davon nebeneinander auf dem gleichen Host betreiben können:

- ▶ MS Virtual PC läuft parallel zur VMware Workstation.
- ▶ VMware Workstation installiert wiederum auch gleich VMware Player mit.
- ▶ VMware Workstation und Player laufen zwar nicht mit dem VMware Server auf dem gleichen Rechner, dafür aber problemlos parallel zur Remote-Konsole des VMware Servers auf einem LAN-Client. So können Sie am selben Arbeitsplatz die Features von VMware Workstation, VMware Player und VMware Server vergleichen.
- ▶ Selbst die konkurrierenden Hersteller vertragen sich auf dem gleichen Host. VMware Server läuft parallel zu MS Virtual Server zeitgleich auf demselben Wirt. Die Funktionen und die Bedienung lassen sich direkt nebeneinander vergleichen – sehr praktisch in der Entscheidungsphase.



Mehrere Produkte auf dem gleichen Host

3.2.1 Installation von VMware Workstation und VMware Player

Ausführliche Praxis-Workshops zur Verwendung dieser Produkte finden Sie in *Teil 2, Kapitel 1, Kapitel 5* und *Kapitel 6*. Die Produkte von VMware finden Sie als freie Versionen oder bei der Workstation als 30 Tage lauffähige Demo-Version, auf der Buch-CD oder auf den Webseiten von VMware:

www.vmware.com/products/

Grundsätzlich gibt es den Player als ein separates Software-Paket für jedermann kostenlos zum Download ohne Registrierung. Wenn Sie VMware Workstation installieren, wird ebenfalls eine Version des Players automatisch mit eingerichtet. Damit können Sie VMs in der Vollversion erstellen und vor der Weitergabe im Player testen. War vorher bereits der Player separat installiert, dann muss dieser erst deinstalliert werden. Für VMware Workstation müssen Sie eine Lizenz erwerben, um die Software über die 30-tägige Evaluierungsphase hinaus verwenden zu können.

Zwei Versionen des Players

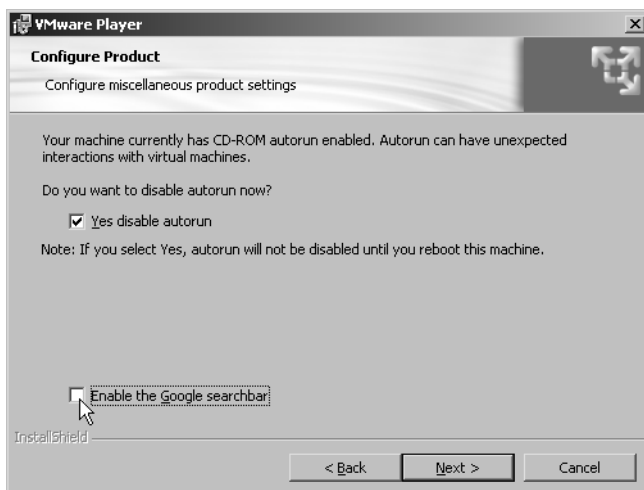


Praktisch ist die Tatsache, dass Sie in der Evaluierungsphase von VMware Workstation bereits VMs für den Player erstellen können, die sich dann später im Player weiterverwenden lassen. Selbst nach dem Ablauf der Evaluierungsphase der Workstation ist es rein technisch noch möglich, VMs in der Workstation zu erstellen und im Player laufen zu lassen. VMs für den Player können auch mit dem kostenlosen VMware Server erstellt werden.

Installation von VMware Workstation und Player unter Windows

Was soll ich schreiben: *Einfach installieren – fertig!* Das Setup dauert eine Weile, ist aber unkompliziert. Die Frage *Do you want to disable autorun now?* können Sie bejahen (Abbildung 3.1). Dadurch startet nicht jede CD, die für einen Gast eingelegt wurde, auch gleich am Host. Nur im Player wird automatisch die *Google-Suchleiste* eingerichtet, die dann in den Kopfzeilen der Gastfenster erscheint. Wenn Sie solche Tools von Drittanbietern nicht besonders mögen, können Sie an dieser Stelle die Einrichtung der Suchleiste unterbinden (Abbildung 3.1). In der Workstation wird noch der Lizenz-Key abgefragt, und schon ist die Installation beendet.

Abbildung 3.1:
CD-Autostart und
Google Searchbar
lassen sich unter-
binden



Standardver- zeichnis

Nach der Installation sollten Sie in der VMware Workstation das Standardverzeichnis für Ihre virtuellen Maschinen ändern, sonst landen alle neu erstellten VMs und alle virtuellen Platten im Benutzerprofil. Sie können das im Menü über EDIT/PREFERENCES/WORKSPACE z.B. auf *e:\vmaschinen* ändern (Abbildung 3.2). Im Player ist keine weitere Anpassung notwendig.

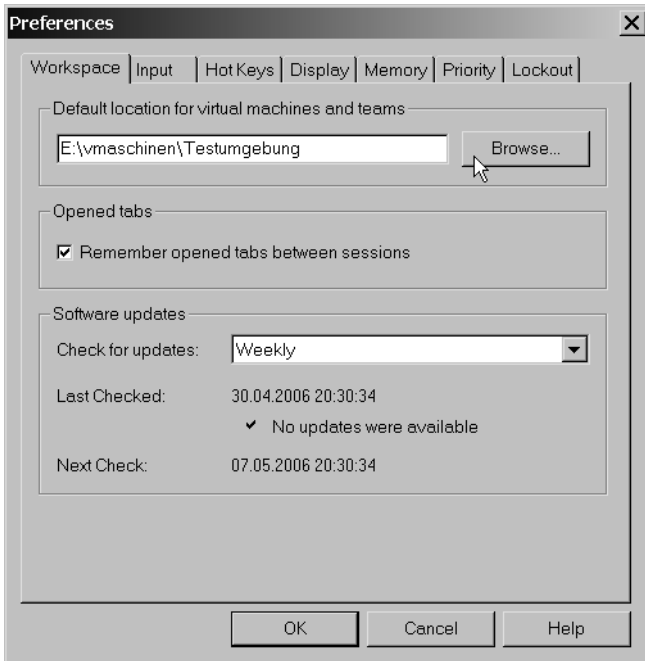


Abbildung 3.2:
Im Standardordner
von VMware
werden automatisch
alle neuen VMs und
virtuellen Platten
angelegt

Installation der Workstation und des Players unter Linux

Die Installation unter Linux verläuft aufgrund der Vielzahl verschiedener Distributionen nicht immer ganz so einfach wie unter Windows. Für alle VMware-Produkte gibt es ein paar grundlegende Hinweise, die ich im *Abschnitt 3.2.3, „Die VMware-Produkte unter Linux installieren“*, zusammengefasst habe.

3.2.2 Installation von VMware Server

Ausführliche Praxis-Workshops zur Verwendung des VMware Servers finden Sie in *Teil 2, Kapitel 1, Kapitel 3* und *Kapitel 8*. Ich möchte Sie zusätzlich auf den sehr ausführlichen Workshop in *Teil 2, Kapitel 4*, verweisen, der den Aufbau eines kompletten Virtualisierungshosts mit Debian- oder SUSE-Linux und VMware Server beschreibt. Zusätzlich richten wir alle Features ein, um den Server komfortabel an eine Windows-Umgebung anzubinden. Verzeichnisfreigaben mit Samba, Mounten von NTFS-Partitionen sind ein Thema genauso wie die Verwendung von 64-Bit-Systeme oder das Kompilieren des Kernels mit PAE-Option für viel RAM auf 32-Bit-Systemen. VMware Server finden Sie als freie Version auf der Buch-CD oder auf den Webseiten von VMware:

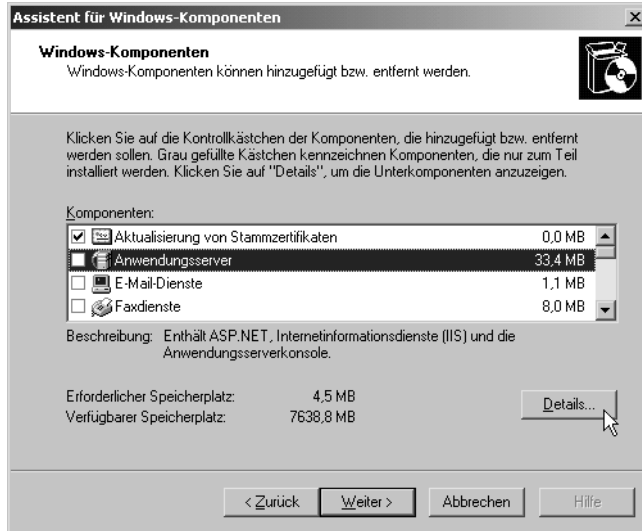
www.vmware.com/products/

Installation des VMware Servers unter Windows

Vorher den IIS installieren

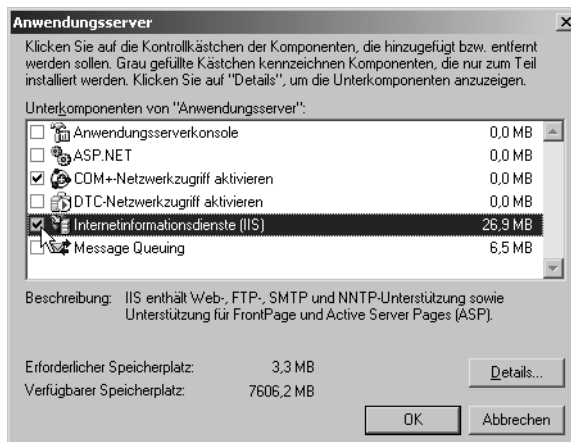
Vor der Installation des VMware Servers unter Windows sollten Sie den IIS (*Internet Information Server*) auf Ihrem Host installieren. Das können Sie einfach über SYSTEMSTEUERUNG/SOFTWARE/WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN tun (Abbildung 3.3).

Abbildung 3.3:
Wählen Sie für die
IIS-Installation bei
Anwendungsserver
Details



Mit der Auswahl ANWENDUNGSSERVER/DETAILS können Sie die Komponenten wählen, die zu installieren sind. Es genügen die Internetinformationsdienste, die COM-Komponenten werden automatisch mit ausgewählt (Abbildung 3.4). Mit dem Button DETAILS auf den IIS könnten Sie weitere Komponenten hinzufügen oder abwählen, es wird nur der WWW-Dienst benötigt.

Abbildung 3.4:
Es genügen die
Standardkomponenten
für den IIS



Sie benötigen den IIS für den VMware Server nicht unbedingt. Sie verzichten damit nur auf das Web-Interface, das einen Überblick über alle VMs im Browser liefert und einige Optionen zum Starten und Herunterfahren der Gäste anbietet (siehe „Das VMware Management Interface (Web-Interface) und VMware Server Console (Remote Console)“ weiter unten). Zusätzlich können darüber per Browser sehr praktisch die Remote-Konsole an den Clients im LAN installieren.



Einige Stichpunkte zum Installationsvorgang des VMware Servers:

- ▶ Bestätigen Sie Windows-Meldungen zur Vertrauenswürdigkeit des Herausgebers, und akzeptieren Sie die Lizenzvereinbarung im nächsten Bildschirm.
- ▶ Mit der Option CUSTOM können Sie Komponenten auswählen, auf die Sie eventuell verzichten wollen (Abbildung 3.5), z.B. das sich *VMware Management Interface* (Web-Interface) des Servers oder die Scripting-APIs. Ich empfehle Ihnen, trotzdem mit der Option COMPLETE das vollständige Paket zu installieren.

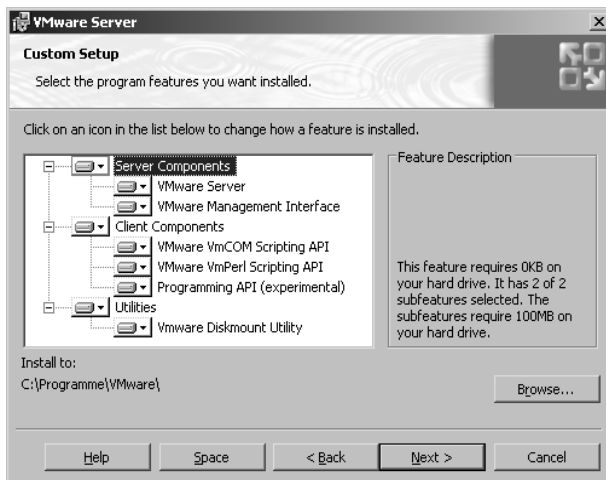
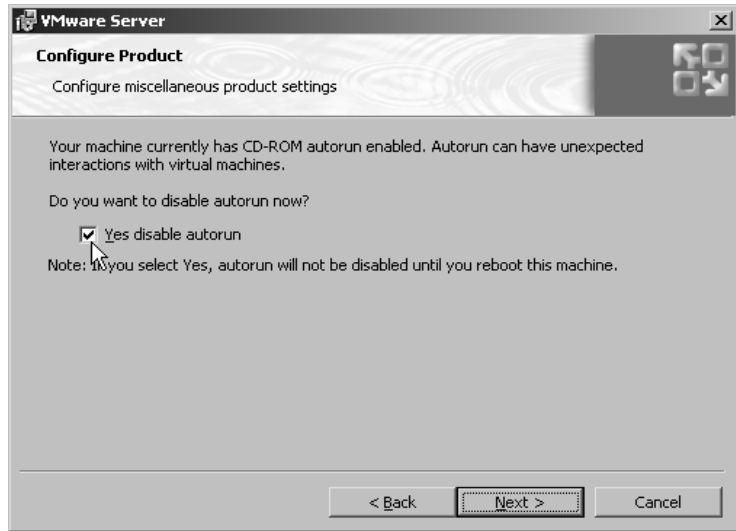


Abbildung 3.5:
Sie sollten den kompletten Server installieren. Mit der Option Custom lassen sich Komponenten aber auch abwählen

- ▶ Mit der Einstellung *Disable Autorun* soll verhindert werden, dass jede CD, die Sie für einen bestimmten Gast einlegen, gleich automatisch auf dem Host gestartet wird (Abbildung 3.6), Sie können die Option übernehmen.

Abbildung 3.6:
Abschalten von
CD-Autorun verhin-
dert, dass jede CD
am Host startet,
obwohl sie für ein
VM eingelegt wurde



Server Console Die Installation dauert etwas länger, zum Abschluss sehen Sie auf dem Desktop ein Icon für die *VMware Server Console*, die den Dreh- und Angelpunkt des VMware Servers bildet (Abbildung 3.7). Sie können sich nach dem Starten der Konsole direkt am Host mit dem Punkt LOCAL HOST als aktuell angemeldeter Benutzer mit dem laufenden VMware Server verbinden oder durch die Eingabe eines Hostnamens, bzw. der IP-Adresse, und eines Anmeldekontos auf jeden Remote-Host zugreifen.

Standardordner festlegen Zum Abschluss der Installation sollten Sie noch in der Konsole den Standardordner für Ihre VMs über das Menü HOST/SETTINGS/GENERAL einstellen (Abbildung 3.7), damit Ihre ersten neu erstellen VMs gleich im richtigen Verzeichnis angelegt werden. Das war es eigentlich schon – Sie können loslegen!

Abbildung 3.7:
Die Server Console
ist die Zentrale des
VMware Servers, sie
kann auf jedem LAN-
Client installiert
werden



Das VMware Management Interface (Web-Interface) und VMware Server Console (Remote Console)

Die VMware Server Console können Sie auch auf jedem beliebigen Netzwerkclient installieren, damit kontrollieren Sie den Server von jedem Platz im LAN. Am einfachsten erfolgt die Installation direkt aus dem so genannten *Web-Interface* des Servers. Von einem Client im Browser starten Sie das *VMware Management Interface* (Web-Interface) des VMware Servers mittels `http://mein_host:8222` oder gleich mit `https://mein_host:8333`. Sofort im Startbildschirm lässt sich ohne Anmeldung die *VMware Server Console* herunterladen und installieren (Abbildung 3.8). Zum Web-Interface siehe auch *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*.

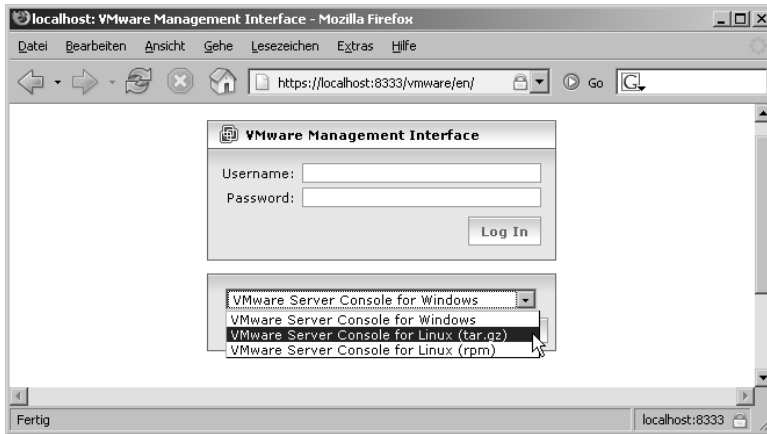


Abbildung 3.8:
Das Management Interface (Web-Interface) kann zum einfachen Installieren der Server Console am Client dienen

3.2.3 Die VMware-Produkte unter Linux installieren

Das grundsätzliche Problem an einer Linux-Installation ist die Vielzahl von unterschiedlichen Distributionen. Im Prinzip versucht VMware, fertig kompilierte Module mit den Installationspaketen auszuliefern. Aber selbst bei den offiziell unterstützten Distributionen gelingt es nicht immer, das zum aktuellen Kernel passende Binärmodul mitzuliefern. Wenn es Versionsänderungen in der Distribution gab, vor allem aber bei den nicht unterstützten Linux-Derivaten, können die mitgelieferten Binärmodule nicht verwendet werden.

Vorbereitung der Installation unter Linux

Wenn der VMware-Installer keine passenden Module dabei hat, dann versucht er, diese aus den Quellen neu zu kompilieren. Und genau an dieser Stelle beginnt oftmals der Ärger. Zur erfolgreichen Übersetzung müssen nämlich einige Voraussetzungen erfüllt sein:

- ▶ Der Compiler muss installiert sein.
- ▶ Die Version des installierten Compilers muss zum verwendeten Kernel passen.

Module neu übersetzen

- Die Kernel-Headers müssen in der richtigen Versionsnummer, passend zum Kernel auf dem System vorhanden sein.

Voraussetzungen erfüllen

Diese Voraussetzungen können Sie in verschiedenen Distributionen unterschiedlich erfüllen, hier drei Beispiele:

- SUSE 10 – (schauen Sie bitte auch in *Teil 2, Kapitel 4*). Für die aktuellen VMware-Versionen läuft unter SUSE 10 die Installation unkompliziert ab. Nur wenn doch einmal Probleme auftauchen, sollten Sie folgende Vorbereitungen treffen. Wirklich alle benötigten Pakete für die Übersetzung der VMware-Module erhalten Sie über *YaST* und die Software-Selektion *KERNEL-ENTWICKLUNG*. Eventuell ist noch der Kernel vor der VMware-Installation zu konfigurieren:

```
cd /usr/src/linux
make clean
make cloneconfig
make prepare
```

- Debian 3.1 – (schauen Sie bitte auch in *Teil 2, Kapitel 4*). Mit *apt* können Sie bequem alle benötigten Pakete für die Übersetzung der VMware-Module installieren:

```
apt-get install kernel-headers-$(uname -r)
build-essential xlibs-dev
```

- Ubuntu 5.10 – Unter Ubuntu können Sie sich mit *sudo* Root-Rechte verschaffen, da eine Anmeldung für die Installation mit dem Nutzer *root* normalerweise nicht möglich ist:

```
sudo apt-get install linux-headers-$(uname -r)
build-essential
```

Folgenden Zusatz benötigen Sie vor der Installation von VMware, da der Kernel mit einem anderen als dem aktuell mitgelieferten Compiler übersetzt wurde (Die benötigte Compiler-Version erfahren Sie mit `cat /proc/version`):

```
sudo apt-get install gcc-3.4 g++-3.4
export CC=gcc-3.4
```

Benötigte Pakete von VMware und zusätzliche Patches

Any-Any-Patch

Die Installationspakete liefert VMware als TAR-Archiv oder RPM-Paket. Im Grunde genommen ist es nicht ausschlaggebend, was Sie davon installieren, TAR funktioniert aber in jedem Linux. Zusätzlich gibt es den so genannten *Any-Any-Patch* von Petr Vandrovec, der Unverträglichkeiten mit nicht unterstützten Versionen behebt. Die aktuellen VMware-Versionen benötigen den Patch nicht mehr unbedingt (Näheres zum Patch siehe in *Teil 2, Kapitel 4*)!

Die TAR-Archive müssen Sie vor dem Setup erst noch auspacken. Wir nehmen an, sie befinden sich auf einer CD, die unter Linux *gemountet* werden muss. Vorher erstellen Sie auf einer Festplatte des Hosts am besten ein Verzeichnis */install* als Zielordner für die entpackten Dateien. Alle Pakete liegen dann ausgepackt im Verzeichnis */install* und können auch für spätere Neuinstallationen immer wieder verwendet werden:

TAR auspacken

```
mount /dev/cdrom /mnt
mkdir /install
cd /install
tar zxvf /mnt/VMware-XXX.tar.gz
tar zxvf /mnt/VMware-XXX.tar.gz
```

Installation der VMware-Pakete unter Linux

Die Installation der VMware-Produkte übernimmt das Skript *vmware-install.pl*, das zuerst alle benötigten Dateien kopiert. Gleich anschließend ruft dieses Skript ein weiteres Skript auf, nämlich *vmware-config.pl*, das überprüft, ob die mitgelieferten Binärmodule zur Version des aktuellen Kernels passen, sonst werden diese überschrieben. Alle Fragen des Setups können Sie mit den Standardvorgaben beantworten. Die EULA müssen Sie erst mit der Leertaste nach unten durchblättern, bevor Sie diese bestätigen können. Sie starten die komplette Installation mit folgenden Befehlen:

```
cd /install/vmware-server-distrib
./vmware-install.pl
```

Wenn Sie den VMware Server mit den RPM-Paketen installieren, müssen Sie anschließend das Skript *vmware-config.pl* manuell starten:

RPM-Installation

```
/usr/bin/vmware-config.pl
```

Unter SUSE geht die Installation scheinbar nach dem Anzeigen der EULA nicht weiter. Die notwendige *yes/no*-Abfrage wird gar nicht angezeigt. An solchen Stellen können Sie mit der Taste *q* die fehlenden Fragen sichtbar machen und dann richtig beantworten.



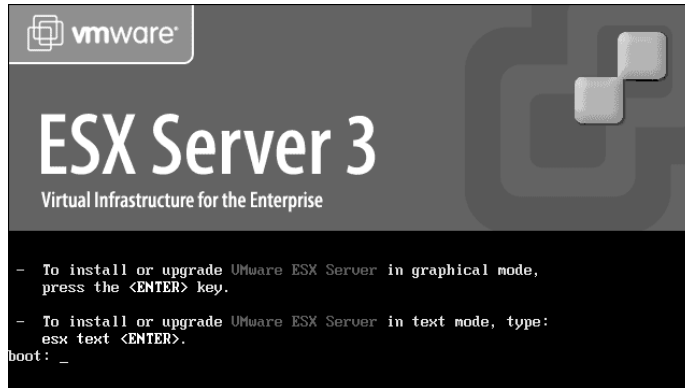
3.2.4 Installation von VMware ESX-Server 3

Da der ESX Server sich vom gesamten Konzept und in den Features von den anderen Produkten stärker unterscheidet, widme ich ihm einen kompletten eigenen Workshop in *Teil 2, Kapitel 9, „VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2“*. Dort sind sehr ausführlich die Installation und die Lizenzierung einer Evaluierungsversion beschrieben. Als Ausblick hier nur ein paar knappe Worte dazu:

Die Installation des ESX Servers ist genauso unkompliziert wie die der anderen Produkte. Das Setup erfolgt wahlweise mit einer grafischen Oberfläche oder textbasiert (Abbildung 3.9). Wie bereits erwähnt, benö-

tigt der ESX kein Host-Betriebssystem, er wird von der CD direkt auf die blanke Hardware installiert. Für diese Hardware sind dagegen einige Voraussetzungen zu erfüllen, da VMware nur für eine engere Auswahl Treiber mitliefert. Für die gebräuchlichsten Hersteller, von der Netzwerkkarte *Intel Pro 1000* bis zum *Qlogic Fiberchannel HBA* (Host Bus Adapter für SAN-Anbindung), ist eine Unterstützung vorhanden. VMware setzt ausschließlich auf SCSI-, RAID- oder SAN-Datenträger. Mit IDE-Platten gibt sich das System nicht zufrieden. Für eine Testumgebung zum ersten Kennenlernen genügt aber bereits ein einfacher Adaptec-SCSI-Controller mit einer kleinen Festplatte und zwei 100-MBit-Intel-Netzkarten. Vorschläge zur Hardware finden Sie ebenfalls in *Teil 2, Kapitel 9*.

Abbildung 3.9:
Der ESX Server
kann wahlweise im
Textmodus oder mit
einer grafischen
Oberfläche instal-
liert werden



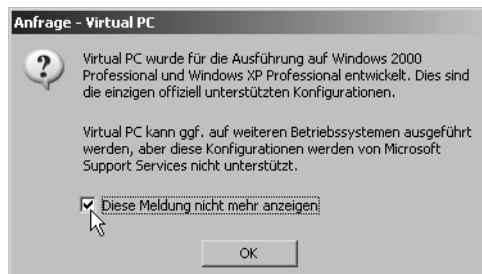
3.2.5 Installation von Microsoft Virtual PC 2004 SP1/2007

Einen ausführlichen Praxis-Workshop zur Verwendung dieses Produktes finden Sie in *Teil 2, Kapitel 2*. Sie erhalten die kostenlose Vollversion auf den Microsoft-Seiten:

<http://www.microsoft.com/windows/virtualpc/>

Sie können Virtual PC teilweise auch auf anderen Windows-Versionen als den offiziell vorausgesetzten installieren, z.B. auf einem Server. Das wird von Microsoft zwar offiziell nicht unterstützt, die erscheinende Fehlermeldung lässt sich aber einfach wegklicken (Abbildung 3.10).

Abbildung 3.10:
Virtual PC läuft z.B.
auch auf einem
Windows-Server



Das Setup ist völlig unkompliziert und selbsterklärend. Nach der Installation sollten Sie auch unter Virtual PC das Standardverzeichnis für Ihre virtuellen Maschinen ändern, alle neu erstellten VMs und alle virtuellen Platten landen sonst immer im Benutzerprofil. Das funktioniert etwas umständlich über die Umgebungsvariable `MYVIRTUALMACHINES`, die sich auf dem Host unter `SYSTEMSTEUERUNG/SYSTEM/ERWEITERT/UMGEBUNGSVARIABLEN` als neue Systemvariable festlegen lässt (Abbildung 3.11).

Standardordner ändern

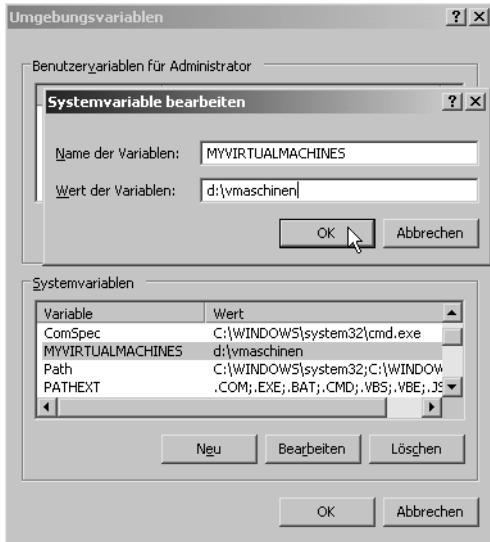


Abbildung 3.11:
Das Standardverzeichnis für VMs und virtuelle Platten muss bei VPC über eine Umgebungsvariable eingestellt werden

3.2.6 Installation von Microsoft Virtual Server 2005 R2

Einen ausführlichen Praxis-Workshop zur Verwendung dieses Produktes finden Sie in *Teil 2, Kapitel 7* und *Kapitel 8*. Vor der Installation des Virtual Servers müssen Sie den IIS auf Ihrem System installieren. Das können Sie einfach über `SYSTEMSTEUERUNG/SOFTWARE/WINDOWS-KOMPONENTEN HINZUFÜGEN/ENTFERNEN` mit der Auswahl `ANWENDUNGSSERVER/DETAILS` tun (Abbildung 3.3 und Abbildung 3.4). Den kostenlosen Virtual Server erhalten Sie gegen Registrierung beim Microsoft Passport-Netzwerk auf den Webseiten von Microsoft:

IIS installieren

www.microsoft.com/germany/virtualserver

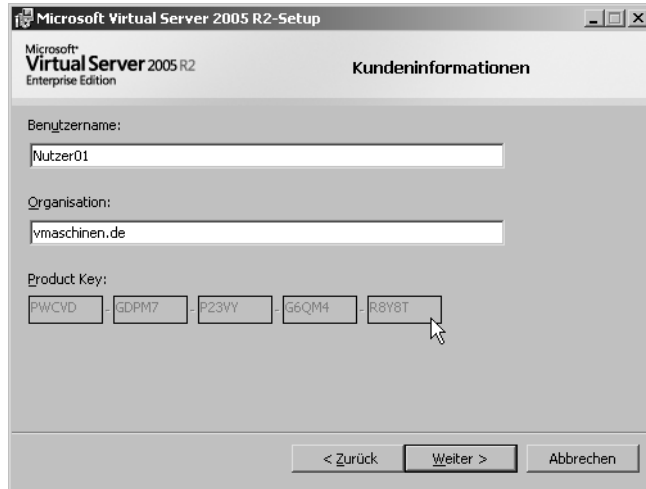
Die Bedienung des Virtual Servers erfolgt größtenteils webbasiert. Für die Verwaltung ist am Client als Browser der Internet Explorer ab Version 5.5 notwendig. Alternativen wie Mozilla Firefox funktionieren nicht.



Einige Stichpunkte zum Installationsvorgang von Virtual Server:

- Kurz nach dem Start der Installation können Sie den voreingestellten Microsoft Produkt-Key bestätigen, der automatisch erscheint, seit das Produkt kostenlos erhältlich ist (Abbildung 3.12).

Abbildung 3.12:
Virtual Server ist
kostenlos, der
Produkt-Key kommt
gleich mit



- Installieren Sie den Server mit der Option VOLLSTÄNDIG.
- Den vorgeschlagenen WEBSITEPORT 1024 müssen Sie nur ändern, wenn bereits andere Dienste auf dem Server den gleichen Port verwenden (Abbildung 3.13). Darüber kommuniziert das Web-Interface des Servers.

Abbildung 3.13:
Über den Website-
Port wird Virtual
Server verwaltet



- ▶ Lassen Sie vom Setup auch gleich die Firewall-Ports öffnen, die zum Zugriff auf den Server benötigt werden (Abbildung 3.14).



Abbildung 3.14:
Alle benötigten
Ports müssen in der
Windows-Firewall
geöffnet werden

- ▶ Das Setup ist sehr zügig fertig, und zum Abschluss erscheint automatisch eine Zusammenfassung im Browser, in der Sie auch gleich den Link zum Web-Interface finden.

Konfiguration der Virtual Server-Verwaltungswebsite (Web-Interface)

Die *Verwaltungswebseite* (*Web-Interface*) von Microsoft Virtual Server ist die zentrale Anlaufstelle zur Verwaltung des Servers und der Gäste (Abbildung 3.15). Sie erreichen die Webseite am Host selbst oder von einem Client im LAN über:

`http://mein_host:1024/`

Nach der Installation sollten Sie in der Verwaltungswebseite noch ein paar Dinge konfigurieren:

- ▶ Unter VIRTUAL SERVER/SERVEREIGENSCHAFTEN/SUCHPFADE/ bestimmen Sie den Standardordner, in dem Ihre neu erstellten VMs und virtuellen Festplatten liegen sollen. In den Workshops ist das z.B. immer `d:\vmaschinen\testumgebung`.
- ▶ Sollten Sie schon virtuelle Platten, etwa von Virtual PC, oder eine Sammlung von ISO-Images haben, dann können Sie unter SUCHPFADE die Ordner hinterlegen, wo diese Dateien liegen. Das erspart Ihnen in der teilweise umständlichen Verwaltung von Virtual Server einige Schreiberei von ellenlangen Verzeichnispfaden (siehe Teil 1, Kapitel 4).

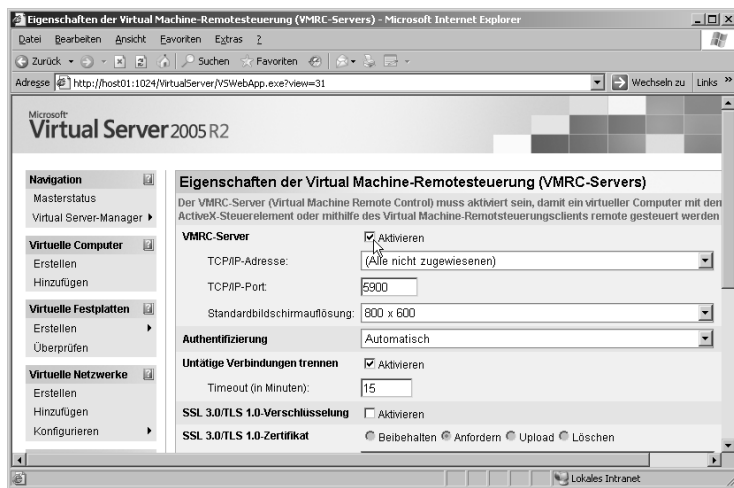
Standardordner

Suchpfade

Remotesteuerung freischalten

- Zusätzlich müssen Sie noch unter VIRTUAL SERVER/SERVEREIGENSCHAFTEN/VIRTUAL MACHINE-REMOTESTEUERUNG für die Fernsteuerung den VMRC-Server aktivieren, damit Sie den Bildschirminhalt der laufenden Gäste sehen und darin arbeiten können (Abbildung 3.15). Das ist auch notwendig, wenn Sie nur am Host arbeiten wollen. Wenn Sie nicht wollen, dass jede Fernsteuerung nach 15 Minuten immer wieder getrennt wird, sollten Sie gleich den Haken bei UNTÄTIGE VERBINDUNGEN TRENNEN entfernen.

Abbildung 3.15:
Mit dem Web-Interface wird der Server verwaltet. Hier müssen Sie auch die Remotesteuerung für die Gäste aktivieren



Der Port 5900 der VMRC wird auch vom beliebten Fernsteuerungstool VNC verwendet. Sollten Sie neben dem Remote-Desktop von Windows auch dieses Tool verwenden, dann müssen Sie dessen Port ändern oder für Virtual Server einen anderen wählen.

Alle weiteren Einstellungen der Remotesteuerung können Sie so lassen, die SSL-Verschlüsselung verwenden wir vorerst nicht. Vergessen Sie nicht, im Browser ans Ende zu scrollen und das kleine OK ganz unten rechts in der Ecke anzuklicken! Für die Remotesteuerung der Gäste gibt es zusätzlich das kleine schlanke Programm *vmrc.exe* als separaten Fernsteuerungsclient. Sie finden es auf dem Host unter *C:\Programme\Microsoft Virtual Server\VMRC Client*. Sie können es sich an einer zentralen Stelle im LAN ablegen. Auf die Verwendung und auf die gesamte Bedienung gehe ich in den Praxis-Workshops und vor allem im folgenden *Kapitel 4* zur Bedienung der Produkte detailliert ein.

3.2.7 Wie geht es jetzt weiter?

Sie verfügen jetzt über die funktionsfähige Installation eines Virtualisierungsproduktes Ihrer Wahl. Damit haben Sie die Vorbereitungsphase abgeschlossen. Sie können sofort mit einem Praxis-Workshop aus *Teil 2* des Buches beginnen, um direkt am Rechner den Umgang mit virtuellen Maschinen zu erlernen. In den Workshops erarbeiten Sie sich ohne langes Vorstudium an einem nützlichen Einsatzbeispiel alle notwendigen Handgriffe und Konzepte.

Nützliche Einsatzbeispiele nachvollziehen

Wenn Sie wollen, können Sie vorher im folgenden *Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*, noch einige grundlegende Dinge zur Bedienung nachlesen. Sie können darauf aber auch erst später zurückkommen, da die wichtigsten Grundlagen auch in den Kapiteln von *Teil 2* vermittelt werden, was einen sofortigen Schnellstart ermöglicht.

4 Bedienung der Produkte – wichtige Funktionen und Tipps

Wenn Sie das vorhergehende *Kapitel 3, „Installation und Konfiguration der einzelnen Produkte“*, durchgearbeitet haben, verfügen Sie bereits über eine lauffähige Installation eines Virtualisierungsproduktes Ihrer Wahl. Sie können sofort mit einem Praxis-Workshop in *Teil 2* beginnen, jedes Kapitel dort vermittelt die notwendigsten Grundlagen zur Bedienung der Virtualisierer am praktischen Einsatzbeispiel ohne viel Vorstudium.

**Sofort loslegen
in Teil 2**

In diesem Kapitel hier finden Sie neben den Grundlagen weitere Funktionen und Hinweise, die nicht in jedem Praxis-Workshop wiederholt werden, die Sie aber zum Einstieg auch nicht sofort benötigen. Da die Bedienung der Produkte in vielen Punkten sehr intuitiv ist, habe ich mich gegen eine akribische Auflistung jedes Menüeintrages entschieden. Stattdessen erhalten Sie einen Überblick über die wichtigsten Bedienkonzepte mit nützlichen Tipps. Sehr komplexe Themen, wie Snapshots, Klonen oder virtuelle Netzwerke, habe ich in ausführliche Workshops in *Teil 3* des Buches ausgelagert.

**Wichtige
Grundlagen
und Tipps**

Für den ESX Server existiert ein gesonderter Workshop in *Teil 2, Kapitel 9, „VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2“*.

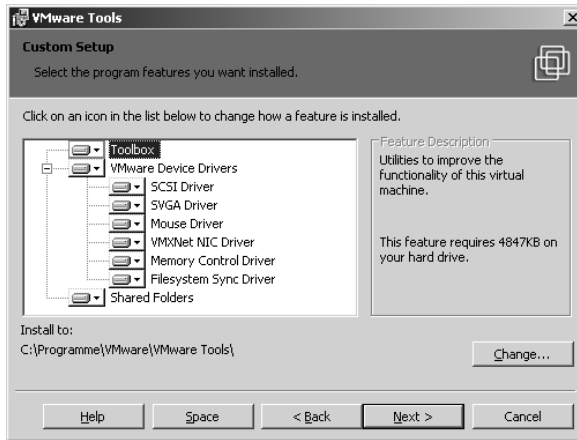
4.1 Was sind die VMware Tools?

Bevor wir uns den einzelnen Virtualisierungsprodukten von VMware zuwenden, muss ich als Vorbereitung noch einige Worte zu den *VMware Tools* verlieren, sie werden in den folgenden Abschnitten immer wieder erwähnt. Die Tools sind ein Treiber- und Programmpaket von VMware, das in den Gästen installiert wird (Abbildung 4.1). Der folgende kurze Überblick ist für das bessere Verständnis einiger Funktionen von VMware notwendig, die Installation finden Sie in einem eigenen Abschnitt, da sie wegen des Unterschieds von Windows- und Linux-Gästen etwas umfangreicher ist (siehe *Abschnitt 4.4, „VMware Tools in Windows- und Linux-Gästen installieren“*).

Das Setup der VMware Tools sollte immer eine der erste Aktionen sein, die Sie in einem neu installierten Gastsystem durchführen. Nur so verfügt Ihr Gast über Funktionen, wie automatisches Herunterfahren, automatischen Wechsel der Maus zwischen Host und Gast oder vernünftige Bildschirmauflösungen.



Abbildung 4.1:
Die VMware Tools
bringen optimierte
Treiber und viele Zu-
satzfunktionen mit



Folgende Funktionen liefern die VMware Tools in den Gästen:

**Die VMware Tools
optimieren den
Gast**

- ▶ *Optimierte Treiber* – Die Tools installieren verschiedene Treiber für VGA, Maus, Netzwerkkarten und für die SCSI-Controller in der VM. Diese Treiber beschleunigen zum einen das Gastsystem, zum anderen ermöglichen sie Funktionen, wie automatische stufenlose Skalierung des Bildschirmauflösung des Gastes und nahtlosen Fokuswechsel zwischen Gast und Host beim Verschieben der Maus.
- ▶ *Drag&Drop, Cut&Paste und Shared Folders* – Die Tools stellen Funktionen zum komfortablen Datenaustausch zwischen Host und Gästen bereit. Dadurch können Sie z.B. Dateien einfach vom Host in die VM ziehen und umgekehrt (*Drag&Drop*) oder einen Ordner auf dem Host für das Gastsystem freigeben (*Shared Folders*).
- ▶ *Systemsteuerung bei PowerOff und Reset* – Durch die Tools werden die Gastsysteme bei einem Klick auf POWEROFF automatisch heruntergefahren, bevor die VM abschaltet oder neu startet.
- ▶ *Skripte im Gast* – Die Tools führen bei bestimmten Aktionen, etwa POWERON, SUSPEND oder POWEROFF, automatisch Skriptdateien im Gast aus. Die Skripte sind einfache Batch-Dateien, standardmäßig im Verzeichnis *Programme\VMware\VMware Tools* im Gast. Das Standardskript *resume-vm-default.bat* sorgt beispielsweise dafür, dass der Gast nach dem Erwachen aus dem Suspend-Modus eine neue IP-Adresse über DHCP bezieht und nicht einfach mit der veralteten Adresse weiterarbeitet. Diese könnte im LAN bereits neu vergeben sein.
- ▶ *Zeitsynchronisation mit dem Host* – Der Gast kann über die Tools die Uhrzeit vom Host beziehen. Das ist z.B. praktisch, wenn die VM nach längerem Suspend wieder mittels RESUME zum Leben erweckt wird. Alternativ können Sie auch einen vorhandenen Zeitserver im LAN verwenden.

- ▶ *Heartbeat* – Die Tools senden regelmäßig ein Signal, ob der Gast noch ordnungsgemäß läuft. Dieses Signal kann zur Überwachung ausgewertet werden.
- ▶ *Shrink für virtuelle Platten* – Die *Shrink*-Funktion (siehe Platten-Workshop in Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“) verdichtet virtuelle Zuwachsplatten und verkleinert dadurch die Datei der virtuellen Platte. Dabei wird Platz wieder freigegeben, den der Gast nicht mehr verwendet, z.B. gelöschte Dateien. Die freigewordenen Sektoren im Gast müssen dazu mit Nullen überschrieben werden, damit die *Shrink*-Funktion die Sektoren aus der virtuellen Platte entfernen kann. Diese Vorbereitungsarbeit leisten ebenfalls die VMware Tools in den Gästen.
- ▶ *Speicherverwaltung und Snapshots* – Beim VMware ESX Server 3 kommen noch Treiber für die Speicherverwaltung und für die Gewährleistung eines konsistenten Dateisystems beim Erstellen von Redo-Logs für Host-Backups hinzu (Details zu diesen Funktionen finden Sie in Teil 2, Kapitel 9).

4.2 Bedienung des VMware Players

Die Bedienung des VMware Players wird im Praxis-Workshop von Teil 2, Kapitel 5, bereits ausgiebig beschrieben, weshalb hier ein kurzer Überblick genügt. Zum spartanischen Menü des Players gibt es nicht viel zu sagen. VMs lassen sich weder erstellen noch konfigurieren, alle Funktionen wie Snapshots oder Klone fehlen. Es gibt keine Favoritenleiste und keine Verwaltung von mehreren VMs im gleichen Fenster (Abbildung 4.2).

Beim Start des Players können Sie in einem Auswahldialog die Konfigurationsdatei (*.vmx) im Ordner einer vorhandenen VM auswählen. Die VM startet dann sofort. Die Gäste starten Sie auch mit einem einfachen Doppelklick auf die *vmx*-Datei. Sie können sich Verknüpfungen zu den *vmx*-Dateien auf dem Desktop oder im Startmenü anlegen, was eine Alternative zur Favoritenleiste der Vollprodukte ist.

**Verknüpfungen
zur vmx-Datei**

Beim Schließen des Fensters beendet der Player auch die VM. Im Normalfall wird der Gast dabei in den *Suspend-Modus* versetzt. Beim Neustart erwacht der Gast dann genau an der gleichen Stelle, ohne erst komplett neu zu booten. Sie können auch festlegen, dass der Gast richtig abgeschaltet wird, die Einstellung finden Sie im Player-Menü unter PLAYER/PREFERENCES (Abbildung 4.2). Sind die *VMware Tools* im Gast installiert, wird das Betriebssystem vor dem Ausschalten noch ordentlich heruntergefahren, ansonsten wirkt das Beenden für den Gast wie ein plötzlicher Stromausfall.

**Suspend-Modus
oder PowerOff**

Abbildung 4.2:
Der Player bietet
nur eine sehr einge-
schränkte Benut-
zeroberfläche



Zu den Funktionen von Tastatur und Maus, zum Datenaustausch über Drag&Drop oder zu den VMware Tools und Bildschirmskalierung sowie Vollbildmodus lesen Sie bitte die Abschnitte weiter unten (Abschnitt 4.3.2, „Die wichtigsten Funktionen und Tipps zur Bedienung von VMware Workstation und Server“). Die Funktionen sind gleich, bis auf die *Shared Folders*, die der Player nicht unterstützt.

4.3 Bedienung von VMware Workstation und VMware Server

Die Menüs der VMware Workstation und des VMware Servers ähneln sich stark. Ich werde beide Produkte zusammen beschreiben. Das ist eine gute Gelegenheit, um auf die wichtigsten Unterschiede in der Bedienung einzugehen. Einen praxisbezogenen Einstieg zu den beiden Produkten finden Sie in *Teil 2, Kapitel 1*, eine erweiterte Anwendung mit Schwerpunkt Netzwerk finden Sie mit dem Aufbau einer virtuellen DMZ in *Teil 2, Kapitel 3*.

4.3.1 Die Bedienoberflächen von VMware Workstation und VMware Server im Überblick

Workstation und Server haben einheitliche Oberflächen

Der Hauptunterschied in der Bedienung der beiden VMware-Produkte liegt darin, dass die Workstation ausschließlich am Host über das lokal laufende Programmfenster bedient wird, während der Server über eine Remote-Konsole von jedem LAN-Client aus gesteuert werden kann. Aufbau und Funktionen der Bedienoberflächen unterscheiden sich aber nur in Details, was sehr praktisch ist bei einem

Umstieg oder beim Parallelbetrieb beider Produkte. Einige der wichtigsten Unterschiede in den Bedienoberflächen von VMware Server und Workstation finden Sie im Folgenden auf einen Blick.

Welche Hauptfunktionen fehlen am Server gegenüber der Workstation?

- ▶ *Keine multiplen Snapshots* – Der Server unterstützt nur einen einzigen Snapshot, es existiert kein grafischer Snapshot-Manager.
- ▶ *Keine Linked Clones* – Es gibt am Server keinen Clone-Wizard, das Menü VM/CLONE fehlt. VMs müssen manuell kopiert werden, um sie zu vervielfältigen, und die so genannten *Linked Clones* (platzsparende Klone basierend auf der gleichen virtuellen Platte) können Sie nur manuell mit einigen Tricks erzeugen (siehe Teil 3, Kapitel 4, „Die Snapshot- und Clone-Funktion der VMware-Produkte“).
- ▶ *Keine Teams* – VMs können am Server nicht zu Teams zusammengefasst werden, die das gemeinsame Starten und Beenden ganzer Testumgebungen auf einen Mausklick ermöglichen.
- ▶ *Die VMware Tools* bieten in Gästen unter dem Server nicht alle Funktionen der Workstation. Es fehlen *Shared Folders* und *Drag&Drop* zum unkomplizierten Datenaustausch zwischen Gast und Host. *Cut&Paste* zur Übertragung von Textinhalten funktioniert dagegen.

Welche wichtigen Funktionen gibt es zusätzlich am Server?

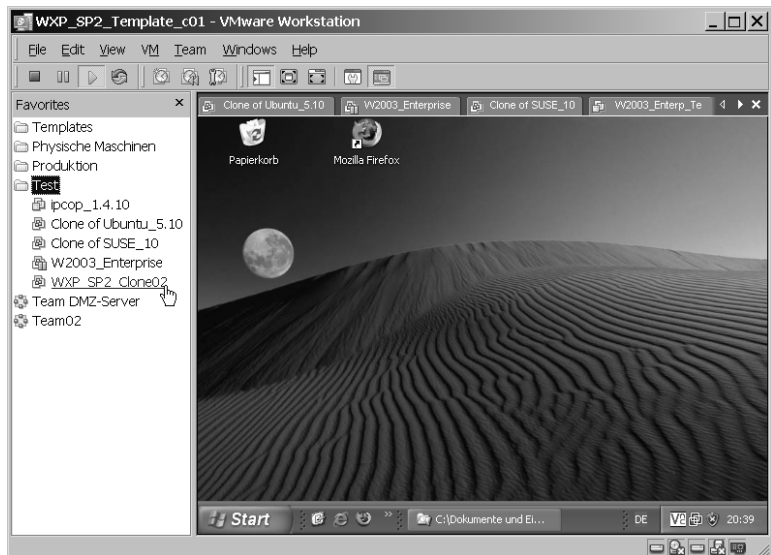
- ▶ *Menü HOST* – Einige Einstellungen finden Sie in der Konsole des Servers nicht im Menüpunkt EDIT, sondern unter dem Menüpunkt HOST, z.B. die NETWORKSETTINGS.
- ▶ *Netzwerk* – Der Server unterstützt eine vierte Netzwerkkarte (Workstation nur drei) in jedem Gast, ansonsten unterscheiden sich die Netzwerkoptionen zwischen Workstation und Server nicht.
- ▶ *VMs als Dienste* – Der VMware Server kann eine VM als Dienst laufen lassen, wodurch auch das automatische Starten und Beenden von VMs beim Starten bzw. Herunterfahren des Hosts möglich ist. Im Web-Interface des Servers können Sie zusätzlich eine bestimmte Startreihenfolge der Gäste festlegen.
- ▶ *Rechte* – Für die einzelnen Gäste können Sie am Server Zugriffsrechte auf Nutzerbasis über das Dateisystem und die Konfigurationsdatei vergeben (siehe Teil 3, Kapitel 5, „Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs“).
- ▶ *Eine Scripting-API* für Perl, COM und C ermöglicht unter dem VMware Server Funktionen wie Starten und Beenden von VMs, über die Kommandozeile oder aus eigenen Programmen heraus. Die VMware Workstation bietet mit dem Programm *vmrun.exe* dafür nur ein Kommandozeilentool (siehe Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“).

- ▶ *VMware Management Interface (Web-Interface)* – Zusätzlich bietet der Server das VMware Management Interface, eine webbasierte Oberfläche, die hauptsächlich einen Überblick über den Zustand aller laufenden VMs liefert, es lassen sich keine VMs damit konfigurieren. Gleich von der Startseite aus können Sie bequem die VMware Server Console auf jedem beliebigen LAN-Client installieren.

Das Fenster der VMware Workstation 5.5

Die Bedienung der VMware Workstation ist nur auf dem lokalen PC möglich (Abbildung 4.3), eine Remote-Konsole, wie beim VMware Server, gibt es nicht.

Abbildung 4.3:
Die Oberfläche der
VMware Work-
station ähnelt dem
VMware Server. Sie
bietet aber mehr
Funktionen wie
multiple Snapshots



Eine Fernsteuerung des VMware Workstation Hosts ist mittels einer Remotedesktop-Verbindung oder Tools wie VNC möglich. Dabei kommt es mitunter vor, dass der Bildschirm einer VM schwarz bleibt oder die Maus in den Gästen sehr schwerfällig reagiert. Eine Alternative ist die direkte Fernsteuerung der Gastsysteme in den VMs, was auf jeden Fall flüssiger vonstatten geht. Dazu müssen die Gäste über das Netzwerk erreichbar sein und jeweils über Remotedesktop oder ein Fernsteuerungstool verfügen. Die Fernsteuerung auf dem Host dient dann nur noch der Konfiguration oder dem Ein- und Ausschalten von Gästen.

Die VMware Server Console (Remote Console) des VMware Servers

Die *VMware Server Console*, die häufig auch als *Remote Console* bezeichnet wird, kann lokal am Host oder auf einem beliebigen PC im Netzwerk installiert werden. Damit ist aus der Ferne eine Bedienung aller Funktionen inklusive der Gastsysteme möglich (Abbildung 4.4). Die Kommunikation erfolgt über eine sichere SSL-Verbindung. Die Konsole unterscheidet sich auf den ersten Blick kaum von der VMware Workstation, es fehlen aber einige Komfortfunktionen, wie multiple Snapshots oder eine Clone-Funktion. Die Installation erfolgt am Host automatisch während des Setups, an den Clients kann die Konsole am einfachsten über das Web-Interface installiert werden, wie es in *Teil 1, Kapitel 3*, bereits beschrieben wurde.



Abbildung 4.4:
Die VMware Server Console ermöglicht die Fernverwaltung des VMware Servers von jedem Client im LAN

Zur schnellen Verbindung der VMware Server Console mit einem bestimmten Host können Sie sich am Client eine Verknüpfung mit folgender Befehlszeile hinterlegen:

```
"C:\Programme\VMware\VMware Server Console\vmware.exe" -h mein_host -u nutzer -w passwort
```



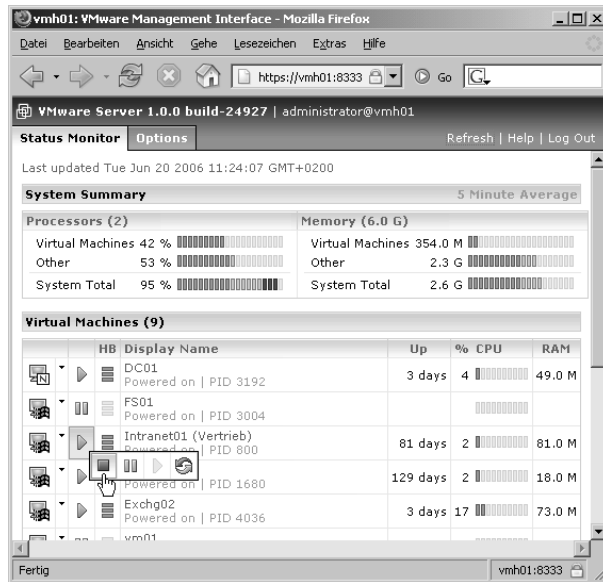
Das VMware Management Interface (Web-Interface) des VMware Servers

Das *VMware Management Interface*, auch Web-Interface genannt, hat beim VMware Server nur noch eingeschränkte Funktionalität. Beim GSX Server (dem kostenpflichtigen Vorgänger) war eine komplette Verwaltung der virtuellen Maschinen, zusätzlich zur VMware Server Console, möglich. Sie erreichen das Web-Interface in einem Browser mit der URL https://mein_host:8333. Mit dem Interface können Sie hauptsächlich folgende Dinge tun:

- ▶ Die VMware Server Console im Startbildschirm vom Web-Interface herunterladen und installieren (siehe *Teil 1, Kapitel 3*).

- ▶ Eine Übersicht über alle VMs auf dem Host mit Informationen zum verwendeten RAM, zur CPU-Zeit und zum Zustand betrachten und die VMs starten sowie beenden.
- ▶ Über OPTIONS/VIRTUAL MACHINE STARTUP AND SHUTDOWN legen Sie die Startreihenfolge der VMs auf dem Host fest. Das gilt für alle VMs, die beim Hochfahren des Hosts automatisch starten sollen (siehe *Startup/Shutdown* bei „Wichtige Einstellungen in Optionen zu jeder VM“).
- ▶ Bei der Arbeit mit Virtual Center erstellen Sie unter OPTIONS/NETWORK CONNECTIONS eindeutige Namen für die virtuellen Netzwerke über alle Hosts, so genannte *Network-Labels*.

Abbildung 4.5:
Das webbasierte
VMware Manage-
ment Interface bietet
einen Überblick über
verschiedene Para-
meter des Hosts und
der VM.



4.3.2 Die wichtigsten Funktionen und Tipps zur Bedienung von VMware Workstation und Server

Wo finden Sie unter der VMware Workstation und beim VMware Server die Funktionen, die für die tägliche Arbeit wichtig sind? Die Funktionen gleichen sich, nur einige wenige Menüpunkte nennen sich anders.

Grundlegender Aufbau der Konsolen von Workstation und Server

Favorites oder Inventory

Neben der üblichen Aufteilung in Menüleiste, Symbolleiste und Statusleiste sind die Fenster grundsätzlich in zwei Teile gegliedert. Links erschienen alle virtuellen Maschinen in einer Liste, FAVORITES bei der Workstation (Abbildung 4.3) bzw. INVENTORY beim Server (Abbil-

dung 4.4). Unter der Workstation lassen sich in den FAVORITES auch Unterordner erstellen, um in größeren Testumgebungen den Überblick über alle Einträge zu behalten, beim Server ist das nicht möglich.

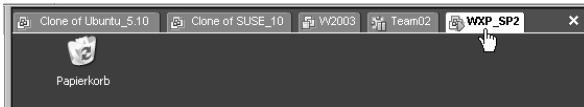


Abbildung 4.6:
Über die Virtual Machine Tabs können alle VMs im rechten Teil des Fensters erreicht werden

Auf der rechten Seite des Fensters ist jeder Gast über einen eigenen Karteikartenreiter zu erreichen, die so genannten *Virtual Machine Tabs* (Abbildung 4.6). Wenn eine VM ausgeschaltet ist, dann erscheinen in diesem rechten Teil Informationen zur Hardware-Ausstattung oder Bemerkungen wie der Pfad zur Konfigurationsdatei (Abbildung 4.4). Ist die VM eingeschaltet, dann sehen Sie stattdessen den Bildschirminhalt des Gastes (Abbildung 4.3). Die Anzeige können Sie über VIEW/CURRENT VIEW umschalten, etwa um bei laufendem Gast schnell einen Blick auf die Konfigurationsübersicht zu werfen.

Wenn der Gast läuft, zeigt die Statusleiste unten rechts kleine Symbole für die Hardware an. Sie erkennen z.B. die Netzwerkkarten- oder Festplattenaktivität (Abbildung 4.7). Mit einem Doppelklick auf ein solches Symbol gelangen Sie ohne Umwege zum Einstellungsdialog der Hardware. So schließen Sie eine Netzwerkkarte schnell an bzw. trennen sie vom Netz, oder Sie wechseln im laufenden Betrieb ein CD-ISO-Image. Beim VMware Server erscheint zusätzlich ein kleines Vorhängeschloss, das anzeigt, ob die Verbindung der Konsole zum Host über SSL gesichert ist oder nicht.

Hardware-Symbole zum Schnellzugriff

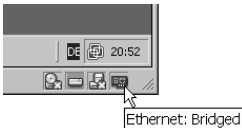
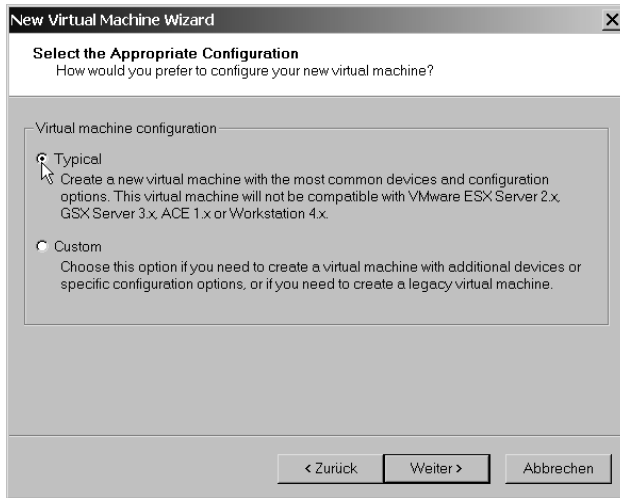


Abbildung 4.7:
Im laufenden Betrieb kann über die Statusleiste sehr praktisch auf die Eigenschaften virtueller Geräte zugegriffen werden

Neue VMs mit VMware Workstation und Server erstellen

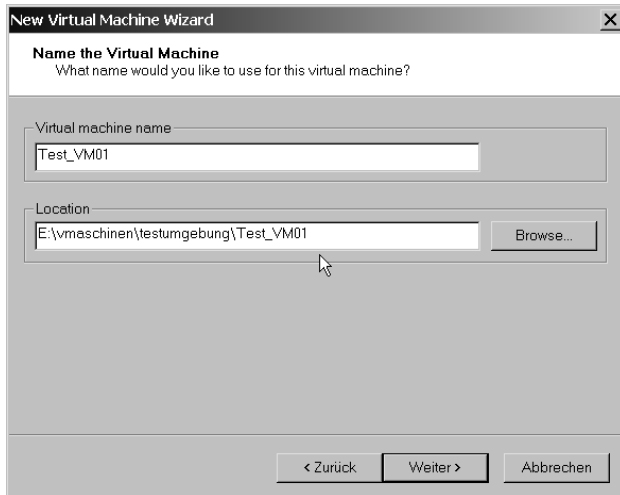
Mit FILE/NEW/VIRTUAL MACHINE starten Sie den Wizard zum Neuerstellen einer VM. Alle Details des Vorganges beschreibe ich detailliert in den Praxis-Workshops. Wählen Sie für Ihre ersten Testmaschinen bei der Abfrage zur Art der Konfiguration am einfachsten TYPICAL, damit werden die meisten Einstellungen schon automatisch vorbelegt, und das Erstellen ist nach wenigen Abfragen beendet (Abbildung 4.8). Mit der Konfigurationsart CUSTOM haben Sie etwas mehr Einfluss, etwa um bereits vorhandene virtuelle Platten einzubinden.

Abbildung 4.8:
Mit einer Typical
Konfiguration
erstellen Sie sehr
schnell die erste
virtuelle Maschine



Zuerst wählen Sie das Gastbetriebssystem aus, VMware optimiert nach dieser Angabe die VM mit sinnvoll vorgelegten Einstellungen, z.B. wird der Plattentyp SCSI oder IDE vorgelegt. Anschließend werden Sie nach dem Namen und dem Speicherort Ihres Gasts gefragt. Wenn Sie, wie in *Teil 1, Kapitel 3*, beschrieben, den Standardordner für die VMs schon eingestellt haben, legt VMware die neuen Gäste gleich dort ab. Sie können im entsprechenden Wizard-Dialog unter VIRTUAL MACHINE NAME einen passenden Namen für den Gast vergeben, dieser wird dann gleich automatisch als Ordner für die Dateien der VM unter LOCATION voreingestellt (Abbildung 4.9).

Abbildung 4.9:
Der Name einer
neuen VM kann
auch gleich als
Verzeichnisname für
den Ordner verwen-
det werden



Den abgefragten Typ der virtuellen Netzwerkkarte belassen Sie auf dem vorgelegten Wert *bridged*, und zum Abschluss erstellt der Wizard eine virtuelle Platte für die VM, wobei Sie die Größe anpassen kön-

nen. Wollen Sie eine vorhandene virtuelle Platte einbinden oder Einfluss auf den Typ IDE bzw. SCSI nehmen, dann sollten Sie den Wizard im Modus *Custom* starten oder nachträglich in der Konfiguration der VM über VM/SETTINGS/HARDWARE die Platte zuweisen.

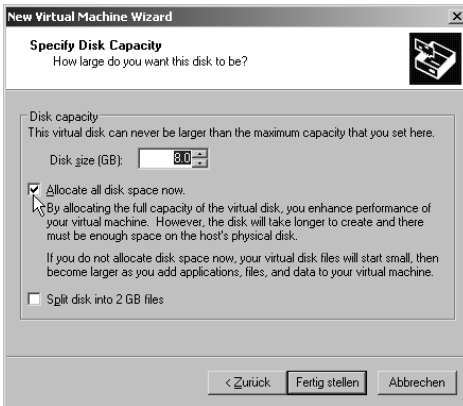


Abbildung 4.10:
Der VMware
Wizard für einen
neuen Gast erstellt
auch gleich die erste
virtuelle Platte

Beim VMware Server schlägt der Wizard vor, die virtuellen Platten in voller Größe (*Preallocated*) erstellen zu lassen. Das benötigt viel Platz, dauert teilweise sehr lange und ist höchstens in Produktionsumgebungen sinnvoll. Entfernen Sie den Haken an **ALLOCATE ALL DISK SPACE NOW** (Abbildung 4.10). Der Wizard erstellt dann eine virtuelle Zuwachsplatte in der maximalen Größe von standardmäßig 8 GB. Das bedeutet, die Platte belegt immer nur den Platz, der vom Gast tatsächlich verwendet wird, und wächst bei Bedarf bis zur maximalen Größe von 8 GB mit (siehe auch *Teil 3, Kapitel 3*).



VMs wieder von VMware Workstation und Server entfernen

Verweise zu den einzelnen VMs finden Sie an verschiedenen Stellen in den Konsolen, die Dateien einer VM liegen auf der Host-Festplatte:

- ▶ *VM aus den Favorites bzw. Inventory entfernen* – Durch einen Rechtsklick auf den Eintrag einer VM in der Liste unter FAVORITES | INVENTORY können Sie den Gast mittels REMOVE aus der Liste entfernen. Die VM bleibt aber auf der Festplatte erhalten, nur der Verweis wird gelöscht.
- ▶ *VM aus den Virtual Machine Tabs entfernen* – Mit einem Klick auf das kleine Kreuz ganz rechts in der Tab-Leiste (Abbildung 4.6) entfernen Sie die aktive VM aus den Tabs. Die VM bleibt dabei auf der Festplatte und unter FAVORITES | INVENTORY erhalten. Bei der Workstation wird eine laufende VM dadurch beendet, beim Server läuft die VM im Hintergrund als Dienst weiter. Beim nächsten Klick auf die gleiche VM unter FAVORITES | INVENTORY öffnet sich wieder ein neuer Tab.

- ▶ *VM von der Platte löschen* – Mit der rechten Maustaste auf einen Eintrag unter FAVORITES | INVENTORY oder auf einen Tab entfernen Sie die zugehörige VM mittels DELETE FROM DISK von der Festplatte. Achtung! Die VM wird damit komplett, samt virtueller Platten und Konfiguration, gelöscht! Sie können auch manuell das Verzeichnis der VM auf der Festplatte löschen und danach den verwaisten Eintrag unter FAVORITES | INVENTORY entfernen.

Eine vorhandene VM in VMware Workstation oder Server aufnehmen

Um vorhandenen VMs, die Sie vielleicht von einem anderen Host kopiert haben, in die Verwaltung der Konsole aufzunehmen gibt es mehrere Möglichkeiten:

- ▶ *Menü File/Open* – Im Menü FILE/OPEN können Sie zur Konfigurationsdatei (*.vmx) der VM navigieren und diese öffnen.
 - ▶ *Drag&Drop* – Mittels Drag&Drop können Sie die Konfigurationsdatei einer VM direkt vom Windows Explorer in die Favoritenleiste ziehen. Das funktioniert nur bei der VMware Workstation.
 - ▶ *Doppelklick auf *.vmx* – Im Windows Explorer starten Sie mit einem Doppelklick auf eine Konfigurationsdatei (*.vmx) ein neues VMware-Fenster. Dabei erscheint die VM automatisch in den Tabs und kann von dort mittels rechter Maustaste und ADD TO FAVORITES auch wieder zu den Favoriten hinzugefügt werden.
- Beim Server funktioniert das nur am Host selbst, die VM wird auch sofort automatisch im Inventory gelistet.
- ▶ *Menü File/Import* – Im Menü FILE/IMPORT können Sie Gäste von Virtual PC/Server oder aus Symantec-Images automatisch importieren und unter VMware verwenden.



VMs, die in der Liste bei FAVORITES | INVENTORY mit einem roten Kreuz dargestellt werden, existieren entweder nicht mehr oder befinden sich nicht mehr an der Stelle, wo VMware sie vermutet. Sie können diese Einträge entfernen, und die VM kann eventuell wieder neue aufnehmen.

VMs starten, beenden oder einfrieren (Suspend)

Um eine VM zu starten oder zu beenden, existieren vier Schaltflächen, die wie die Schalter eines echten Rechners (Abbildung 4.11) wirken.

Abbildung 4.11:
Mit vier Schaltern
werden VMs ein-
und ausgeschaltet



- ▶ **POWERON** – Dieser Schalter startet einen Gast.
- ▶ **POWEROFF** – Dieser Schalter beendet einen Gast. Sind die VMware Tools im Gast installiert, fahren Sie das Gastsystem vor dem

Abschalten noch sauber herunter. Das Verhalten legen Sie im Menüpunkt VM/SETTINGS/OPTIONS/POWER/POWER CONTROLS zu jedem Gast fest (Abbildung 4.12). Zusätzlich können Sie einen Gast über den Menüpunkt VM/POWER/POWEROFF immer sofort hart beenden; z.B. wenn das Gastsystem abgestürzt ist oder wenn Ihnen das Herunterfahren zu lange dauert. Dieser Menüpunkt wirkt auf den Gast immer wie ein virtueller Stromausfall.

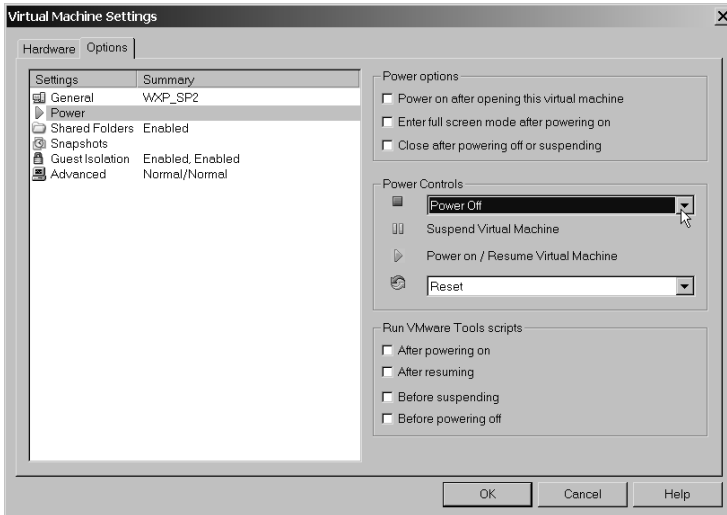


Abbildung 4.12:
Die VMware Tools
fahren bei PowerOff
oder Reset einen
Gast automatisch
herunter

- ▶ **SUSPEND** – Mit dieser Funktion speichert VMware den RAM-Inhalt und den aktuellen Status eines laufenden Gastes in zwei Dateien auf der Festplatte (*.vmss und *.vmem) und beendet die VM. Der nächste Start (Resume) stellt alle Informationen wieder her, und der Gast läuft nach wenigen Sekunden an genau der gleichen Stelle weiter. Damit sparen Sie sich das langwierige Herunter- und Hochfahren von Gästen in Testumgebungen.

Sie können die Suspend-Funktion auch zum schnellen Übertragen einer laufenden VM auf einen anderen Host-Rechner mit minimaler Ausfallzeit nutzen, indem Sie die VM in den Suspend-Modus bringen, auf eine andere Hardware kopieren und dort wieder zum Leben erwecken. Liegt die VM auf einem externen Speicher, etwa einer LAN-Freigabe, auf den beide Hosts Zugriff haben, dann geschieht das Abspeichern und Wiederherstellen des Status innerhalb weniger Sekunden, da nicht die gesamte VM kopiert werden muss (siehe auch Teil 2, Kapitel 8, „Cluster mit VMs und einem iSCSI Target als externem Speicher“).

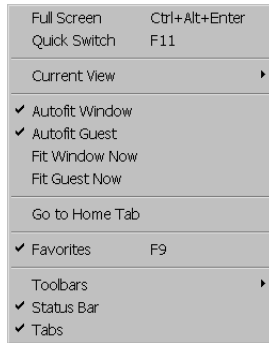


- ▶ **RESET** – Der Gast wird neu gestartet. Wie bei PowerOff können Sie auch für diesen Schalter einstellen, ob das Gastsystem vorher heruntergefahren wird oder nicht.

Steuerung der Bildschirmgröße und der Auflösung in den Gästen

Wenn ein Gast läuft, dann wird sein Bildschirm im Fenster auf der rechten Seite unter den Tabs angezeigt. Im Menü VIEW können Sie bestimmen, wie dabei die Bildschirmgröße dargestellt wird (Abbildung 4.13).

Abbildung 4.13:
Das Anpassen des
Fensters einer VM
und der Bildschirm-
auflösung des Gastes
kann automatisch
erfolgen



- ▶ FIT WINDOW NOW – Das VMware-Fenster wird an die Auflösung des Gastes angepasst. Hat der Gast eine höhere Auflösung, als das Fenster darstellen kann, dann erscheinen Scrollbalken.
- ▶ FIT GUEST NOW – Die Auflösung des Gastes wird an die Größe des VMware-Fensters angepasst. Das funktioniert nur, wenn die VMware Tools im Gast installiert sind.
- ▶ AUTO FIT... – Sind diese beiden Haken gesetzt, dann erfolgt die Anpassung der Auflösung oder der Fenstergröße automatisch. Sobald Sie die Größe des VMware-Fensters ändern, wirkt AUTO FIT GUEST. Stellen Sie dagegen im Gast eine andere Auflösung ein, wirkt AUTO FIT WINDOW.
- ▶ FULL SCREEN – Damit bringen Sie den Gast in den Vollbildmodus. Er nimmt die gesamte Größe des Host-Bildschirms ein, was wirkt, als würde das Gastsystem direkt auf der Hardware laufen. Zurück zum Host gelangen Sie mit **[Strg] + [Alt]**. Nur beim VMware Player erscheint im Vollbild ganz oben eine kleine Leiste, über die Sie wieder zurück ins Fenster gelangen.



Was beim Umschalten ins Vollbild mit der Bildschirmauflösung im Gast passieren soll, das können Sie unter VMware Workstation im Menü EDIT/PREFERENCES/DISPLAY/FULLSCREEN festlegen. Entweder skalieren die VMware Tools den Gast auf die aktuelle BildschirmEinstellung des Hosts, oder der Gast behält seine Auflösung, was bei LCD-Bildschirmen allerdings oft zu unscharfer Darstellung oder schwarzen Rändern führt.

- QUICK SWITCH – Eine sehr praktische Variante des Vollbildmodus ist der Quick-Switch-Modus. Dabei bleibt im Vollbild die Tab-Leiste erhalten, und Sie können zwischen verschiedenen laufenden VMs umschalten, ohne jedes Mal erst den Vollbildmodus verlassen zu müssen. Zusätzlich erscheint am oberen Rand des Bildschirms die Menüleiste, sobald Sie den Mauszeiger ganz nach oben bewegen. Darüber beenden Sie den Quick-Switch-Modus auch wieder.

Für die Funktionen *Quick Switch* und *Full Screen* existieren zusätzlich zum Menü auch zwei Symbole, die ein komfortables Umschalten ermöglichen (Abbildung 4.14).



Abbildung 4.14:
Für die Funktionen
Quick Switch und
Full Screen existie-
ren zusätzlich zum
Menü auch zwei
Symbole

Tastatur, Maus und FoKuswechsel zwischen Gast und Host

Ob Tastaturanschläge und Mausebewegungen in einem Gast oder auf dem Host wirken, wird davon bestimmt, wer den Fokus hat. Hier spielen auch wieder die VMware Tools eine entscheidende Rolle. Ohne die Tools müssen Sie erst in ein Gastfenster klicken, um darin arbeiten zu können, z.B. während der neuen Installation eines Betriebssystems. Den Gast können Sie dann nur mit der Tastenkombination **[Strg] + [Alt]** wieder verlassen.

[Strg] + [Alt]

Bei installierten VMware Tools erfolgt der Fokuswechsel automatisch, sobald Sie die Maus ins Fenster einer VM ziehen oder wieder in den Bereich des Hosts schieben. Dabei kann es vorkommen, dass sich Ihr Mauszeiger zufällig nicht mehr im Bereich des Gastfensters befindet. Wenn Sie Tastatureingaben machen, landen diese dadurch auf dem Host und nicht im Gast. Sie müssen den Mauszeiger einfach wieder ins Gastfenster bringen, um dort weiterzuschreiben. Sie können auch einstellen, dass bereits ein Tastendruck im aktiven VMware-Fenster genügt, um den Fokus zu erhalten, egal wo der Mauszeiger in diesem Moment steht. Oder Sie legen fest, dass der Fokuswechsel nie automatisch erfolgt. Das gesamte Verhalten steuert der Menüpunkt EDIT/PREFERENCES/INPUT (Abbildung 4.15). Hier bestimmen Sie bei Bedarf auch einen anderen Hotkey als **[Strg] + [Alt]**.

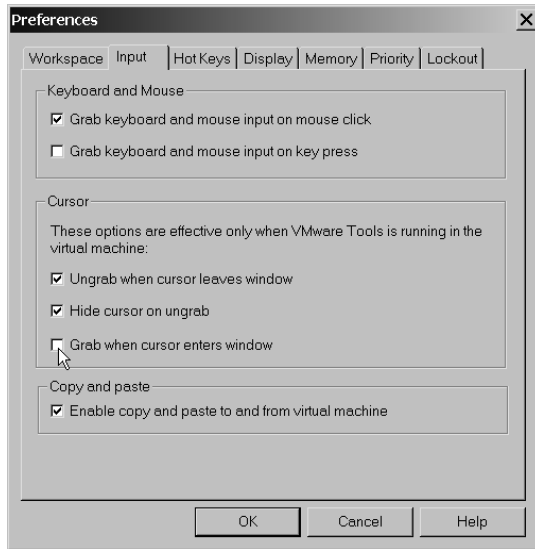
Fokuswechsel dank VMware Tools

Im Unterschied zu allen anderen Tastaturaktionen kann VMware die Kombination **[Strg] + [Alt] + [Entf]** nicht abfangen. Sie wirkt immer auf den Host selbst. Aus diesem Grunde existieren zwei andere Möglichkeiten, um diese Kombination an einen Gast zu senden.

**[Strg] + [Alt] +
[Entf]**

- Als Ersatz können Sie die Kombination **[Strg] + [Alt] + [Einfg]** drücken, wenn die VM den Fokus hat.
- Über das Menü können Sie mittels VM/SEND **[Ctrl] + [Alt] + [Del]** ebenfalls die Kombination an den Gast senden.

Abbildung 4.15:
Das Verhalten von
Maus und Tastatur
beim Wechsel
zwischen Gast und
Host lässt sich
detailliert festlegen



Einen Screenshot machen oder ein Video aufzeichnen

Eine sehr praktische Funktion ist die Möglichkeit, unter VMware Workstation das gesamte Geschehen in einem Gast mittels VM/CAPTURE MOVIE als Video aufzuzeichnen. Aus dem Mitschnitt kann ein Lehrvideo oder eine Software-Demo erstellt werden. Diese Funktion steht im VMware Server nicht zur Verfügung. Server und Workstation beherrschen aber beide das Anfertigen eines statischen Screenshots vom Gast-Bildschirm mittels VM/CAPTURE SCREEN bzw. FILE/CAPTURE SCREEN.



Wenn Sie vom Gastsystem einen Schnappschuss mit Mauszeiger machen wollen, verlassen Sie das Fenster mit **[Strg] + [Alt]**. Dabei werden im Gast leider manche geöffnete Menüs geschlossen, z.B. das Startmenü oder Kontextmenüs. Um das zu verhindern, wählen Sie unter EDIT/PREFERENCES/HOT KEYS einen *Custom*-Hotkey, z.B. *Ctrl* (Abbildung 4.16) Laufende Gäste müssen nach der Änderung neu gestartet werden.

Ab jetzt verlassen Sie den Gast mit **[Strg]**, wobei alle Menüs geöffnet bleiben. Wenn der Mauspfel im Gast beim Verlassen verschwindet, dann liegt das an der Option EDIT/PREFERENCES/INPUT/HIDE CURSOR ON UNGRAB.

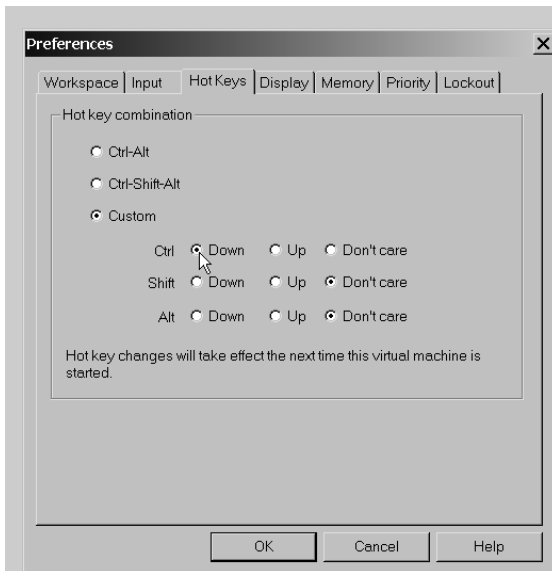


Abbildung 4.16:
Es ist auch möglich,
einen anderen Hot-
key zum Verlassen
des Gastes zu wählen

Für viele aufeinander folgende Screenshots ist ein Screenshot-Tool direkt im Gast (z.B. IrfanView) wesentlich praktischer, weil VMware bei jedem Schnappschuss erst den Dialog *Speichern unter* öffnet und das ständige Verlassen des Gastes recht umständlich ist. Außerdem kann die Funktion von VMware nur den gesamten Bildschirm und keine bestimmten Fenster im Gast fotografieren.

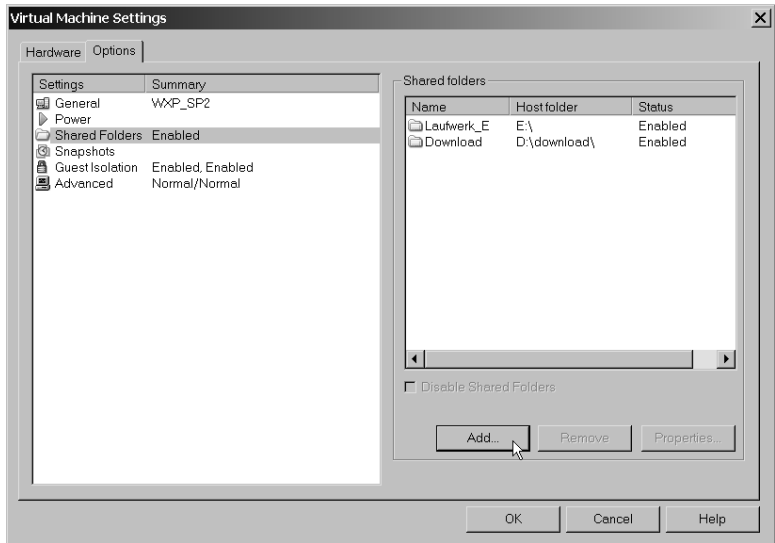
Datenaustausch über Copy&Paste, Drag&Drop oder Shared Folders

Laufen die VMware Tools in einem Gast, dann kopieren Sie Texte mittels *Copy&Paste* zwischen den VMs und dem Host. Nur die Workstation und der Player beherrschen auch *Drag&Drop*, wodurch Sie ganze Dateien einfach mit der Maus in ein Gastfenster ziehen können, um diese in den Gast zu kopieren oder umgekehrt. Diese Funktionen können über EDIT/PREFERENCES/INPUT/COPY AND PASTE bzw. VM/SETTINGS/OPTIONS/GUEST ISOLATION (Letzteres nur an der Workstation) auch unterbunden werden, etwa aus Sicherheitsgründen.

Shared Folders sind eine weitere Funktion, die nur die VMware Workstation beherrscht. Während man mit *Drag&Drop* schnell einige wenige Dateien hin und her kopieren kann, bieten *Shared Folders* den permanenten Zugriff aus den Gästen auf bestimmte freigegebene Ordner des Hostrechners. Damit richten Sie ein Verzeichnis zum Datenaustausch ein, um nicht jede benötigte Datei erst in den Gast kopieren zu müssen, z.B. eine Setup-Routine für ein bestimmtes Programm.

**Shared Folders
zum Datenaus-
tausch**

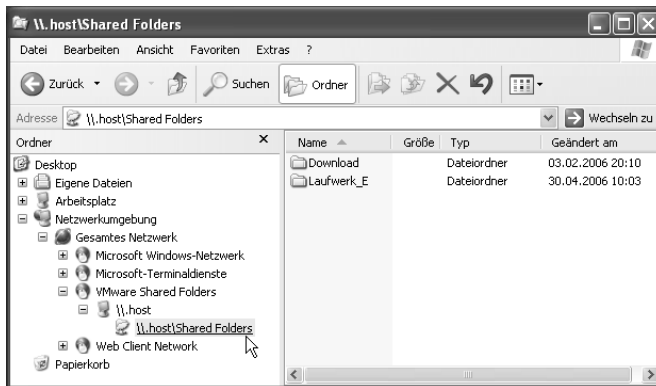
Abbildung 4.17:
Shared Folders sind
Freigaben von Ver-
zeichnissen des
Hosts



Unter Linux
/mnt/hgfs

Sie schalten die Funktion der Shared Folders über VM/SETTINGS/OPTIONS/SHARED FOLDERS ein (Abbildung 4.17). Die hier freigegebenen Verzeichnisse erscheinen in einem Windows-Gast unter der Netzwerkumgebung bei `\\.\host\Shared Folders` (Abbildung 4.18). In einem Linux-Gast werden die Ordner im Verzeichnis `/mnt/hgfs` sichtbar.

Abbildung 4.18:
Shared Folders er-
scheinen im Gast als
Netzwerkfreigaben



Hauptspeicherverwaltung für den Host und die Gäste unter VMware

Neben der einfachen Zuweisung der RAM-Größe für jeden Gast unter VM/SETTINGS/HARDWARE/MEMORY bestimmt am Host eine zentrale Einstellung, wie der verfügbare physische Hauptspeicher zugeteilt wird. Sie finden den Menüpunkt MEMORY bei der Workstation unter EDIT/PREFERENCES und beim Server unter HOST/SETTINGS (Abbildung 4.19). Hier stellen Sie unter RESERVED MEMORY mit einem Schieberegler zuerst ein, wie viel RAM alle VMs verwenden

dürfen und wie viel auf jeden Fall für den Host reserviert bleibt. Die Standardeinstellung muss höchst selten angepasst werden. Nur bei Performanceproblemen, wenn auf dem Host noch andere speicherhungrige Applikationen laufen, sollten Sie den Regler etwas nach links ziehen, um dem Host mehr Luft zum Atmen zu geben.

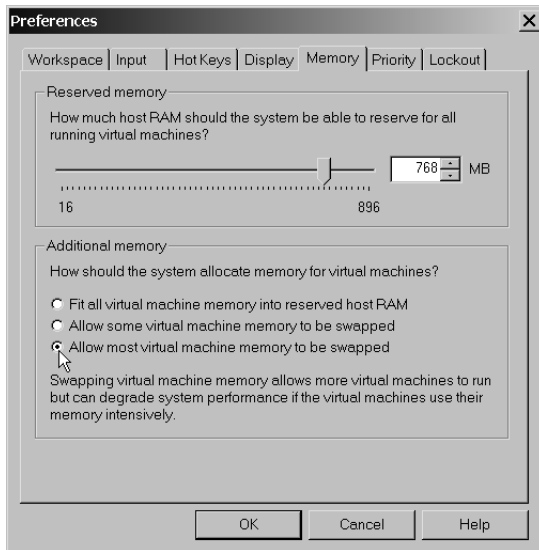


Abbildung 4.19:
Der physische RAM
kann zwischen den
Gästen und dem Host
aufgeteilt werden.
Zusätzlich stellt
VMware virtuellen
Speicher bereit

Wichtiger ist die Auswahl ADDITIONAL MEMORY darunter. Sie bestimmt, wie sich der Host verhält, wenn VMs gestartet werden sollen, denen zu viel Speicher zuwiesen wurde. Normalerweise kann RAM nicht emuliert werden. Also dürften nur so viele VMs laufen, wie Speicher im Host eingebaut ist. Ich bin in *Teil 1, Kapitel 1*, bereits auf die Möglichkeit von VMware eingegangen, mehr Hauptspeicher zur Verfügung zu stellen, als eigentlich vorhanden ist. Mit den Einstellungen an dieser Stelle können Sie das erlauben oder verbieten (Abbildung 4.19).

**Mehr Speicher
zuweisen als
physisch vor-
handen ist**

Nehmen wir an, Sie haben einen Host mit 1024 MB physischem RAM. Für die VMs wurden mit dem Schieberegler 768 MB reserviert, es bleiben also 256 MB für den Host. Sie wollen drei VMs mit jeweils 512 MB zugewiesenem RAM laufen lassen. Die Einstellungen wirken folgendermaßen:

- ▶ Fit all virtual machine memory into reserved host RAM – Sie können nur eine VM starten, bereits die zweite würde den verfügbaren Hauptspeicher überschreiten. Beim Start der zweiten VM erscheint eine Fehlermeldung.
- ▶ Allow some virtual machine memory to be swapped – Sie können zwei Maschinen starten. Der physische RAM wird damit eigentlich schon um 256MB überschritten. Aber das Speichermanagement von VMware lässt leichte Überschreitungen zu. Bei der dritten VM ist dann aber Schluss, beim Start erscheint eine Fehlermeldung.

- Allow most virtual machine memory to be swapped – Sie können alle drei VMs starten. Damit wird der physische RAM um 768 MB überschritten. In diesem extremen Beispiel muss das System allerdings massiv Hauptspeicherseiten in eine Festplattendatei auslagern (*swappen*), und die Performance der Gäste und des Host-Systems bricht zusammen.

In der Praxis hilft oft nur Ausprobieren. Selbst in Produktionsumgebungen kann eine leichte Mehrzuweisung von Hauptspeicher funktionieren. Trotzdem wird das Feature vor allem in Testumgebungen mit vielen Maschinen eine nützliche Hilfe sein, wenn man den Bogen dabei nicht überspannt.



Da die Verwaltung der Gäste auch etwas Speicher benötigt, entsteht ein leichter Overhead, wodurch die Gäste in der Praxis etwas mehr Hauptspeicher beanspruchen, als ihnen zugewiesen wurde. Dadurch kann es bei der Einstellung *Fit all virtual machine memory into reserved host RAM* dazu kommen, dass sich keine Gäste mehr starten lassen, obwohl rein rechnerisch noch RAM frei wäre.

Performanceprobleme durch die Speicherverwaltung von VMware

Memory Trimming und Page Sharing

VMware empfiehlt bei besonders I/O-lastigen Anwendungen, im Gast die Funktionen zur Speicherverwaltung abzuschalten, die dafür sorgen, dass sich mehrere VMs gleiche Speicherseiten teilen (*Memory Page Sharing*) bzw. unbenutzter Speicher eines Gastes an andere VMs vergeben werden kann (*Memory Trimming*). Sollten Sie Probleme mit der Leistung einer VM haben, finden Sie die Einstellungen unter VM/SETTINGS/OPTIONS/ADVANCED.

Wichtige Einstellungen in Optionen zu jeder VM

Unter VM/SETTINGS/OPTIONS finden Sie zu jedem Gast weitere wichtige Einstellungen, die das Verhalten der VM bestimmen (Abbildung 4.20). Viele davon sind selbsterklärend, die meisten benötigen Sie nicht sofort. Die wichtigsten Optionen finden Sie hier. Das automatische Herunterfahren, die Shared Folders und die Skripte im Gast funktionieren nur dann, wenn die VMware Tools in den VMs installiert sind.

- *General* – Sie können den Namen der VM ändern und das Arbeitsverzeichnis anpassen, in dem VMware die Redo-Logs oder die RAM-Inhalte bei Suspend und Snapshot speichert, um diese Dateien beispielsweise auf einer anderen Festplatte abzulegen. Normalerweise müssen Sie hier keine Änderungen vornehmen.



Um schnell zum Ordner einer VM zu gelangen, etwa um die Dateien zu sehen, können Sie hier aus dem Feld WORKING DIRECTORY den Pfad kopieren und im Windows Datei-Explorer in die Adressleiste einfügen.

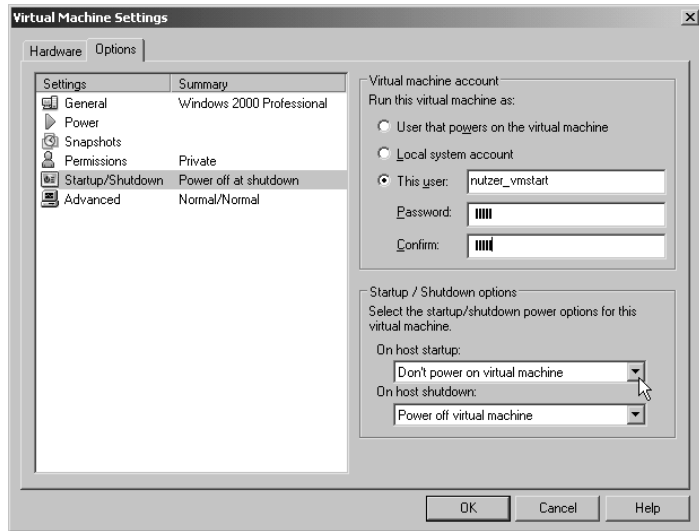
- ▶ *Power* – Hier legen Sie unter anderem fest, ob beim Betätigen des Power-Buttons das System einfach abschaltet oder ob die VMware Tools versuchen, es sauber herunterzufahren (Abbildung 4.12). Weiterhin können Sie unter TOOLS SCRIPTS festlegen, ob in einem Gast bei bestimmte Aktionen Skripte ausgeführt werden, die Sie im Gast hinterlegen können. Sie finden die Skripte bei installierten VMware Tools im Gast unter `C:\Programme\VMware\VMware Tools`, z.B. `resume-vm-default.bat`.
- ▶ *Shared Folders* – Diese Funktion existiert nur an der VMware Workstation. Hier geben Sie Verzeichnisse des Hosts frei, die dann im Gast in der Netzwerkumgebung erscheinen. Voraussetzung sind installierte VMware Tools im Gast. Siehe „Datenaustausch über Copy&Paste, Drag&Drop oder Shared Folders“.
- ▶ *Snapshot* – An dieser Stelle unterbinden Sie Snapshots generell für einen Gast oder sperren den aktuellen Snapshot beim VMware Server gegen Überschreiben. Die gesamte Snapshot-Funktion beschreibe ich in *Teil 3, Kapitel 4, „Die Snapshot- und Clone-Funktion der VMware-Produkte“*.
- ▶ *Permissions* – Dieser Punkt existiert nur am VMware Server. Sie legen mit `MAKE THIS VIRTUAL MACHINE PRIVAT` fest, ob die VM in der Remote-Konsole von allen Nutzern gesehen wird oder ob sie nur noch dem Benutzer gehört, der den Haken an dieser Stelle gesetzt hat.
- ▶ *Startup/Shutdown* – Dieser Punkt existiert nur am VMware Server. Er ist eines der entscheidenden Kriterien, die den Server von den Desktop-Produkten abheben. Wenn Sie hier einen bestimmten Nutzer hinterlegen oder das Systemkonto wählen, dann läuft die VM als Dienst im Hintergrund. Sie läuft damit auch weiter, wenn am Host kein Nutzer angemeldet ist (Abbildung 4.20). Weiterhin bestimmen Sie, ob die VM beim Hochfahren des Hosts mit dieser Nutzeranmeldung automatisch startet bzw. beim Herunterfahren automatisch beendet wird. Damit genügt es, nur den Host herunterzufahren, um den Rest kümmert sich VMware. Das ist beispielsweise bei Stromausfall für die Konfiguration der USV-Steuerung sehr praktisch.

Beispiel USV-Steuerung

Für alle Gäste mit Autostart können Sie im *Web-Interface* über `OPTIONEN` auch die Reihenfolge des Starts und Zeitabstände festlegen, um z.B. den Domänencontroller vor den restlichen Maschinen hochzufahren. Leider ist diese Funktion noch nicht über die VMware Server Console erreichbar.



Abbildung 4.20:
Der VMware Server
kann Gäste als
Dienst unter einem
wählbaren Account
laufen lassen und
automatisch mit
dem Host starten



- **Guest Isolation** – Diese Funktion existiert nur an der VMware Workstation. Sie können Drag&Drop für bestimmte Gäste abschalten, um diese Gäste zu isolieren.
- **Advanced** – Hier legen Sie z.B. fest, welche Priorität ein Gast hat, wenn er den Fokus besitzt bzw. wenn er im Hintergrund läuft. Sie können auch die intelligente Speicherverwaltung von VMware abschalten. Der Template-Modus schützt VMs der VMware Workstation vor Löschen, wenn Sie als Vorlage für *Linked Clones* dienen (siehe Teil 3, Kapitel 4, „Die Snapshot- und Clone-Funktion der VMware-Produkte“).

Weitere Funktionen wie Snapshots, Netzwerk oder Clones

Mit den hier vorgestellten Funktionen können Sie die Produkte von VMware ausreichend bedienen und Ihre ersten Testumgebungen aufbauen. In Teil 2 des Buches finden Sie zahlreiche Anwendungsbeispiele.

Die umfangreichen Funktionen von VMware zum Netzwerk werden in Teil 3, Kapitel 2, behandelt und im Praxis-Workshop von Teil 2, Kapitel 3, „*Virtuelle DMZ mit Firewall und Webserver im Internet*“ umgesetzt.

Zu den Snapshots, Clones und Teams existiert ebenfalls ein eigener Workshop in Teil 3, Kapitel 4, genauso zu den virtuellen Platten in Teil 3, Kapitel 3.

4.4 VMware Tools in Windows- und Linux-Gästen installieren

Wie ich bereits erwähnt habe, sollten Sie in jedem Gast die VMware Tools installieren, um damit in den Genuss einer erweiterten Funktionalität Ihrer VMs zu kommen.

4.4.1 Installation der VMware Tools in Windows-Gästen

In einem Windows-Gast installieren Sie die Tools einfach über den Menüpunkt VM/INSTALL VMWARE TOOLS. Dabei passiert Folgendes:

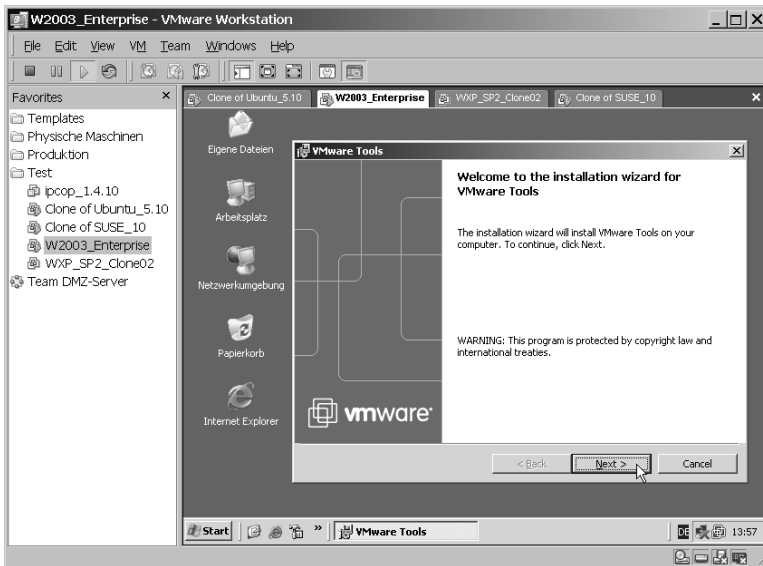


Abbildung 4.21:
Die Installation der
VMware Tools
erfolgt automatisch
von einem ISO-
Image und ist in
Windows-Gästen
selbsterklärend

1. VMware legt automatisch ein ISO-Image ins virtuelle CD-ROM-Laufwerk ein. Auf diesem ISO-Image befinden sich die Installationsdateien der Tools. Für verschiedene Gastsysteme existieren unterschiedliche Images im Programmverzeichnis von VMware, z.B. C:\Programme\VMware\VMware Workstation\windows.iso.
2. Ist im Windows-Gast CD-Autorun aktiv, was meist der Fall ist, startet das Setup der Tools automatisch (Abbildung 4.21). Mit der Option *Custom* erhalten Sie zu Beginn des Setups einen Überblick über die zu installierenden Komponenten (Abbildung 4.1). Sie können die *Setup.exe* auch manuell von der CD im Gast starten, wenn das Setup nicht von allein beginnt.
3. Das ISO-Image wird nach erfolgter Installation wieder abgehängt. Sollte das nicht automatisch geschehen, dann hilft der Menüpunkt VM/CANCEL VMWARE TOOLS INSTALL.

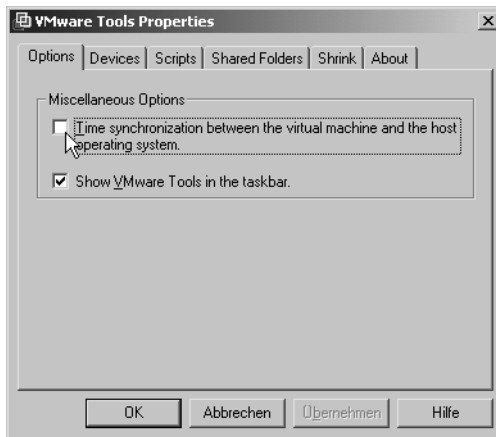
Abbildung 4.22:
Bei installierten
VMware Tools er-
scheint ein Symbol
in der Taskleiste des
Gastsystems



Skripte der VMware Tools

Wenn die Tools in der VM laufen, sehen Sie unten rechts in der Taskleiste des Gastsystems ein kleines Symbol (Abbildung 4.22), über das Sie eine Toolbox starten können. In dieser VMware Toolbox lassen sich Zeitsynchronisation, bestimmte Geräte oder die Skripte ein- und ausschalten (Abbildung 4.23). Weiterhin kann das Verdichten (*Shrink*) der virtuellen Platten mit den Tools im Gast vorbereitet werden (siehe Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“).

Abbildung 4.23:
Einige Funktionen
der VMware Tools
können direkt im
Gast ein- und ausge-
schaltet werden



4.4.2 Installation der VMware Tools in Linux-Gästen

Compiler und Kernel-Header

Unter Linux ist die Installation der VMware Tools nicht ganz so komfortabel wie in einem Windows-Gast. Aber wenigstens gilt es in den aktuellen Linux-Distributionen unter den neuen VMware-Versionen nicht mehr, all die Klippen zu umschiffen, die in älteren Varianten lauerten. Trotzdem – sollte es zu Problemen kommen, beachten Sie bitte die Voraussetzungen zur VMware-Installation unter Linux in Teil 1, Kapitel 3, sie gelten auch für die Tools! Compiler und Kernel-Header werden immer dann benötigt, wenn VMware keine passenden Binärmodule (fertig übersetzte Programme) für die aktuelle Version Ihrer im Gast installierten Distribution mitliefert. Dann muss das Installationsskript die Module für die VMware Tools aus den Quellen neu übersetzen. Die daraus resultierenden Probleme habe ich bereits in Teil 1, Kapitel 3, zusammengefasst.



Achten Sie unter Linux immer auf Groß- und Kleinschreibung bei Befehlen und Dateinamen! Sie können eine praktische Funktion zur automatischen Ergänzung von Befehlen an der Kommandozeile nutzen. Wenn Sie in einem Befehl ein Verzeichnis oder eine Datei angeben müssen, z.B. den Namen des Installationspaketes, dann genügt es oft, nur die ersten eins bis zwei Buchstaben des Dateinamens zu tippen und dann  zu drücken. Existiert im Verzeichnis eine Datei mit passendem Namen, ergänzt die Shell automatisch den Befehl. Existieren mehrere Dateien mit dem gleichen Anfang, zeigt ein nochmaliger Druck auf  alle Dateinamen an. Zum Starten der Installation der Tools tippen Sie z.B. nur Folgendes ein:

```
./v 
```

Die Linux-Shell ergänzt den Befehl automatisch mit dem vollen Namen des Installationsskripts der VMware Tools, vorausgesetzt Sie stehen im richtigen Verzeichnis:

```
./vmware-install.pl
```

Die VMware Tools für Linux stellt VMware in zwei Versionen bereit, als TAR- oder als RPM-Paket. Beide Pakete befinden sich in der Datei *linux.iso* im VMware-Installationsverzeichnis auf dem Host. Sobald Sie im Menü den Punkt VM/INSTALL VMWARE TOOLS wählen, wird das ISO-Image ins virtuelle CD-Laufwerk eingehängt und erscheint im Gastsystem als eingelegte CD. Ab jetzt unterscheiden sich die Methoden. Es kommt auf die Distribution an, welchen Weg der Installation Sie wählen sollten. Ich erkläre den Vorgang wieder an zwei Beispielen mit verschiedenen Distributionen.

TAR oder RPM in der ISO-Datei

Installation der Tools mit dem TAR-Paket unter Ubuntu Linux:

Unter vielen Distributionen ist es besser, die Tools an der Kommandozeile zu installieren, während die grafische Benutzeroberfläche, wie GNOME oder KDE, nicht läuft.

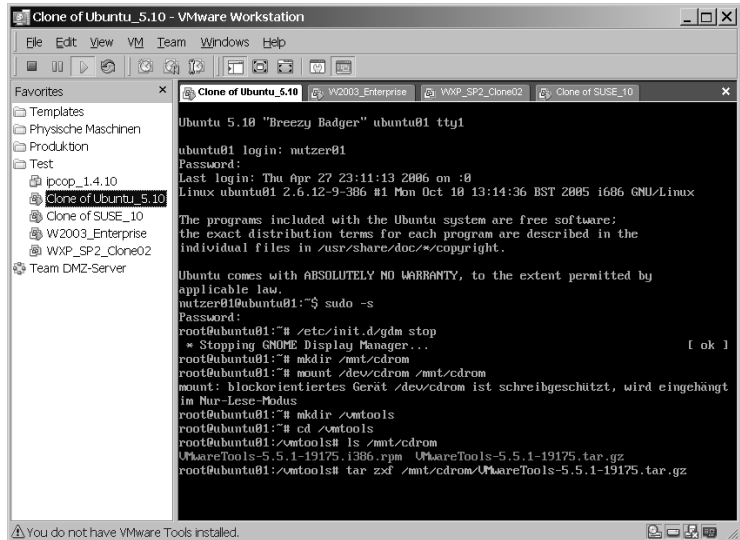
1. Wählen Sie im Menü den Punkt VM/INSTALL VMWARE TOOLS, um dem Gast das ISO-Image mit den VMware Tools als CD zuzuweisen.
2. Die Installation der Tools im Gast erfolgt auf der Kommandozeile (Abbildung 4.24). Sie beenden die grafische Benutzeroberfläche folgendermaßen:

Halten Sie die Tastenkombination  +  + , lassen Sie nur  wieder los, und drücken Sie  – lassen Sie dabei  +  zwischenzeitlich nicht los! Damit gelangen Sie auf die Kommandozeile. Normalerweise erledigt das die Kombination  +  + , aber unter VMware ist der kleine Umweg mit der Umschalttaste notwendig. Solange GNOME noch läuft, gelangen Sie mit  +  +  +  wieder zurück zur grafischen Oberfläche.

Zur Kommandozeile wechseln

3. An der Kommandozeile melden Sie sich mit dem Nutzer an, den Sie auch zur Anmeldung unter GNOME verwenden. Eine Anmeldung mit *root* funktioniert bei Ubuntu Linux nicht.

Abbildung 4.24:
Die Installation der
VMware Tools erfolgt
am sichersten von der
Kommandozeile ohne
laufende GUI



4. Geben Sie folgenden Befehl ein, um für die weiteren Kommandos *root*-Rechte zu erhalten. Dabei werden Sie nach dem Passwort des Nutzers *root* gefragt:

```
sudo -s
```

5. Jetzt können Sie die grafische Oberfläche GNOME beenden (oder KDE bei Kubuntu):

```
/etc/init.d/gdm stop
```

bzw.

```
/etc/init.d/kdm stop
```

6. Die CD mit den Tools ist zu mounten, und anschließend wird das TAR-Paket im neu angelegten Verzeichnis *vmtools* entpackt. Dort können Sie die Dateien später jederzeit wieder zu einer Neuinstallation verwenden:

```
mkdir /mnt/cdrom
mount /dev/cdrom /mnt/cdrom
mkdir /vmtools
cd /vmtools
```

Sie können sich den Inhalt der CD anzeigen lassen:

```
ls /mnt/cdrom
```

Das TAR-Paket ist zu entpacken, die aktuellen Versionsnummern müssen Sie ersetzen:

```
tar xzf /mnt/cdrom/VMwareTools-X.X.X-xxxxx.tar.gz
```

Die CD sollte wieder dismountet werden:

```
umount /mnt/cdrom
```

Installationsdateien auspacken

- Die eigentliche Installation der VMware Tools erfolgt mit einem Skript. Zuerst wechseln Sie ins Verzeichnis der ausgepackten Installationsdateien:

```
cd /vmtools/vmware-tools-distrib
```

Dann starten Sie das Installationsskript, wobei Sie alle Fragen der Installationsroutine mit den Standardvorgaben beantworten können:

```
./vmware-install.pl
```

- Das Installationsskript fragt Sie am Ende, ob es das Konfigurationsskript `/usr/bin/vmware-config-tools.pl` automatisch starten soll, worauf Sie mit *yes* antworten. Anschließend können Sie in einer Liste die Bildschirmauflösung wählen, die Ihr Gast verwenden soll. Das wird später die maximale Auflösung sein, bis zu der Ihr Gast skalieren kann. Geben Sie hier am besten die Auflösung Ihres Host-Systems an (Abbildung 4.27). Sie können `vmware-config-tools.pl` jederzeit wiederholen, um z.B. eine höhere Maximalauflösung zu konfigurieren.

vmware-config-tools.pl

- Die Benutzeroberfläche GNOME kann wieder starten:

```
/etc/init.d/gdm start
```

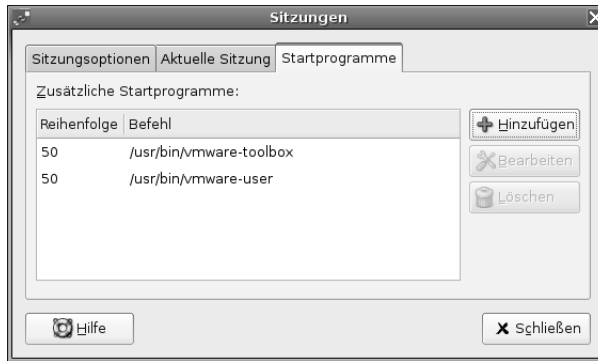
Die Tools sind fertig installiert. Als Beispiel, welche Probleme es bei der Installation unter Linux geben kann, ist unter Ubuntu Linux nach der Installation noch der Menüpunkt VIEW/FIT GUEST NOW ausgegraut, mit dem die Auflösung des Gastes an das VMware-Fenster angepasst werden kann. Schuld daran sind einige fehlende Linux-Module, die Sie am einfachsten auf der Kommandozeile mittels *APT* aus dem Internet oder von der Distributions-CD im Gast nachinstallieren können:

Probleme unter Ubuntu mit Fit Guest Now

```
apt-get update  
apt-get install gdk-imlib1
```

Sollte die Funktion FIT GUEST NOW beim nächsten Neustart des Gastes wieder nicht verfügbar sein, dann starten Sie die notwendigen Programme der Tools automatisch zusammen mit Ihrer GNOME-Sitzung. Einstellen lässt sich das im Gast über SYSTEM/EINSTELLUNGEN/SITZUNGEN/STARTPROGRAMME (Abbildung 4.25). Für die Funktion FIT GUEST NOW ist das Programm `/usr/bin/vmware-user` zuständig.

Abbildung 4.25:
Die Programme der
VMware Tools star-
ten nicht in allen
Distributionen auto-
matisch. Die Toolbox
muss nicht unbe-
dingt laufen

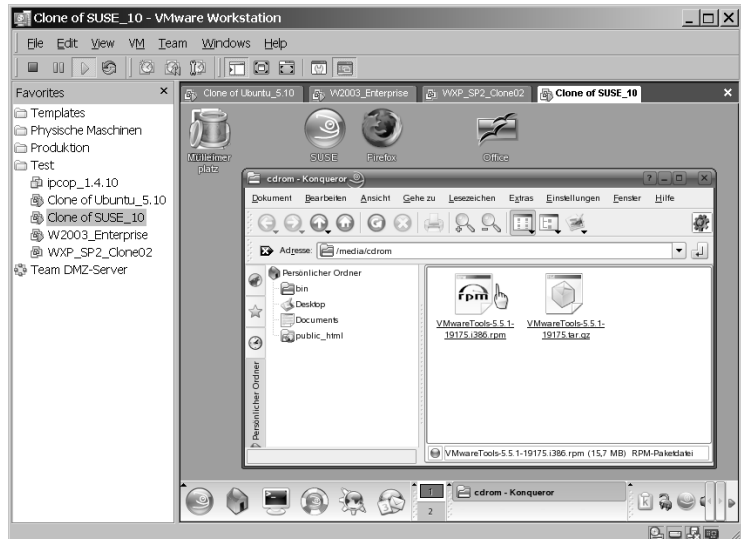


Installation mit dem RPM-Paket unter SUSE 10 Linux

In diesem Beispiel mit SUSE Linux installieren Sie die VMware Tools mit dem RPM-Paket direkt unter der grafischen Benutzeroberfläche KDE, was etwas komfortabler ist als an der Kommandozeile:

1. Wählen Sie den Menüpunkt VM/INSTALL VMWARE TOOLS, wodurch das ISO-Image *linux.iso* mit den Installationspaketen automatisch dem Gast zugewiesen wird. Im Gast bestätigen Sie die Frage zum automatischen Öffnen der eingelegten CD.
2. In einem Fenster im Gastssystem erscheint automatisch der Inhalt der CD im Dateimanager *Konqueror* (Abbildung 4.26). Sie finden dort ein Icon zum RPM-Paket der VMware Tools. Mit einem Klick öffnen Sie das Paket, und mit dem Button **PAKET MIT YAST INSTALLIEREN** startet die Installation. Dabei wird Ihr *root*-Passwort abgefragt.

Abbildung 4.26:
Die Installation in
einem SUSE-Gast
kann unter KDE
erfolgen



3. Jetzt installiert *Yast* die VMware Tools, was Sie am Fortschrittsbalken verfolgen können. Zum Abschluss der Installation erscheint keinerlei Bestätigungsmeldung. Das Konquerer-Fenster können Sie schließen.
 4. Wechseln Sie jetzt in ein Terminalfenster, und verschaffen Sie sich mit dem Befehl `sudo root`-Rechte. Der Befehl fragt Sie nach dem Passwort des Nutzers *root*:
- ```
sudo -s
```
5. Mit dem Befehl `/usr/bin/vmware-config-tools.pl` starten Sie im Terminalfenster die Konfiguration der Tools. Dabei werden Sie nach der Bildschirmauflösung gefragt, die Ihr Gast verwenden soll. Das wird später die maximale Auflösung sein, bis zu der Ihr Gast skalieren kann. Geben Sie hier am besten die Auflösung Ihres Host-Systems an (Abbildung 4.27). Sie können `vmware-config-tools.pl` jederzeit wiederholen, um z.B. eine höhere Maximalauflösung zu konfigurieren.

**vmware-config-tools.pl**

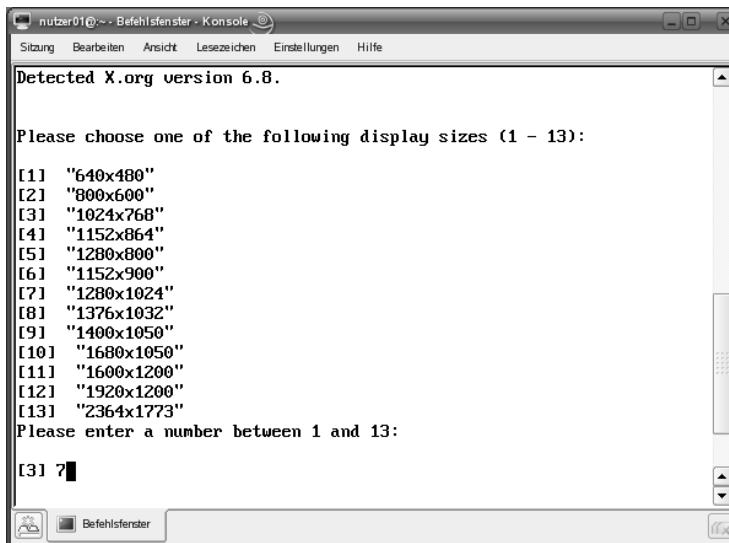


Abbildung 4.27:  
Die beim Setup der  
VMware Tools aus-  
gewählte Auflösung  
ist die Maximale, bis  
zu der ein Gast ska-  
lieren kann

6. Zum Abschluss ist ein Neustart des SUSE-Gastes erforderlich, danach stehen alle Funktionen der VMware Tools zur Verfügung.

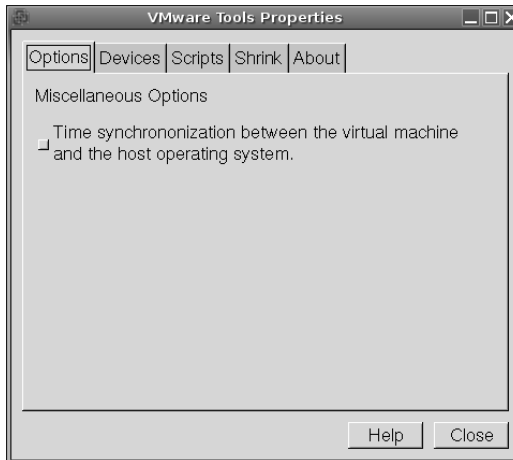
## VMware Toolbox unter Linux starten

Die VMware Toolbox muss nicht unbedingt im Gast laufen, auch ohne die Box stehen alle Funktionen zur Verfügung. Bei Bedarf, um z.B. die Zeitsynchronisation abzuschalten, starten Sie die Box unter Linux mit folgendem Befehl:

```
vmware-toolbox &
```



Abbildung 4.28:  
Die VMware Tool-  
box unter Linux



## 4.5 Microsoft Virtual Machine Additions

Als Einleitung zu den Microsoft-Produkten sind zuerst ein paar Worte zu den so genannten *Virtual Machine Additions* notwendig, sie tauchen bei der Beschreibung einiger Funktionen immer wieder mit auf.

### 4.5.1 Was sind die Microsoft Virtual Machine Additions?

Microsoft liefert mit den *Virtual Machine Additions*, ähnlich wie die VMware Tools, für seine virtuellen Maschinen ein Software-Paket, das im Gast optimierte Treiber bereitstellt und zusätzliche Funktionen ermöglicht, etwa das automatische Herunterfahren der Gastbetriebssysteme. Ein Überblick über diese Funktionen ist für das bessere Verständnis des weiteren Kapitels nützlich:

- ▶ *Optimierte Treiber* – Die Tools installieren Treiber für VGA, Maus oder für die SCSI-Controller in der VM. Diese Treiber beschleunigen zum einen das Gastsystem, zum anderen ermöglichen sie eine automatische Skalierung des Gastfensters und nahtlosen Fokuswechsel zwischen Gast und Host beim Bewegen der Maus. Sobald Sie die Größe des Fensters einer VM unter Virtual PC ändern, passen die Additions automatisch die Bildschirmauflösung des Gastes stufenlos an, so dass der Gast immer genau das Fenster ausfüllt. Diese Funktion unterstützt Virtual Server allerdings nicht.
- ▶ *Drag&Drop, Cut&Paste und Freigegebene Ordner* – Die Tools stellen Funktionen zum komfortablen Datenaustausch zwischen Host und Gästen bereit. Freigegebene Ordner, zum einfachen Zugriff

des Gastes auf Dateien und Verzeichnisse des Hosts, unterstützt nur Virtual PC. Beim Virtual Server kann ein Datenaustausch nur über das Netzwerk erfolgen.

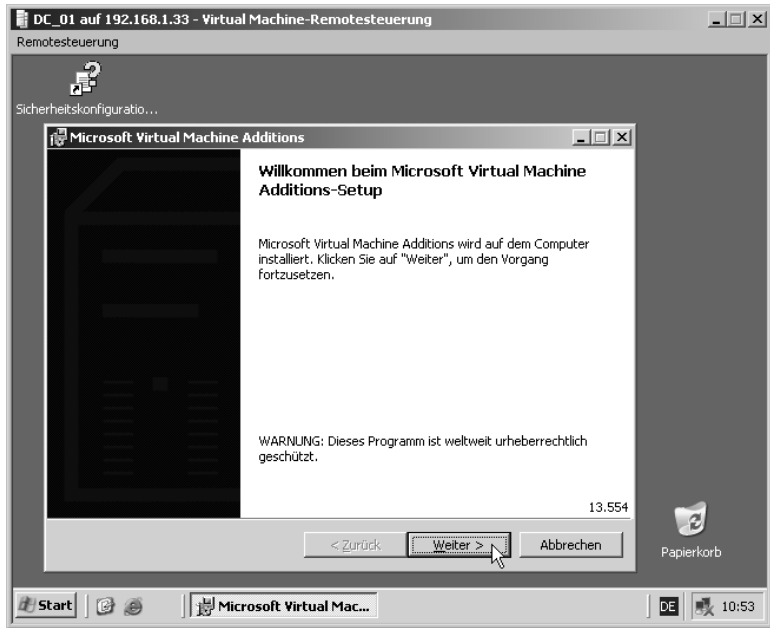
- ▶ *Systemsteuerung beim Ausschalten* – Durch die Tools können die Gastsysteme automatisch heruntergefahren werden, bevor die VM abschaltet.
- ▶ *Zeitsynchronisation mit dem Host* – Der Gast kann über die Tools die Uhrzeit vom Host beziehen.
- ▶ *Heartbeat* – Die Additions senden regelmäßig ein Signal, ob der Gast noch ordnungsgemäß läuft. Dieses Signal kann zur Überwachung ausgewertet werden.
- ▶ *Vorbereiten virtueller Platte auf das Verdichten (Precompact)* – Durch Überschreiben unbenutzter Sektoren im Gast mit Nullen können virtuelle Zuwachsplatten später verkleinert werden, indem die unbenutzten Nullsektoren aus der Datei der virtuellen Platte entfernt werden (siehe Teil 3, Kapitel 3).

#### 4.5.2 Installation der Virtual Machine Additions im Gast

Die Installation der Virtual Machine Additions ist unkompliziert. Sie erfolgt bei Virtual PC über das Menü AKTION im Fenster einer laufenden VM (siehe Teil 2, Kapitel 2, „Mobile virtuelle Entwicklungs- und Demo-Umgebung mit Virtual PC“). Unter Virtual Server können Sie die Additions entweder in der Remotesteuerung eines Gastes oder in der Konfiguration eines Gastes über den Menüpunkt VIRTUAL MACHINE ADDITIONS installieren. Bei der Installation wird dem Gast ein ISO-Image als virtuelle CD zugewiesen, auf dem sich das Setup der Additions befindet. Wenn im Gast CD-Autorun eingeschaltet ist, dann startet die Installation automatisch, ansonsten können Sie einfach in der VM die *setup.exe* von der CD mit einem Doppelklick anstarten (Abbildung 4.29). Nach der Installation ist ein Neustart des Gastes erforderlich.

Virtual Machine Additions für einige ausgewählte Linux-Distributionen (SUSE und Red Hat) sind von Microsoft angekündigt und befinden sich im Beta-Test.

Abbildung 4.29:  
Die Virtual Machine  
Additions sollten in  
jedem Gast instal-  
liert werden



## 4.6 Bedienung von Microsoft Virtual PC

Den Umgang mit Microsoft Virtual PC beschreibe ich an einem ausführlichen Praxisbeispiel in *Teil 2, Kapitel 2*. Durch die sehr übersichtliche Anzahl von Optionen ist Virtual PC unkompliziert zu bedienen. Die wichtigsten Tipps und Stolpersteine werden ebenfalls im Praxis-Workshop von *Teil 2, Kapitel 2*, erläutert.

### 4.6.1 Unterschiede von Virtual PC und Virtual Server

Der Unterschied zwischen Virtual PC und dem großen Bruder Virtual Server ist wesentlich ausgeprägter als zwischen VMware Workstation und VMware Server. Neben den völlig anderen Oberflächen der beiden Microsoft-Virtualisierer unterscheiden sich auch die Funktionen. Deshalb ist es nicht sinnvoll, beide Produkte in einem Kapitel gemeinsam zu beschreiben. Was bei VMware eher gleitend ineinander übergeht, ist bei Microsoft klarer getrennt: Virtual Server für produktive Anwendungen, Virtual PC für flexible Testumgebungen mit ständigen Änderungen und Anpassungen an den VMs.

Hier finden Sie kurz einige wesentliche Unterschiede von Virtual PC und Virtual Server:

- ▶ Virtual PC verfügt nur über ein einziges internes Netzwerk zum Aufbau abgeschotteter Bereiche für Testumgebungen oder isolierte Maschinen, z.B. einer DMZ. Bei Virtual Server können dagegen beliebige Netzwerke konfiguriert werden. Dafür kennt Virtual Server kein NAT (siehe auch *Teil 3, Kapitel 1*, und *Teil 3, Kapitel 2*).
- ▶ Virtual Server wird ausschließlich über eine webbasierte Oberfläche von jedem beliebigen Client bedient. Das funktioniert aber nur mit einem Browser ab Internet Explorer 5.5.
- ▶ In der Weboberfläche von Virtual Server funktioniert die automatische stufenlose Skalierung der Bildschirmauflösung in den Gästen nicht, dadurch sind die Fenster recht unflexibel. Für Serveranwendungen ist das eher Nebensache, für Testumgebungen teilweise unpraktisch.
- ▶ Die Bedienung von Virtual Server ist streckenweise etwas umständlich, besonders wenn ständig neue VMs mit häufig anderen virtuellen Platten oder CD-Images benötigt werden. Das liegt an der fehlenden Schaltfläche DURCHSUCHEN im Web-Interface bei allen Dialogen, wo Pfadangaben notwendig sind. Hier muss der Anwender ständig mit kompletten Pfadangaben hantieren, wenn er z.B. schnell die Platte einer anderen VM einbinden will oder wenn er den Verweis auf die Basis einer Differenzplatte eingeben muss (siehe *„Umgang mit Verzeichnisnamen und Suchpfaden in den Dialogen der Verwaltungswebseite“*).
- ▶ Virtual PC kennt keine virtuellen SCSI-Platten, Virtual Server hat dagegen keine Soundunterstützung in den Gästen.
- ▶ Alle VMs von Virtual PC laufen immer auf dem gleichen Prozessor, egal wie viele im Host eingebaut sind – es findet keine Lastverteilung statt. Virtual Server verteilt die Last der Gäste auf alle physischen CPUs.
- ▶ VMs laufen beim Virtual Server als Dienst. Bei Virtual PC laufen die Gäste als Anwendung und werden beendet, sobald sich der Benutzer vom Host abmeldet.

## 4.7 Bedienung von Microsoft Virtual Server

Einen praxisbezogenen Einstieg zum Microsoft Virtual Server 2005 R2 finden Sie in *Teil 2, Kapitel 7*. Dort wird der Aufbau einer virtuellen Pilotumgebung als 1:1-Kopie des Produktivnetzes beschrieben, um in Ruhe Patches, Software-Updates oder Migrationen an einem Double der realen Umgebung zu testen.

### 4.7.1 Die Bedienoberflächen von Microsoft Virtual Server im Überblick

#### Firewall-Ports 1024 und 5900

Nach der Installation von Virtual Server und der Freischaltung der *Virtual Machine-Remotesteuerung* (siehe Teil 1, Kapitel 3) finden Sie am Host die wichtigsten Verknüpfungen im Startmenü unter PROGRAMME/MICROSOFT VIRTUAL SERVER. Dort befinden sich auch Verknüpfungen zur Hilfe und zu den Handbüchern. Die Firewall-Ports 1024 und 5900 der Windows-Firewall müssen am Host geöffnet sein, um die Verwaltungswebseite und die Fernsteuerung der virtuellen Maschinen von einem Client im LAN aus zu verwenden. Standardmäßig erledigt das Öffnen der Ports bereits das Setup von Virtual Server.

#### Die Virtual Server-Verwaltungswebseite (Webadministration)

Dreh- und Angelpunkt der Verwaltung von Virtual Server und der virtuellen Maschinen ist die *Virtual Server-Verwaltungswebseite*. Sie erreichen diese Webseite am Host selbst und von jedem LAN-Client über die URL [http://mein\\_host:1024](http://mein_host:1024) (Abbildung 4.30). Sie benötigen dazu mindestens den Internet Explorer ab Version 5.5. Alternativen, wie Mozilla Firefox, funktionieren nicht. Im Browser erstellen Sie neue VMs und neue Festplatten, Sie sehen den Status der Gäste und können sie starten, beenden oder fernsteuern. Weiterhin haben Sie die Kontrolle über die virtuellen Netzwerke und konfigurieren Einstellungen für den Host. Über ein ActiveX-Plugin ist im Browser der Bildschirminhalt der Gäste zu sehen, und Sie arbeiten damit remote im Gastsystem.

#### Der Virtual Machine-Remotesteuerungsclient (VMRC)

#### vmrc.exe

Für die Remotesteuerung der Gastsysteme gibt es zusätzlich das kleine schlanke Programm *vmrc.exe* als separaten Fernsteuerungsclient (Abbildung 4.37). Sie finden es auf dem Host unter START/PROGRAMME/MICROSOFT VIRTUAL SERVER bzw. im Verzeichnis `C:\Programme\Microsoft Virtual Server\VMRC Client\vmrc.exe`. Von dort können Sie die *vmrc.exe* auch an eine zentrale Ablage im Netzwerk kopieren, um sie von jedem LAN-Client zu verwenden oder um Mitarbeitern Zugriff auf den Bildschirm bestimmter Gäste zu gewähren. Ich komme weiter unten noch darauf zurück.

#### Windows-Remotedesktop zur Verwaltung des Host-Systems

Zusätzlich zu den speziellen Verwaltungstools von Virtual Server ist in einigen Fällen eine Remotedesktop-Verbindung zum Host-Rechner nützlich, z.B. um das Dateisystem zu verwalten oder um bestimmte Pfade zu virtuellen Maschinen, virtuellen Platten oder ISO-Images zu suchen. Eine komplette Administration über Remotedesktop ist nicht zu empfehlen, weil es dabei vor allem in der Fernsteuerung der Gäste zu Problemen bei der Bildschirmdarstellung kommen kann.

## 4.7.2 Die wichtigsten Funktionen und Tipps zur Bedienung von Microsoft Virtual Server

Wo finden Sie in der Verwaltungswebseite von Microsoft Virtual Server die Funktionen, die für die tägliche Arbeit wichtig sind?

### Grundlegender Aufbau der Verwaltungswebseite von Microsoft Virtual Server 2005 R2

Die *Virtual Server Verwaltungswebseite* bietet alle Funktionen von der Konfiguration des Servers und der VMs bis zur Fernsteuerung der Gastsysteme unter einer Oberfläche (Abbildung 4.30). Auf der linken Seite erreichen Sie alle Funktionen über eine Menüstruktur, rechts daneben erscheinen die entsprechenden Dialoge, etwa die Hardware-Ausstattung einer VM oder die Einstellungen zum Server. Hat ein Menüpunkt einen kleinen schwarzen Pfeil, so verfügt er über Untermenüs, die sich unter dem Mauszeiger automatisch öffnen. Über kleine rote Fragezeichen können Sie die Hilfefunktion zu jedem Bereich der Webseite starten.

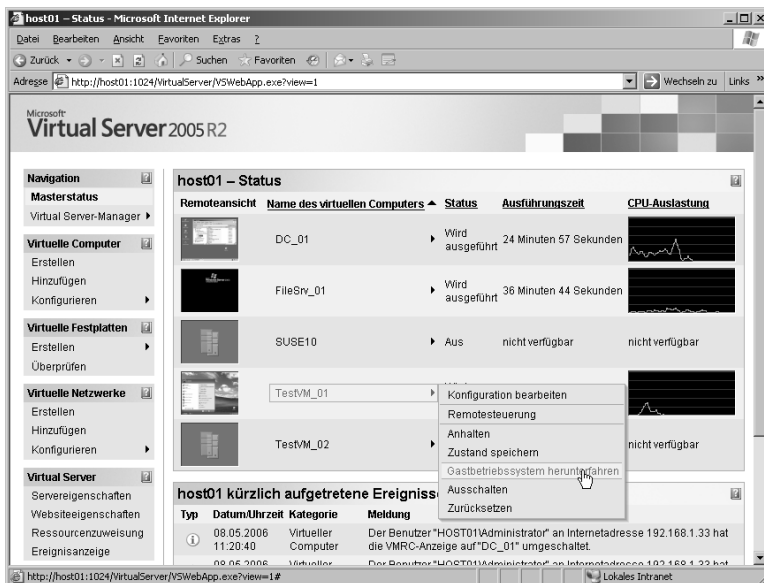


Abbildung 4.30: Die Virtual Server-Verwaltungswebseite ist der Dreh- und Angelpunkt der gesamten Bedienung

Die Startseite der Verwaltungswebseite ist der so genannte *Masterstatus*, wo Sie in einer Liste übersichtlich alle auf dem Host eingerichteten virtuellen Maschinen und deren Status sehen. Der Bildschirminhalt laufender Gäste wird in einer kleinen Miniatur dargestellt, daneben stehen der Name der VM, der Status, die Ausführungszeit und ein Diagramm mit der CPU-Auslastung (wenn die VM läuft). Die Sortierung der Liste ändern Sie mit einem Mausklick auf die Spaltenüberschriften. Jede VM hat rechts neben Ihrem Namen ebenfalls einen kleinen schwarzen Pfeil. Gehen Sie mit der Maus darauf, dann

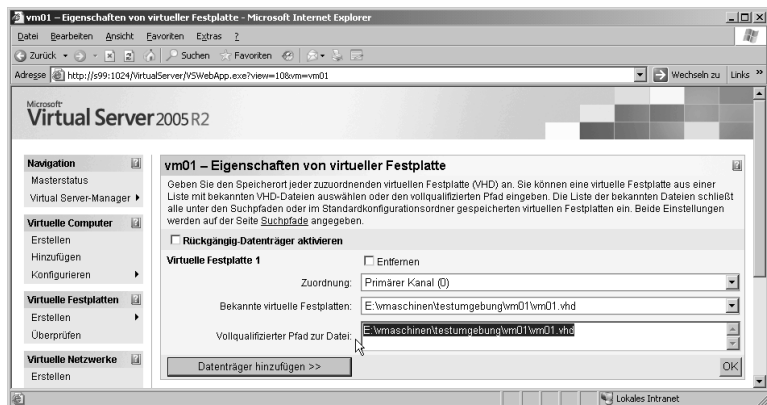
### Masterstatus

erscheint ein Untermenü zur Steuerung des Gastes, z.B. Ausschalten, Konfiguration bearbeiten oder Remotesteuerung (Abbildung 4.30). Im unteren Abschnitt des Masterstatus werden die letzten Meldungen des Ereignisprotokolls von Virtual Server angezeigt.

### Umgang mit Verzeichnisnamen und Suchpfaden in den Dialogen der Verwaltungswebseite

Auf eine Besonderheit von Virtual Server muss ich Sie gleich zu Beginn aufmerksam machen – es ist der etwas umständliche Umgang mit Verzeichnisnamen und den Pfaden zu Dateien, wie virtuellen Platten oder ISO-Images. Wenn Sie beispielsweise einer VM eine vorhandene virtuelle Platte hinzufügen wollen, dann müssen Sie im entsprechenden Dialog auf der Verwaltungswebseite den Ordner und Namen dieser virtuellen Platte vollständig angeben, damit Virtual Server sie findet (Abbildung 4.31).

Abbildung 4.31:  
Pfadangaben zu bestimmten Dateien, wie virtuellen Platten, müssen immer vollständig angegeben werden



Bei der Verwaltung über eine Webseite gibt es beim Aufspüren von Dateien in unbekannten Ordnern allerdings ein kleines Problem. Die Schaltfläche DURCHSUCHEN (Browse) auf einer Webseite kann immer nur die lokale Festplatte des Clients durchsuchen, auf dem der Browser gerade läuft. Wenn Sie also von der Ferne den Virtual Server administrieren, könnten Sie mittels DURCHSUCHEN auf der Verwaltungswebseite nicht das Dateisystem des Servers durchsuchen, wo die gewünschten Dateien liegen. Stattdessen hätten Sie nur Zugriff auf Ihren lokalen Client, was aber keinen Sinn ergibt. Anstelle eine andere Lösung, etwa mit Active Server Pages zu programmieren, haben sich die Entwickler bei Microsoft für den einfachen Weg entschieden – sie haben die Schaltfläche DURCHSUCHEN bei den entsprechenden Dialogen auf der Verwaltungswebseite einfach weggelassen. Das hat zur Folge, dass Sie jeden Pfad zu einer virtuellen Platte, einem ISO-Image oder einer Konfigurationsdatei eigentlich immer vollständig eintippen müssen, wenn er in einem Dialog benötigt wird (Abbildung 4.31).

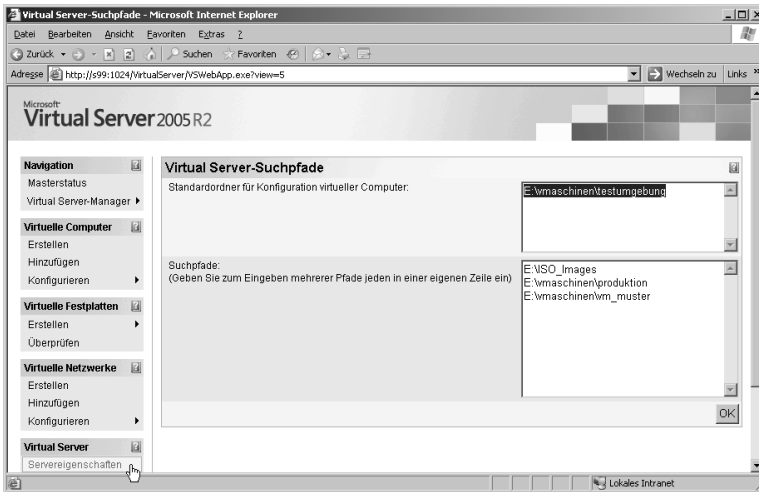


Abbildung 4.32:  
Über die Servereigenschaften können Suchpfade zu häufig verwendeten Ablageorten von VMs oder ISO-Images hinterlegt werden

Um die Suche nach den richtigen Ablageorten und die Schreiberei der Verzeichnispfade etwas zu vereinfachen, können Sie über VIRTUAL SERVER/SERVEREIGENSCHAFTEN/SUCHPFADE wenigstens die Pfade zu Ihren wichtigsten Ordnern auf dem Server hinterlegen (Abbildung 4.32). Dadurch bekommen Sie in den entsprechenden Dialogen alle Dateien in diesen Suchpfaden aufgelistet und können eine davon auswählen. Sie sollten z.B. den Ordner mit Ihren ISO-Images in die Suchpfade aufnehmen, um jederzeit ein ISO-Image als virtuelle CD auswählen zu können (Abbildung 4.33).

**Suchpfade für Dateien festlegen**

An einigen Stellen funktioniert die Auflistung von Dateien auch ohne Suchpfade. Alle Dateien einer VM, die sich im gleichen Verzeichnis wie die virtuelle Maschine befinden, z.B. eine virtuelle Platte, werden in den Konfigurationsdialogen zu diesem Gast unter BEKANNTE VIRTUELLE FESTPLATTEN immer aufgelistet (Abbildung 4.31). Sie müssen also nicht für jeden Gast einen Eintrag in den Suchpfaden hinterlegen. Wenn Sie allerdings einer VM die Platte eines anderen Gastes zuweisen wollen (für Testzwecke oder zum Reparieren des enthaltenen Betriebssystems usw.), dann müssen Sie den Pfad zu dieser Platte vollständig in das Feld VOLLQUALIFIZIERTER PFAD ZUR DATEI eingeben.

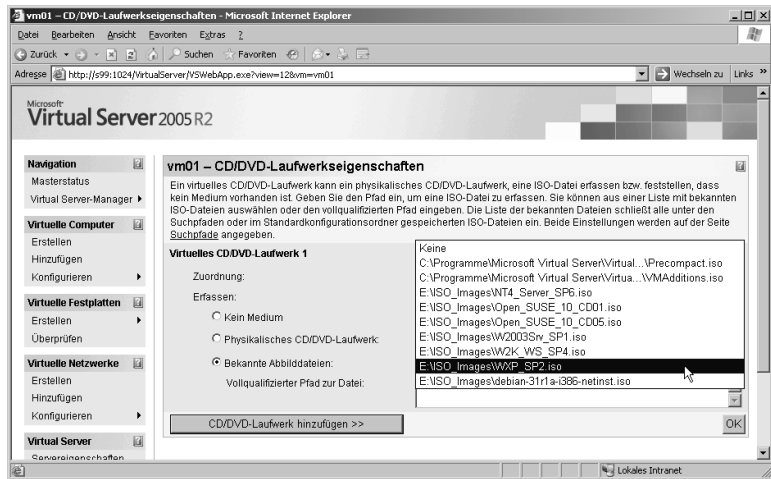
Zusätzlich zu den Suchpfaden gibt es den STANDARDORDNER FÜR KONFIGURATION VIRTUELLER COMPUTER (Abbildung 4.32). In diesem Pfad legt Virtual Server automatisch alle neu erstellten virtuellen Maschinen und virtuellen Platten ab. Standardmäßig ist dieser Ordner auf C:\Dokumente und Einstellungen\All Users\Dokumente\Shared Virtual Machines\ voreingestellt, Sie haben das in Teil 1, Kapitel 3, bereits auf *vmaschinen\testumgebung* geändert. Beim Anlegen einer neuen VM genügt es, den Namen der neuen virtuellen Maschine einzutippen (Abbildung 4.34). Virtual Server legt dann automatisch im Standardordner ein Verzeichnis gleichen Namens an und erstellt dort den neuen Gast. Sollten Sie allerdings eine VM in einem anderen Ver-

**Standardordner für neue VMs**



zeichenspfad erstellen wollen (z.B. *mustermaschinen* oder *produktion*), dann müssen Sie wieder den gesamten Pfad ausschreiben.

Abbildung 4.33:  
In den Dateidialogen, z.B. bei der Auswahl eines ISO-Images, werden die Inhalte der Suchpfade aufgelistet



**Pfade mit Cut & Paste aus dem Explorer**

In relativ statischen Produktionsumgebungen, in denen nicht täglich an den Gästen Konfigurationsänderungen stattfinden, stellt die Arbeit mit den Verzeichnispfaden kein Problem dar. Wenn Sie allerdings auf dem Virtual Server viele Testumgebungen aufbauen und ständig VMs umkonfigurieren, etwa neue Platten einbinden oder austauschen bzw. ISO-Images von verschiedenen Quellen verwenden, dann wird der Umgang mit den Ordnern etwas lästig. Für die Verwendung vollständiger Verzeichnispfade, zu denen kein Suchpfad existiert, hilft ein kleiner Trick. Wenn Sie zusätzlich zur Verwaltungswebseite vom Client aus eine Remotedesktop-Verbindung zu Ihrem Host aufbauen, dann können Sie dort im Datei-Explorer komfortabel in den Verzeichnissen navigieren und aus der Adresszeile des Datei-Explorers die richtigen Pfadangaben mittels Cut & Paste in die Verwaltungswebseite übertragen. Das erspart Tippfehler und lange Schreiberei.

### Eine neue VM mit Virtual Server erstellen

Nach den grundlegenden Ausführungen zum Umgang mit Verzeichnispfaden können Sie Ihre erste VM erstellen. Das geschieht über den Menüpunkt **VIRTUELLE COMPUTER/ERSTELLEN** (Abbildung 4.34). Für Ihre erste Test-VM genügt es, wenn Sie einen Namen, etwa *testvm01*, eingeben und die Einstellung für den Hauptspeicher des Gastes Ihren Gegebenheiten anpassen. Alle anderen Einstellungen belassen Sie vorerst so und klicken OK. Im Anschluss öffnet sich der Dialog zur Konfiguration der neuen VM im Browser, ich komme später detaillierter darauf zurück, Sie müssen vorerst nichts ändern. Im Verzeichnis *\testumgebung\testvm01* auf dem Host finden Sie Ihre erste virtuelle Maschine. Sie besteht aus einer Konfigurationsdatei mit der Endung *\*.vmc* und einer virtuellen Platte mit der Endung *\*.vhd*.

**Virtuellen Computer erstellen**

**Name des virtuellen Computers**  
Geben Sie den Dateinamen für den virtuellen Computer ein, um den virtuellen Computer im Standardkonfigurationsordner zu speichern, der auf der Seite *Virtual Server-Suchpfade* angegeben ist. Geben Sie einen vollqualifizierten Pfad ein, um einen virtuellen Computer an einem anderen Speicherort zu erstellen.

Name des virtuellen Computers:

**Arbeitsspeicher**  
Die Größe des Arbeitsspeichers darf zwischen 4 MB und 818 MB liegen (736 MB werden als Maximalwert empfohlen).

Arbeitsspeicher des virtuellen Computers (in MB):

**Virtuelle Festplatte**  
Bevor Sie ein Betriebssystem auf diesem virtuellen Computer installieren können, müssen Sie ihm eine neue oder vorhandene virtuelle Festplatte zuordnen. Eine virtuelle Festplatte ist eine VHD-Datei, die auf der physikalischen Festplatte gespeichert ist und das Gastbetriebssystem, Anwendungen und Datendateien enthält.

☒ Neue virtuelle Festplatte erstellen  
Mit dieser Option wird eine unformatierte dynamisch erweiterbare virtuelle Festplatte im Verzeichnis der Konfigurationsdatei des virtuellen Computers erstellt. Die maximal zulässige Größe ist 127 GB für IDE-Festplatten und 2040 GB für SCSI-Festplatten.

Größe:  Einheiten:  Bus:

☐ Eine vorhandene virtuelle Festplatte verwenden

Pfad:

Dateiname (.vhd):

Bus:

☐ Virtuelle Festplatte später zuordnen (Keine)

Abbildung 4.34:  
Zum Erstellen der  
ersten virtuellen  
Maschine genügen  
die Standardvor-  
gaben

Virtual Server erstellt für Ihre VM standardmäßig eine virtuelle Zuwachsplatte mit der maximalen Größe von 16 GB, im Beispiel *testvm01.vhd*. Das bedeutet, die Platte belegt immer nur den Platz, der vom Gast tatsächlich verwendet wird, und wächst bei Bedarf bis zur Größe von 16 GB mit, das spart Platz auf dem Host. Beim Erreichen der maximalen Größe meldet der Gast dann eine volle Platte. Dieser Plattentyp ist für eine Testumgebung genau richtig. Wollen Sie bei der Erstellung einer VM allerdings einen anderen Plattentyp festlegen (z.B. differenziell oder mit fester Größe – Plattentypen siehe *Teil 3, Kapitel 3*), dann müssen Sie an dieser Stelle den Punkt bei **VIRTUELLE FESTPLATTE SPÄTER ZUORDNEN (KEINE)** setzen, so dass die VM vorläufig ohne Platte erstellt wird. Erst nachträglich erstellen Sie eine passende Platte im Menü **VIRTUELLE FESTPLATTEN**, wobei Sie ausführlichere Parameter festlegen können. Die Platte binden Sie anschließend über die Konfiguration des Gastes ein. Existiert die virtuelle Platte bereits vor der Erstellung der VM, dann binden Sie diese gleich über den Punkt **EINE VORHANDENE VIRTUELLE FESTPLATTE VERWENDEN** ein (Abbildung 4.34).

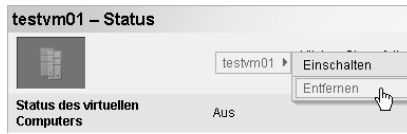
Die virtuelle  
Platte der VM

## VMs von Virtual Server wieder entfernen

Wenn Sie eine neu erstellte VM wieder entfernen wollen, dann sind dazu zwei Schritte notwendig. Als Erstes entfernen Sie den Eintrag in der Verwaltungswebseite, indem Sie im Masterstatus oder in der Konfiguration einer VM auf den kleinen schwarzen Pfeil am Namen des Gastes gehen und im automatisch erscheinenden Menü **ENTFERNEN** wählen (Abbildung 4.35). Die VM wird dadurch aus der Liste entfernt, bleibt aber auf der Festplatte vollständig erhalten. Wollen Sie den Gast endgültig verwerfen, mitsamt allen virtuellen Platten und

dem Gastsystem, dann müssen Sie den Ordner der VM auf dem Host-Datenträger manuell löschen, in unserem Beispiel `\testumgebung\testvm01`.

Abbildung 4.35:  
Das Entfernen einer  
VM löscht nicht die  
zugehörigen Dateien  
auf dem Host-  
Datenträger



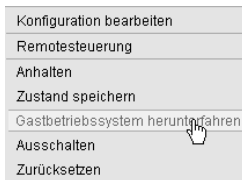
### Eine vorhandene VM in die Verwaltungswebseite aufnehmen

Wollen Sie eine VM wieder in die Verwaltung aufnehmen bzw. eine kopierte VM von einem anderen Host oder von Virtual PC neu hinzufügen, dann gelingt das über den Menüpunkt VIRTUELLE COMPUTER/HINZUFÜGEN. Dabei ist wieder der komplette Pfad zur Konfigurationsdatei `*.vnc` notwendig, wenn die VM nicht in einem bekannten Suchpfad liegt.

### VMs starten, beenden, anhalten oder einfrieren (Status speichern)

Wurde eine VM neu hinzugefügt oder neu erstellt, erscheint sie automatisch in der Liste im Masterstatus von Virtual Server (Abbildung 4.30). Zu jedem Eintrag existiert ein Untermenü, das Sie über den kleinen schwarzen Pfeil neben dem Namen der VM erreichen. Die gesamte Steuerung des Gastes erfolgt über dieses Menü (Abbildung 4.36).

Abbildung 4.36:  
Die Steuerung der  
Gäste erfolgt über  
ein kleines Menü



Die einzelnen Menüpunkte haben folgende Bedeutung, einige erscheinen nur bei laufender VM, andere nur wenn die Virtual Machine Additions im Gastsystem installiert sind:

- ▶ *Konfiguration bearbeiten* – Über diesen Menüpunkt startet der Konfigurationsdialog zu einem Gast, wo Sie z.B. die virtuelle Hardware bearbeiten können.
- ▶ *Remotesteuerung* – Sie gelangen in die Remotesteuerung eines Gastes – siehe „Fernbedienen der Gäste über die Virtual Server-Remotesteuerung im Browser oder über den VMRC Client“.
- ▶ *Anhalten* – Eine laufende VM wird angehalten, wobei sie allerdings weder abgeschaltet noch gesichert wird. Ihr werden nur sämtliche CPU-Ressourcen entzogen, wobei Sie sofort einfriert. RAM-Inhalt, aktueller Status usw. bleiben erhalten, und die VM läuft nach dem Fortsetzen sofort weiter. Das ist z.B. praktisch, wenn CPU-Ressourcen einer VM kurzzeitig für andere Gäste benötigt werden.

- ▶ *Zustand speichern* – Mit dieser Option werden der Status und der RAM-Inhalt der VM in einer Datei auf dem Host abgespeichert und der Gast dann abgeschaltet. Dieser Zustand kann später wieder hergestellt werden, und das Gastsystem steht in Sekunden an genau der gleichen Stelle wie vor dem Abschalten. Das spart viel Zeit beim Hochfahren von VMs in Testumgebungen. Diese Funktion kann auch zum schnellen Übertragen einer laufenden VM auf einen anderen Host-Rechner mit minimaler Ausfallzeit genutzt werden, indem die abgeschaltete VM samt Statusdatei kopiert und auf dem anderen Host wieder gestartet wird. Noch schneller geht das, wenn die Dateien gleich auf externem Speicher, wie einem SAN oder einer Netzwerkfreigabe, liegen.
- ▶ *Gastbetriebssystem herunterfahren* – Dieser Punkt wird nur angezeigt, wenn die Virtual Machine Additions im Gast installiert sind. Über diesen Menüpunkt können Sie das Betriebssystem im Gast herunterfahren, die VM schaltet danach ab.
- ▶ *Ausschalten* – Die VM wird sofort abgeschaltet. Das entspricht einem PowerOff eines physischen Rechners.
- ▶ *Zurücksetzen* – Die VM wird neu gestartet, das entspricht der Reset-Taste eines physischen Rechners.

Wenn Sie in Ihrer VM Rückgängig-Datenträger aktiviert haben, erscheinen zusätzliche Optionen im Menü. Rückgängig-Datenträger puffern Schreibzugriffe auf die virtuellen Festplatten. Dadurch werden die Daten in den Platten nicht mehr verändert. Die Änderungen in den Rückgängig-Datenträgern lassen sich vor dem Abschalten verwerfen bzw. festschreiben. Diese Funktion wird im Praxis-Workshop von Teil 2, Kapitel 7, „Eine virtuelle Pilotumgebung als Testfeld für produktive Einsätze“ in Abschnitt 7.5.3, *Verwendung von Rückgängig-Datenträgern zur Sicherung des Gastsystems* beschrieben.



### Fernbedienen der Gäste über die Virtual Server-Remotesteuerung im Browser oder über den VMRC Client

Wenn die VM gestartet ist, dann wollen Sie natürlich den Bildschirminhalt sehen und im Gastsystem mit Tastatur und Maus arbeiten. Virtual Server stellt dafür eine Remotesteuerung bereit. Dazu muss die *Virtual Machine-Remotesteuerung* im Menü SERVEREIGENSCHAFTEN freigeschaltet sein (siehe Teil 1, Kapitel 3). Die Fernsteuerung erreichen Sie im Menü einer jeden VM über den Punkt REMOTESTEUERUNG (Abbildung 4.36). Genauso können Sie einfach die Miniatur eines Gastbildschirmes im Masterstatus anklicken. Die Fernsteuerung der Gäste erfolgt dann über eine ActiveX-Plug-In direkt im Browser.

#### ActiveX-Plug-In

Abbildung 4.37:  
Die Remotesteuerung  
zeigt den Inhalt des  
Gastbildschirmes im  
Browser oder im  
Fenster der VMRC



#### Remotesteue- rungsclient vmrc.exe

Eine etwas komfortablere Methode als die Fernsteuerung im Browser ist der *Virtual Machine-Remotesteuerungsclient* (VMRC). Wie bereits erwähnt finden Sie das Programm unter `C:\Programme\Microsoft Virtual Server\VMRC Client\vmrc.exe`. Die Bedienung funktioniert ähnlich wie das ActiveX-Plug-In, es stehen aber ein paar zusätzliche Funktionen, z.B. der Vollbildmodus, bereit (Abbildung 4.37).

Gängige Praxis ist es, eine Instanz der Verwaltungswebseite im Browser zu öffnen und parallel dazu eine Instanz des VMRC laufen zu haben. Im Browser wird dann der gesamte Host mit den VMs verwaltet, oder Gäste werden gestartet und beendet. Die Arbeit in den Gastsystemen erfolgt dagegen über den Remotesteuerungsclient `vmrc.exe`. Nachdem das Programm gestartet ist, fragt es nach einem Link zu einem Host oder zu einem bestimmten Gast (Abbildung 4.38). Mit folgender Syntax sehen Sie alle VMs eines Hosts als Liste von Miniaturansichten und können eine auswählen:

```
vmrc://mein_host:5900/
```

Um sich direkt mit einem bestimmten Gast zu verbinden, hängen Sie den Namen des Gastes an die URL an:

```
vmrc://mein_host:5900/vm01
```



Sie können für Mitarbeiter Verknüpfungen zu wichtigen VMs anlegen, die dann mit einem Doppelklick sofort den Bildschirm eines bestimmten Gastes anzeigen. Die Befehlszeile könnte so aussehen:

```
"E:\Pfad zur exe\vmrc.exe" mein_host:5900/vm01
```

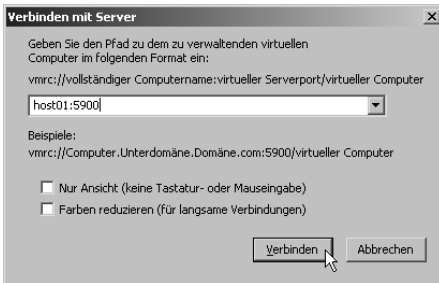


Abbildung 4.38:  
Mit dem Remote-  
steuerungsclient  
(VMRC) verbinden  
Sie sich direkt auf  
einen Host, um in  
den Gastsystemen  
zu arbeiten

Ob über das ActiveX-Plug-In oder über die *vmrc.exe* – grundsätzlich zeigt die Remotesteuerung den Inhalt eines Gastbildschirmes an. Um mit dem Gast arbeiten zu können, klicken Sie einfach mit der Maus ins Fenster. Dadurch erhält der Gast den Fokus, und alle Tastenschläge und Mausbewegungen landen im Gastsystem. Um wieder zurück auf den eigenen Desktop zu gelangen, entziehen Sie dem Gast wieder den Fokus mit einem Hotkey, der so genannten *Hosttaste*. Diese Hosttaste ist standardmäßig **AltGr** und kann im Menü der Fernsteuerung über **HOTTASTE FESTLEGEN** geändert werden (Abbildung 4.39). Es ist oftmals besser, eine andere Taste, z.B. die rechte Taste **Strg**, zu benutzen. Wollen Sie beispielsweise in einem Gast den Backslash (\) schreiben, dann verlassen Sie mit **AltGr** ständig den Gast und erhalten nicht das gewünschte Zeichen.

### Fokuswechsel zwischen Gast und Host

Eine weitere Besonderheit ist die Tastenkombination **Strg** + **Alt** + **Entf**, die sich nicht abfangen lässt und dadurch immer auf den lokalen PC wirkt. Um diese Tastenkombination an einen Gast zu senden, dient entweder die Kombination aus Hosttaste + **Entf**, oder Sie verwenden im Menü **REMOTESTEUERUNG** den Punkt **SONDERTASTEN** (Abbildung 4.37). Sie benötigen das im Gast z.B. für den Anmeldebildschirm von Windows.

**Strg** + **Alt** +  
**Entf**

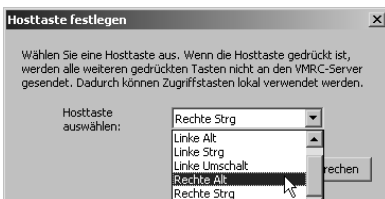


Abbildung 4.39:  
Manchmal ist es  
besser, einen anderen  
Hotkey als **AltGr**  
für Virtual Server zu  
definieren

Im Menü **REMOTESTEUERUNG** finden Sie zusätzliche Funktionen, wobei einige nur bei der *vmrc.exe*, nicht aber im ActiveX-Plug-In existieren (Abbildung 4.37). Einer der Menüpunkte ist **ZUR ADMINISTRATORANZEIGE WECHSELN**. Dahinter verbirgt sich eine Gesamtübersicht aller VMs des Hosts als Miniaturen in einer einfachen Liste. Mit einem Klick auf die angezeigten Miniaturen verbinden Sie sich mit dem entsprechenden Gast. Ist der Gast ausgeschaltet, dann wird er dabei automatisch gestartet. Sehr praktisch ist der Menüpunkt **ZUM NÄCHSTEN VIRTUELLEN COMPUTER WECHSELN**, der am besten über eine Tastenkombination aus Hosttaste und **→** oder **←** aufgerufen

### Zusätzliche Funk- tionen über das Menü Remote- steuerung

wird. Dieser Punkt existiert nur bei der *vmrc.exe*. Damit wechseln Sie sehr schnell zwischen den Bildschirmen aller laufenden VMs, ähnlich wie bei einem KVM-Switch (Tastatur- und Monitorumschalter).

##### **Vollbildmodus und fehlende Funktionen**

Das Wechseln zwischen den Gastbildschirmen funktioniert ebenfalls im Vollbildmodus, zu dem Sie mit der Hosttaste und  gelangen. Mit Hosttaste und  verlassen Sie den Vollbildmodus auch wieder. Beim Einschalten des Vollbildmodus wird der Gast allerdings nicht automatisch an die Bildschirmauflösung des physischen Rechners angeglichen. In der Remotesteuerung von Virtual Server fehlen im Gegensatz zu Virtual PC oder VMware einige Funktionen. So ist es z.B. nicht möglich, Inhalte der Zwischenablage in die Gäste zu übergeben, um z.B. einen Text oder eine Pfadangabe zu kopieren (Cut & Paste). Weiterhin kann auch die Fenstergröße nicht stufenlos durch Ziehen mit der Maus verändert werden. Es ist nur möglich, im Gast die Bildschirmauflösung zu ändern, woraufhin sich das Fenster der Fernsteuerung anpasst.



Wenn Sie nicht wollen, dass die Remotesteuerung nach einer gewissen Zeit immer die Verbindung zum Host verliert, sobald Sie länger nicht in einer Session gearbeitet haben, dann setzen Sie das Timeout unter SERVEREIGENSCHAFTEN/VIRTUAL MACHINE-REMOTESTEuerung (VMRC-SERVER) hoch oder schalten es ab.

##### **Fernbedienen der Gäste über Remotedesktop (RDP) als Alternative zur VMRC**

Eine Alternative zur Bedienung der Gäste über die Remotesteuerung von Virtual Server ist es, in allen Gästen den Remotedesktop freizuschalten. Dann bauen Sie eine Remotedesktop-Verbindung über das Netzwerk direkt mit jedem Gastsystem auf. Das erscheint auf den ersten Blick umständlich, bietet aber einige Vorteile zur Fernbedienung von Virtual Server:

- ▶ Die Performance einer RDP-Verbindung (RDP – Remote Desktop Protocol) ist über das Netzwerk teilweise besser. Bildschirmausgaben und das Handling der Maus funktionieren flüssiger.
- ▶ Cut & Paste vom Client mit dem Gast sind in vollem Umfang über RDP möglich, etwa um Texte hin und her zu kopieren.
- ▶ Der Gast kann über das RDP auf Laufwerke des Clients zugreifen. Erfolgt die Steuerung vom Host selbst, dann hat der Gast damit einen Ersatz für die *Freigegebenen Order* von Virtual PC, die einen Datenaustausch ermöglichen, ohne eine Netzwerkverbindung einzurichten. Das ist vor allem in Testumgebungen praktisch. Genauso ist über das RDP ein Zugriff aus den Gästen auf lokale Drucker des Clients möglich.

- Über den Umweg des RDP ist es sogar möglich, die Soundausgabe in einem Gast zu nutzen, sobald der Fernsteuerungsclient über eine Soundkarte verfügt. Standardmäßig verfügen Gäste unter Virtual Server sonst nicht über eine Soundkarte.

#### Sound im Gast verwenden



Wenn Sie Sound eines Windows 2003 Servers über RDP hören wollen, müssen Sie erst im Gastsystem den Sound für das RDP freischalten, zu finden über VERWALTUNG/TERMINALDIENST-KONFIGURATION/VERBINDUNGEN in der RDP-VERBINDUNG. Entfernen Sie unter dem Reiter CLIENTEINSTELLUNGEN den Haken bei *Deaktivierung der Audiozuordnung*.

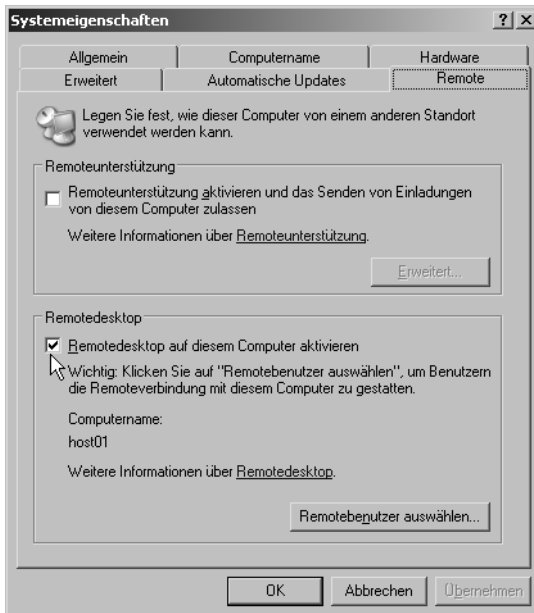


Abbildung 4.40:  
Der Remotedesktop  
in den Gästen bietet  
in einigen Fällen  
bessere Funktionali-  
tät als die Remote-  
steuerung von  
Virtual Server

Sie schalten den Remotedesktop in Gästen unter Windows 2003 oder Windows XP über SYSTEMSTEUERUNG/SYSTEM/REMOTE frei (Abbildung 4.40). In Windows 2000-Gästen ist eine Installation der Terminaldienste im *Remoteverwaltungsmodus* erforderlich, was über SYSTEMSTEUERUNG/SOFTWARE erfolgt. Andere Gäste, etwa Linux oder ältere Windows-Versionen, können nur über Tools, wie z.B. VNC, direkt ferngesteuert werden. Vom Host oder von einem PC im Netzwerk verbinden Sie sich mit dem Remotedesktopclient direkt zum Gast. Sie finden den Client unter Windows XP bzw. Windows 2003 Server im Startmenü bei ZUBEHÖR/KOMMUNIKATION/REMOTEDESKTOPVERBINDUNG. Im Client können Sie die Bildschirmauflösung einstellen oder auch die Verwendung der lokalen Soundausgabe oder lokaler Ordner erlauben (Abbildung 4.41).

#### Remotedesktop freischalten





Standardmäßig verbindet sich ein Remotedesktopclient auf einen Windows Server 2003 immer im Hintergrund auf eine zusätzlich Session des Zielrechners. Sie arbeiten damit auf einem eigenen Desktop und sehen nicht den Bildschirminhalt, den Sie unter Virtual Server sehen würden. Um sich direkt auf die Konsole des fernzusteuernenden Gastes zu verbinden, können Sie die Remotedesktop-Verbindung mit folgender Befehlszeile starten:

```
%SystemRoot%\system32\mstsc.exe /console
```

Abbildung 4.41:  
Beim Verbinden zu  
einem Gast über  
Remotedesktop  
können lokale Lauf-  
werke oder Sound-  
karten durchgereicht  
werden



### Einen Screenshot machen oder ein Video aufzeichnen

Virtual Server bietet keine integrierte Funktion, um vom Bildschirminhalt des Gastes eine Aufnahme zu machen. Das können Sie trotzdem recht bequem über den Host selbst tun, indem Sie das Fenster der Fernsteuerung aufnehmen. Wollen Sie innerhalb des Gastes Screenshots von bestimmten Fenstern schießen, dann empfiehlt sich die Installation eines Tools wie IrfanView oder XnView im Gast selbst.

### Hauptspeicher- und CPU-Verwaltung für den Host und für die Gäste unter Microsoft Virtual Server

Die Hauptspeicherverwaltung von Microsoft Virtual Server ist relativ einfach zu verstehen. Es gilt nur eine Regel: Die Summe des Speichers aller laufenden VMs zuzüglich des Speichers, den der Host selbst für sich benötigt, muss physisch zur Verfügung stehen. Auch Virtual Server benötigt zur Verwaltung der VMs etwas zusätzlichen Hauptspeicher, so dass jeder Gast ein paar Prozent mehr RAM benötigt, als ihm zugewiesen wurde. Es ist nicht möglich, einige VMs mehr zu starten, als es der physische Speicher zulassen würde, wie das bei VMware in bestimmten Grenzen realisierbar ist.

Dagegen bietet Virtual Server als Besonderheit über das Menü VIRTUAL SERVER/RESSOURCENZUWEISUNG die Zuteilung von CPU-Ressourcen an die Gäste (Abbildung 4.42). Damit begrenzen Sie für bestimmte Gäste die maximale CPU-Leistung und konfigurieren eine relative Wichtigkeit der einzelnen Gäste. Beispielsweise haben alle Gäste mit der Standardwichtung 100 eine höhere Priorität als z.B. Testmaschinen mit der Wichtung 50. Besonders wichtige Gäste versehen Sie mit einem Wert von 200, damit diese immer genügend CPU-Leistung zur Verfügung gestellt bekommen.

## CPU-Ressourcen verteilen

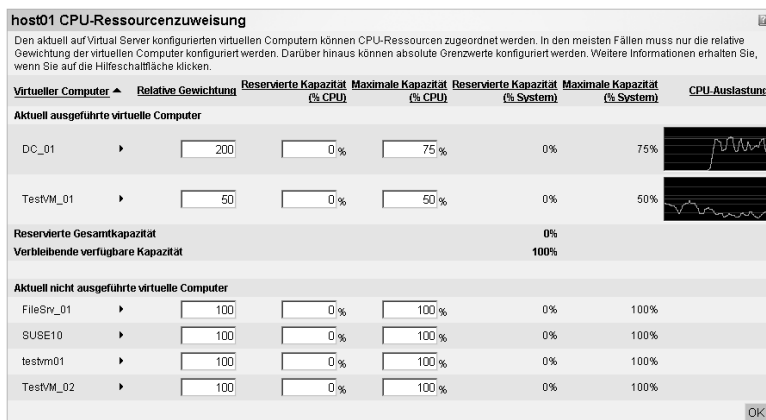


Abbildung 4.42:  
Unter Virtual Server lässt sich die CPU-Leistung im laufenden Betrieb begrenzen und nach prozentualer Wichtigkeit verteilen

## Wichtige Einstellungen und Anzeigen in den Gästen selbst

In die Einstellungen zu jedem Gast gelangen Sie entweder über den Punkt KONFIGURIEREN im Menü einer VM (Abbildung 4.36). Zusätzlich bekommen Sie im Menü VIRTUELLE COMPUTER/KONFIGURIEREN eine Liste aller VMs des Hosts angezeigt, die Sie auswählen können. Neben dem Zugriff auf die gesamte Hardware-Ausstattung der VM sehen Sie im oberen Teil der Konfiguration gleich sehr übersichtlich den Status des Gastes, inkl. Laufzeit und I/O-Werten (Abbildung 4.43).

Im unteren Teil der Konfiguration haben Sie Zugriff auf verschiedene Einstellungen und auf die virtuelle Hardware des Gastes. Einige wichtige Funktionen finden Sie hier als Überblick:

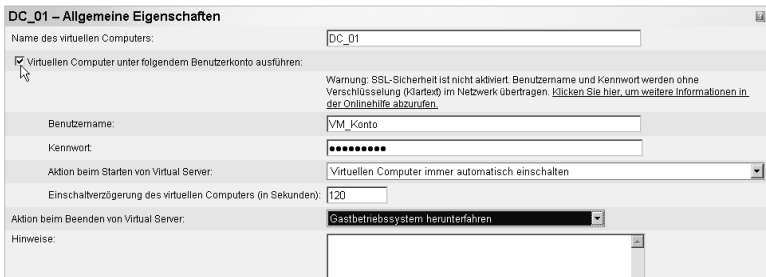
- ▶ *Allgemeine Einstellungen* – Der entscheidende Punkt bei den Serverversionen der vorgestellten Virtualisierungsprodukte ist Ihre Fähigkeit, Gäste als Dienst laufen zu lassen. An dieser Stelle legen Sie fest, unter welchem Benutzer das erfolgt und ob die Gäste bei Host-Start bzw. Shutdown automatisch gestartet und beendet werden (Abbildung 4.44).
- ▶ *Virtual Machine Additions* – Mit diesem Menüpunkt wird die Installation der Additions in den Gästen angestoßen.

Abbildung 4.43:  
Die Konfiguration  
einer VM zeigt auch  
den Status an und  
ermöglicht den  
Zugriff auf die  
Remotesteuerung



- **Skripts** – Sie können Skripte hinterlegen, die bei bestimmten Ereignissen ausgeführt werden. Dazu muss unter ALLGEMEINE EINSTELLUNGEN ein Benutzer hinterlegt sein, unter dem die VM als Dienst läuft. Weiterhin muss unter SERVEREIGENSCHAFTEN/VIRTUAL SERVER-SKRIPTS die Skriptverwendung freigeschaltet sein.

Abbildung 4.44:  
Alle produktiven  
Gäste sollten unter  
Virtual Server als  
Dienst laufen. Sie  
können dann auto-  
matisch starten und  
herunterfahren



- **Hardware** – Über die Menüpunkte wie Arbeitsspeicher, Festplatten usw. können Sie Ihrem Gast Hardware hinzufügen, entfernen oder konfigurieren. Beispielsweise können Sie ISO-Images als virtuelle CDs zuweisen, weitere virtuelle Platten hinzufügen oder einen virtuellen SCSI-Controller einbauen, an dem Sie später virtuelle SCSI-Platten betreiben. Ich komme im Workshop in Teil 2, Kapitel 7, bei der praktischen Anwendung der Funktionen darauf zurück.

## **Weitere Funktionen wie Differenzplatten, Klone oder das Netzwerk von Microsoft Virtual Server**

Mit den hier vorgestellten Funktionen können Sie Microsoft Virtual Server 2005 R2 ausreichend bedienen, um Ihre erste virtuelle Umgebung aufzubauen.

In *Teil 2* des Buches finden Sie praktische Anwendungsbeispiele, beispielsweise für eine virtuelle Pilotumgebung in *Kapitel 7* und für eine ausführliche Cluster-Konfiguration mit virtuellen Maschinen in *Kapitel 8*.

Die Netzwerkfunktionalität von Virtual Server beschreibe ich ausführlich in *Teil 3, Kapitel 1 und Kapitel 2*. Zu den virtuellen Platten und Controllern existiert ebenfalls ein eigener Workshop in *Kapitel 3*.



# Teil 2

## Praxis-Workshops mit nachvollziehbaren Projekten

Sie haben Teil 1 dieses Buches abgeschlossen und wollen nun endlich virtuelle Maschinen nutzbringend einsetzen? Oder Sie gehören zu den Menschen, die sich gar nicht erst lange mit der Lektüre von Bedienungsanleitungen abgeben? Sie erarbeiten sich Lösungen am liebsten selbst – systematisch, Schritt für Schritt an einem konkreten Praxisbeispiel?

**Sofort praktisch loslegen**

*Herzlich willkommen in Teil 2!*

### Was lernen Sie im zweiten Teil?

Hier finden Sie zu bestimmten Aufgabenstellungen fertige Anleitungen, die schnell zum Erfolg führen. Jedes Projekt können Sie sofort am Rechner nachvollziehen. Kleinere Wiederholungen zwischen den einzelnen Kapiteln sind gewollt, dadurch wird jeder Workshop zur völlig unabhängigen Anleitung für eine konkrete Anwendung und ein bestimmtes Virtualisierungsprodukt. Jeder Workshop vermittelt den Umgang mit dem verwendeten Virtualisierer und liefert zusätzlich zu den Grundlagen auch Konzepte und Tipps.

**Nachvollziehbare Beispiele**

Sehr komplexe Sachverhalte, welche die Anleitungen unnötig aufblähen würden und die zum Nachvollziehen nicht direkt notwendig sind, sind in die Technikkapitel von *Teil 3* ausgelagert. Verweise auf die entsprechenden Stellen führen alle Wissensdurstigen in die Tiefen des Kaninchenbaus.

**Verweise zum Technikteil**

### Aufbau der Workshops

Alle Workshops haben unterschiedliche Schwierigkeitsgrade für den Einsteiger bis zum Profi. Die beschriebenen Projekte können Sie mit VMware oder mit einem Microsoft-Produkt gleichermaßen nachvollziehen. Jedes Kapitel arbeitet jeweils mit einer anderen Virtualisierungssoftware. Einige Projekte werden auch mit den alternativen Produkten durchexerziert und die Unterschiede erklärt.

**Alle Schwierigkeitsgrade und alle Produkte**

**Auf einen Blick – jeder Praxisartikel liefert gleich zu Beginn folgende Informationen:**

- ▶ *Kurze Projektbeschreibung* – Was wollen/können Sie mit dem Workshop konkret erreichen?
- ▶ *Hauptprodukt* – An welchem Virtualisierungsprodukt wird das Projekt beschrieben? Mit welchen anderen Produkten ist es nachvollziehbar?
- ▶ *praktische Verwendung* – Welchen praktischen Nutzen hat das Projekt, wie können Sie die entstandenen virtuellen Maschinen sinnvoll verwenden?
- ▶ *Schwerpunkte* – Auf welche Themen geht dieser Workshop ganz besonders ein (z.B. Netzwerk, Snapshots, Klonen, P2V ...)?
- ▶ *Zielgruppe* – Für welche Anwender ist das Projekt besonders nützlich?

# 1 Eine Testumgebung mit VMware Workstation oder Server aufbauen

Anhand eines Praxisbeispiels erfahren Sie alles über die grundlegenden Funktionen und Konzepte von VMware Workstation und VMware Server, und Sie erhalten wichtige Tipps. Als Einstieg installieren Sie eine Test-VM, um ein alternatives Betriebssystem auszuprobieren, um Software zu testen oder um einen Client als Vorlage für ein produktives Rollout aufzubauen. Zum Abschluss klonen Sie die VM und erstellen ein virtuelles Netzwerk aus mehreren Maschinen. Nach diesem Workshop können Sie die Produkte bereits ausreichend bedienen, um z.B. eine Pilotumgebung aufzubauen.

**Einfache Test-VM  
oder Vorlage für  
ein Client-Rollout**

## Workshop im Überblick

### Hauptprodukt

- ▶ VMware Workstation und VMware Server – die Bedienung ist weitestgehend gleich.

### Praktische Verwendung

- ▶ Testmaschinen zum gefahrlosen Testen von Software und Patches oder zum Vorbereiten einer Software-Verteilung bzw. eines Client-Rollouts
- ▶ Linux unter Windows ausprobieren
- ▶ Abgeschottetes Surfen ohne Angst vor Viren auf dem Host
- ▶ Unterschiedliche Browsergenerationen in mehreren VMs betreiben

### Schwerpunkte

- ▶ Alle grundlegenden Funktionen von VMs kurz und knapp
- ▶ Erstellen, Bedienen und Verwalten von VMs
- ▶ Installation eines Betriebssystems im Gast
- ▶ Grundlagen zu virtuelle Platten, Redo-Logs und Snapshots
- ▶ Virtuelle Netzwerkkarten und unkomplizierte Netzwerkanbindung

### Zielgruppe

- ▶ Alle Einsteiger (und Aufsteiger) in das Thema
- ▶ Umsteiger von anderen Produkten



## 1.1 Vorteile virtueller Maschinen in Testumgebungen

### Zusätzliche Test-PCs oder Linux parallel betreiben

Egal ob Sie als Privatperson gerne einen separaten Rechner hätten, um ein Betriebssystem wie Linux auszuprobieren, oder ob Sie als Techniker, Entwickler bzw. Trainer eine Testumgebung benötigen – virtuelle Maschinen sind die ideale Lösung. Zusätzliche Rechner oder nervige Dual-Boot-Installationen können Sie sich dadurch sparen. Mit einer VM auf Ihrem PC brauchen Sie die Arbeit nicht zu unterbrechen, um auf die Schnelle ein anderes System zu booten. So läuft Linux ganz nebenbei auf dem gewohnten XP-Desktop, und weitere Maschinen stehen kurzfristig bereit, um neue Patches oder Software sicher zu testen. VMs bieten sich auch als virtuelle Kopie der produktiven Server für eine Pilotumgebung an.

### Besondere Vorteile von VMs

Als Zugabe bieten virtuelle Rechner weitere Vorteile, wie *Suspend-Modus* zum blitzschnellen Einfrieren und Auftauen eines Gastsystems inkl. aller laufenden Applikationen. Eine weitere Besonderheit sind *Snapshots* zur Sicherung und Wiederherstellung bei zerschossenen Konfigurationen. Mit einem Snapshot können Sie einen Zustand Ihrer VM sichern und jederzeit dahin zurückkehren. Sie können dadurch im Gast beliebige Tests ausführen oder Software installieren, ohne Angst um Ihr System in der VM zu haben. Sollte an einem Punkt etwas schief gehen, z.B. durch eine fehlerhafte Installation oder einen Virus, dann lassen sich jederzeit alle Änderungen verwerfen, ohne das System komplett neu zu installieren. Ein weiterer Vorteil virtueller Maschinen ist das schnelle Vervielfältigen (Klonen) von fertig eingerichteten Gästen durch einfaches Kopieren auf dem Host.

### 1.1.1 Unterschiede zwischen VMware Server und VMware Workstation

Dieser Einführungs-Workshop hilft Ihnen bei der Einrichtung Ihrer ersten VM und gibt wichtige Tipps zum Umgang mit virtuellen Maschinen. Er ist für VMware Workstation und VMware Server gleichermaßen gültig.



Die Folgeversion Workstation 6 unterscheidet sich nur in Details von der Version 5.5, bietet aber einige interessante Neuerungen. Mehr Informationen finden Sie im Teil 3, Kapitel 8 – Aktualisierungen, Ergänzungen und Neuerungen.

Der Hauptunterschied in der Bedienung beider Produkte ist, dass der VMware Server vom Host und von jedem Client im LAN über eine Remote-Konsole, die *VMware Server Console*, gesteuert werden kann. Am Host ist diese Konsole bereits automatisch eingerichtet. VMware Workstation wird dagegen immer nur am lokalen PC bedient.

Die Oberflächen ähneln sich stark und unterscheiden sich im Umgang nur minimal. Beim Server fehlen einige Komfort-Features wie multiple Snapshots, Klone oder Teams, dafür kommen Funktionen wie das Starten der Gäste als Dienst im Hintergrund dazu.

Auf die Unterschiede weise ich Sie in diesem Workshop an den entsprechenden Stellen hin. Einen ausführlichen Überblick über die Produkte mit Vor- und Nachteilen, Entscheidungshilfen zur Auswahl und Hinweise zur Bedienung finden Sie in *Teil 1* des Buches, eine detaillierte Auflistung der Unterschiede dort in *Kapitel 4*, „*Bedienung der Produkte – wichtige Funktionen und Tipps*“.

### 1.1.2 Weiterführende Workshops zu den Produkten

Dieser Workshop vermittelt Ihnen die Grundlagen und wichtige Tipps zum Umgang mit VMware Server und VMware Workstation. Zusätzlich mache ich Sie auf folgende weiterführende Workshops zu speziellen Anwendungsbeispielen und zu den anderen VMware-Produkten aufmerksam:

- ▶ *VMware Player* – Workshops zur Verwendung des kostenlosen VMware Players finden Sie in *Teil 2, Kapitel 5* und *Kapitel 6*. Der Umgang mit dem Player unterscheidet sich durch seine extrem eingeschränkte Oberfläche stark von der VMware Workstation und vom Server.
- ▶ *VMware Server und Workstation 5.5* – Neben diesem Einführungs-Workshop finden Sie weiterführende Projekte mit Schwerpunkt Netzwerk und Clustering in *Teil 2, Kapitel 8* (virtuelle DMZ und Cluster mit iSCSI).
- ▶ *VMware Server unter Linux* – Den Aufbau eines kostenlosen Server-Hosts unter Linux beschreibt *Teil 2, Kapitel 4*, ausführlich.
- ▶ *VMware ESX Server 3* – Der ESX Server unterscheidet sich in Konzept und Bedienung stärker von den anderen Produkten. Eine separate Anleitung zum ersten Kontakt mit dem VMware ESX Server 3 und dessen Besonderheiten finden Sie in *Teil 2, Kapitel 9*.

## 1.2 Voraussetzungen zur Arbeit mit virtuellen Maschinen unter VMware

Nur in diesem Einführungs-Workshop werde ich noch ein paar knappe Worte zu den Voraussetzungen und zur Installation der Virtualisierungssoftware verlieren. Detaillierte Informationen, die Sie zum schnellen Einstieg aber nicht sofort benötigen, finden Sie in *Teil 1* des Buches.

### 1.2.1 Der Host-Rechner oder Wirt als Basis für die VMs

Als Host-PC, oder auch Wirt, bezeichnet man den wirklich vorhandenen Rechner, auf dem die Virtualisierungssoftware installiert ist. Eine virtuelle Maschine, kurz VM, nennt man auch Gast. Mehrere Gäste können parallel auf einem Host laufen.

#### Anforderungen an die CPU und den RAM auf dem Host

Der Host sollte eine CPU im GHz-Bereich besitzen und mit mind. 512 MB RAM bestückt sein, besser mehr. Da RAM nicht emuliert wird, teilen sich alle laufenden VMs und der Host den verfügbaren realen Speicher. Unter VMware können Sie allen VMs in der Summe zwar mehr Speicher zuweisen, als physisch vorhanden ist. Durch Auslagerungsvorgänge kann darunter allerdings die Performance stark leiden, weshalb beim physischen RAM immer gilt: *Viel hilft viel*.

#### Notwendiger Plattenplatz auf den physischen Datenträgern

**Dateisystem  
NTFS verwenden**

Weiterhin muss der Host über ausreichend Plattenplatz verfügen. Je nach Betriebssystem und installierten Programmen benötigt jede VM mindestens 1–4 GB. Für eine bessere Performance sind mehrere Festplatten im Host empfehlenswert, mindestens eine für das Host-System und eine für die virtuellen Maschinen. Eine NTFS-Partition ist wegen ihrer Unterstützung von größeren Dateien als 2 GB einer FAT-Partition unbedingt vorzuziehen.

#### Unterstützte Host-Betriebssysteme

Als Betriebssystem auf dem Host werden von VMware alle aktuellen Windows-Versionen und auch Linux unterstützt. Auf Windows 98 oder Windows ME läuft VMware nicht.

### 1.2.2 Installieren und Einrichten von VMware Workstation und VMware Server

Die Installation der Produkte wird ausführlich in *Teil 1, Kapitel 3, „Installation und Konfiguration der einzelnen Produkte“* beschrieben. Auf einem Windows-System ist sie selbsterklärend und völlig unkompliziert, Sie können sofort starten. Für den VMware Server sollten Sie vor dem Setup den IIS (*Internet Information Server*) auf dem Host installieren, wenn Sie das Web-Interface verwenden wollen, das ist aber für diesen Workshop nicht zwingend notwendig.

**Linux-Host**

Wichtige Hinweise für eine Installation von VMware-Produkten unter Linux finden Sie ebenfalls in *Teil 1, Kapitel 3*, hier verläuft das Setup nicht immer völlig unkompliziert, weshalb bei fehlenden Linux-Kenntnissen für den ersten Kontakt ein Windows-Host empfehlens-

werter ist. In Teil 2, Kapitel 4, „Linux-Host mit VMware Server und Integration ins Windows-Netz“ wird sehr ausführlich der komplette Aufbau eines schlanken kostenlosen Linux-Hosts mit Windows-Anbindung und VMware Server Schritt für Schritt beschrieben. Dieser Server kann Ihnen als Basis für Test- und Produktivumgebungen dienen.

### Übersichtliche Ordner als Ablage für die VMs erstellen

Gleich nach der Installation der Produkte ist es empfehlenswert, für die zukünftigen VMs ein eigenes Verzeichnis auf der Host-Festplatte anzulegen. Beispielsweise einen Ordner *vmaschinen* mit Unterordnern wie *testumgebung*, *produktion* und *mustermaschinen*. So gestalten Sie Ihre entstehende virtuelle Welt von Beginn an übersichtlich. Ist eine zweite Festplatte im PC eingebaut, legen Sie Ihre VMs für bessere Performance am besten dort ab.

Im Menüpunkt EDIT/PREFERENCES/WORKSPACE/DEFAULT LOCATION lässt sich unter VMware Workstation das neue Standardverzeichnis für die virtuellen Maschinen einstellen. Beim Server findet sich der Punkt in der *VMware Server Console* unter dem Menü HOST/SETTINGS/GENERAL. So müssen Sie nicht beim Erstellen jeder neuen VM immer wieder in Ihr gewünschtes Verzeichnis navigieren.

**Standardordner festlegen**

## 1.3 Die erste virtuelle Maschine erstellen und konfigurieren

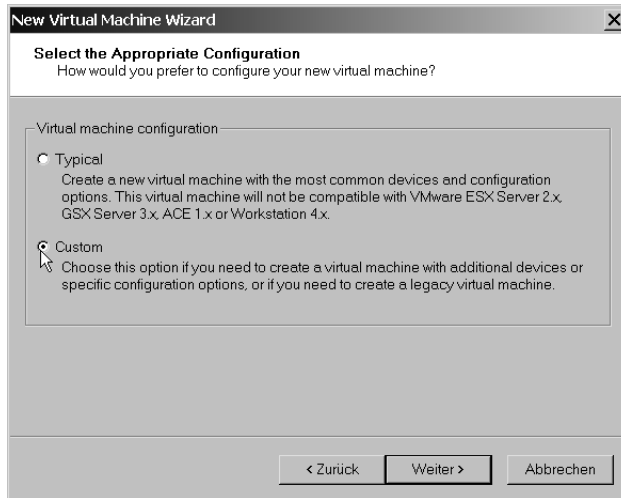
Nach so viel Vorrede können Sie nun endlich den virtuellen Schraubenzieher ansetzen, der sich unter VMware *New Virtual Machine Wizard* nennt. Mit ihm bauen Sie Ihre erste VM zusammen, ganz ohne Verletzungsgefahr an scharfen Gehäusekanten.

### 1.3.1 Grundausstattung der VM mit dem Virtual Machine Wizard konfigurieren

Über FILE/NEW VIRTUAL MACHINE startet der komfortable Wizard und fragt Sie nach einem Konfigurationstyp (Abbildung 1.1). Mit *Typical* könnten Sie sich eigentlich einige Mausklicks ersparen und die VM vom Wizard fast automatisch erstellen lassen. Da Sie Ihre VM aber genauer kennen lernen wollen, empfiehlt sich eine *Custom*-Konfiguration, wodurch Sie etwas mehr Kontrolle über verschiedene Einstellungen erhalten.

**Mehr Kontrolle mit Custom**

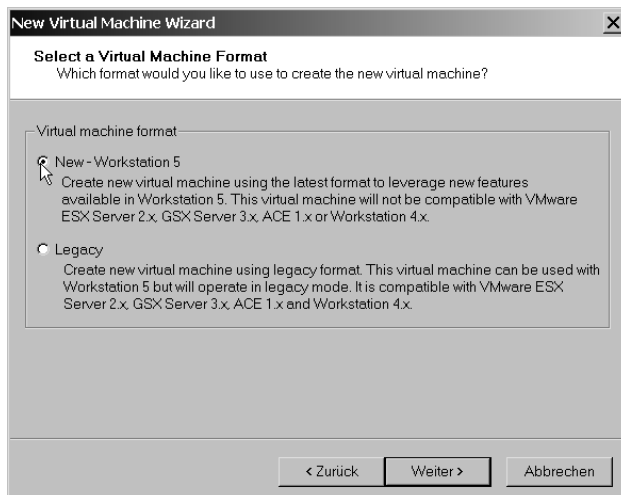
Abbildung 1.1:  
Mit einer Custom-  
Konfiguration haben  
Sie mehr Kontrolle  
über die Optionen  
bei der Erstellung  
einer VM



### Kompatible VMs zu älteren Versionen erstellen oder nicht

Bei der VMware Workstation können Sie sich entscheiden, ob die neue VM als *Legacy*-VM kompatibel zu älteren Versionen von VMware sein soll (Abbildung 1.2). Beim Server erscheint diese Abfrage nicht. Die neuen VMs der VMware Workstation 5.5 und des VMware Servers laufen nicht unter VMware GSX Server 3 oder VMware ESX Server 2, bzw. unter älteren Workstation-Versionen. Nur wenn Sie virtuelle Maschinen regelmäßig mit älteren Versionen austauschen wollen, sollten Sie bei der Frage nach dem Typ der VM mit LEGACY antworten, ansonsten wählen Sie immer NEW – WORKSTATION 5. Diese VMs sind zwischen VMware Player, Workstation 5.5, VMware Server und VMware ESX Server 3 kompatibel, was für fast alle Anwendungsfälle ausreichend ist. VMware Server erstellt immer Gäste in der neueren Version.

Abbildung 1.2:  
Legacy-VMs sind  
zwar kompatibel,  
aber eingeschränkt  
in den Funktionen



In einer kompatiblen Legacy-Maschine funktionieren keinerlei Snapshots und Klone, so dass dieser Typ nur eine Notlösung sein kann.



### Betriebssystem, Name und Ordner der VM festlegen

Im folgenden Bildschirm fragt der Wizard das zukünftige Gastbetriebssystem in der VM ab, das Sie aus der angebotenen Liste auswählen können. Während der Konfiguration werden auf dieser Grundlage bereits einige Parameter, wie RAM-Größe oder Plattentyp, vorgelegt, und VMware optimiert das Laufzeitverhalten des Gastes.

Im Anschluss ist für die VM ein passender Name festzulegen und ein eigenes Verzeichnis für die Dateien der Maschine auszuwählen. Für dieses erste Beispiel genügt als Name der VM *testvm01*. Sie haben den Standardordner für Ihre VMs bereits über EDIT/PREFERENCES eingestellt, der Name der VM wird auch gleich als Name des neuen Ordners übernommen (Abbildung 1.3). Über den Button BROWSE können Sie das Zielverzeichnis ändern. Im Ordner *\vmaschinen\testumgebung\testvm01* liegen später alle Dateien zu Ihrer virtuellen Maschine, z.B. die virtuellen Platten und die Konfiguration.

**Aussagekräftige Kürzel**

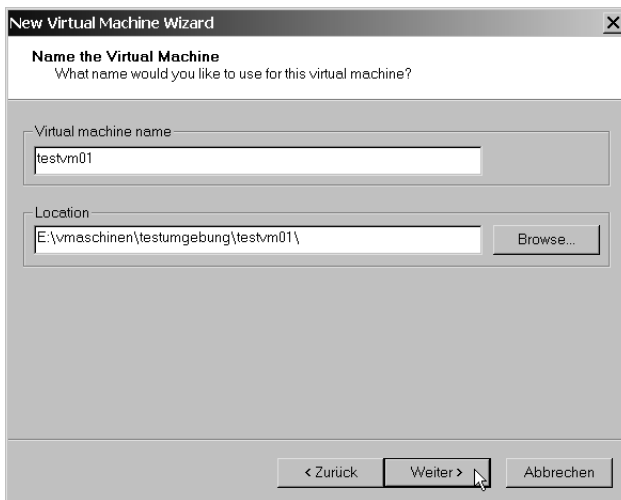


Abbildung 1.3:  
Im Ordner einer  
VM liegen später  
alle zugehörigen  
Dateien

Zwingen Sie sich bei der Benennung und der Verzeichnismwahl von Anfang an zur Ordnung, um nicht den Überblick über den schnell wachsenden virtuellen Rechnerpark zu verlieren.



## Dienstkonto für die VM und Verhalten beim Host-Start unter VMware Server festlegen

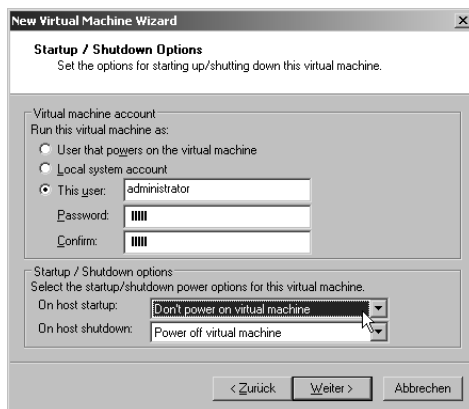
Nur beim VMware Server erscheinen jetzt im Wizard zwei Dialogfenster, die bestimmen, ob die VM auch für andere Nutzer sichtbar und unter welchem Benutzer die VM als Dienst ausgeführt wird. Für Ihre ersten Testumgebungen benötigen Sie die Funktionen noch nicht.

Ist der Haken an MAKE THIS VIRTUAL MACHINE PRIVATE gesetzt, dann ist die Maschine in der VMware Server Console nur für Administratoren und für den Nutzer, der die VM angelegt hat, sichtbar. Da Sie in der Testumgebung wahrscheinlich für den Anfang mit dem Administratorkonto oder zumindest immer mit dem gleichen Nutzer arbeiten werden, spielt diese Einstellung noch keine Rolle.

Im folgenden Dialog zum VIRTUAL MACHINE ACCOUNT (Abbildung 1.4) bestimmen Sie, ob der Gast als Dienst auf dem Host ausgeführt wird oder nicht, siehe auch Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“. Zur Rechteverwaltung erfahren Sie mehr in Teil 3, Kapitel 5, „Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs“.

Wenn Sie die Auswahl USER THAT POWERS ON THE VIRTUAL MACHINE stehen lassen, dann läuft die VM unter dem Nutzer, der gerade an der Remote-Konsole angemeldet ist, und kann nicht automatisch mit dem Host zusammen starten. Wählen Sie für den Anfang einfach einen Nutzer, der auf dem Host über genügend Rechte verfügt und von dem Sie das Passwort kennen, am einfachsten *Administrator*. Weiterhin können Sie in diesem Dialog bestimmen, ob die VM automatisch mit dem Host starten soll bzw. automatisch mit ihm herunterfährt.

Abbildung 1.4:  
Nur unter VMware  
Server können VMs  
unter einem Nutzer-  
konto als Dienst  
laufen und automa-  
tisch mit dem Host  
starten



## Prozessoren, RAM, I/O-Adapter und Netzwerkkarte im Gast

**Dual-CPU** Im Wizard folgt die Frage nach der Anzahl der Prozessoren. VMware kann an eine virtuelle Maschine zwei Prozessoren durchreichen, wenn im Host zwei CPUs vorhanden sind oder wenn Hyperthreading aktiviert ist. Das macht aber nur Sinn bei Anwendungen im

Gast, die zwei Prozessoren auch wirklich ausnutzen, etwa Datenbanken. In den meisten Fällen genügt eine einzige CPU in einem Gast.

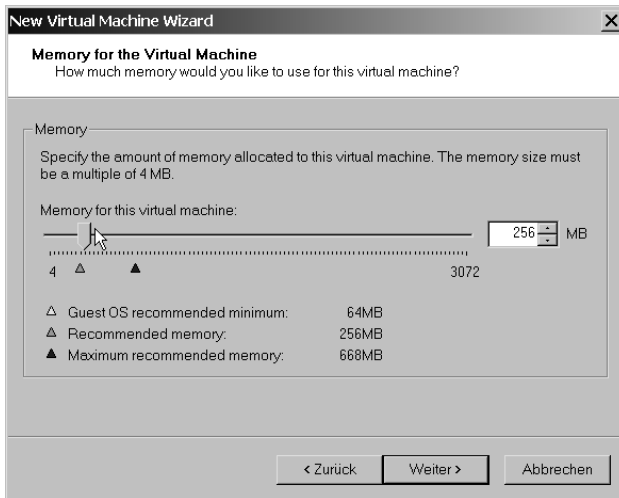


Abbildung 1.5:  
Hauptspeicher  
müssen sich alle  
laufenden VMs mit  
dem Host teilen

RAM können Sie Ihrer VM flexibel zuweisen (Abbildung 1.5). Beachten Sie aber, dass Hauptspeicher nicht emuliert wird. Den wirklich eingebauten RAM müssen sich alle laufenden VMs und der Host-PC teilen. Zwar können Sie unter VMware insgesamt mehr Speicher zuweisen, als physisch vorhanden ist. Für Testumgebungen mit vielen Maschinen kann das ein Ausweg sein. Allerdings führt das häufig zu starken Performanceeinbußen wegen notwendiger Auslagerungsvorgänge. Wenn möglich sollten Sie dem Gastsystem ausreichend RAM zuweisen, um vernünftig arbeiten zu können, dabei aber für den Host und für weitere laufende VMs genug übrig lassen. Bei 512 MB eingebautem Speicher im Host und zwei VMs mit Windows sollten beispielsweise jeder VM maximal 128 MB zugewiesen werden. Eine einzige VM kann dagegen mit 256 MB laufen. Hier sollten Sie immer Ihre eigenen Gegebenheiten, wie laufende Applikationen und Betriebssysteme, beachten. Im Zweifelsfalle folgen Sie einfach den Vorgaben des Wizards oder probieren die maximale Speicherzuweisung aus. Ausführlichere Informationen, wie VMware seinen Hauptspeicher verwaltet, finden Sie in *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*.

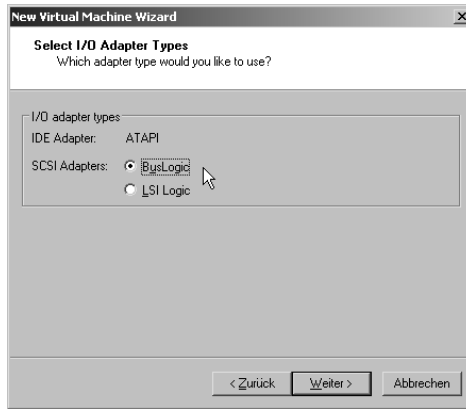
## Hauptspeicher

Die Voreinstellung des Wizards für die Netzwerkkarte übernehmen Sie vorerst. Ich gehe unter *Abschnitt 1.7.3, „Netzwerk zum Datenaustausch und zur Kommunikation mit dem Host und dem LAN“*, ausführlicher darauf ein. Genauso übernehmen Sie im nächsten Bildschirm den Vorschlag zum Typ des emulierten SCSI-Adapters *BusLogic* oder *LSI Logic*, der Wizard schlägt passend zum ausgewählten Gastbetriebssystem bereits die richtige Einstellung vor (Abbildung 1.6). Ausführlichere Informationen zu den Controllertypen enthält *Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“*.

## Netzwerkkarten und I/O-Adapter



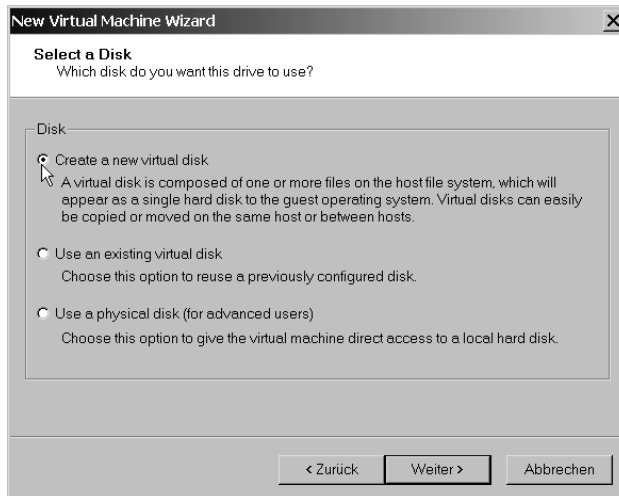
Abbildung 1.6:  
Der Typ des virtuellen  
Controllers wird  
vom Wizard bereits  
richtig vorgelegt



### Die virtuellen Platten – das Herzstück einer VM

Jetzt erstellen Sie mittels CREATE A NEW VIRTUAL DISK den ersten Datenträger für die virtuelle Maschine (Abbildung 1.7). Die virtuellen Platten sind das Herzstück der VM, weil in ihnen das eigentliche Betriebssystem sowie Programme und Daten liegen. Umfassende Informationen zu virtuellen Platten, Adaptertypen, Redo-Logs usw. finden Sie in *Teil 3, Kapitel 3*, für Ihre ersten virtuellen Maschinen genügen die Grundlagen aus diesem Workshop.

Abbildung 1.7:  
Sie können neue  
virtuelle Platten  
erstellen oder auch  
physische Daten-  
träger einbinden



### Behälterdatei oder physische Platte

Virtuelle Platten sind üblicherweise große Dateien, die auf der physischen Festplatte des Host-PC abgelegt werden. Ich bezeichne diese Dateien gerne als Behälterdateien auf dem Host, weil sie wie Behälter oder Container den Inhalt der virtuellen Platte des Gastsystems enthalten. In diese Dateien werden alle Schreib- und Lesezugriffe der VM umgeleitet, wobei das Betriebssystem in der VM denkt, mit einer richtigen Hardware-Platte zu arbeiten. Die Behälterdatei einer virtuellen Platte kann auf dem Host einfach kopiert und mittels USE AN EXIS-

TING VIRTUAL DISK (Abbildung 1.7) in eine andere VM eingebunden werden. Das entspricht dem Umbauen einer echten Festplatte von einem PC in einen anderen. Durch eine Kopie einer virtuellen Platte erhalten Sie einen 1:1-Klon des enthaltenen Betriebssystems. Virtuelle Platten lassen sich auf DVD brennen, als fertige Appliances über das Internet verteilen oder auf dem Laptop mitnehmen.

Man könnte mit USE A PHYSICAL DISK sogar physische Platten direkt in eine VM einbinden. Da dies aber bei unvorsichtiger Anwendung Daten auf dem Host zerstören kann, lassen Sie bei Ihren ersten Gehversuchen diese Option besser links liegen!



Mit CREATE A NEW VIRTUAL DISK legt der Wizard eine neue Platte an. Bei richtiger Vorauswahl des Betriebssystems schlägt der Wizard den passenden Typ IDE oder SCSI für die Platte vor (Abbildung 1.8). Bei der Auswahl des Plattentyps IDE oder SCSI spielt es übrigens keine Rolle, welche Hardware der Host-PC wirklich besitzt, die entsprechenden Controller werden in der VM nur emuliert. SCSI hat den Vorteil, mehr als vier Platten in die VM einbinden zu können und eine bessere Performance als IDE zu bieten.

#### SCSI oder IDE

Bei Problemen mit der virtuellen Platte sollten Sie zur Vorsicht immer den Festplattentyp IDE wählen, weil es damit keinen Treiberträger im Betriebssystem der VM gibt. Windows XP lässt sich z.B. ohne zusätzliche Treiber nicht in einem Gast mit SCSI-Platte neu installieren, weil das Setup während der Installation nicht den emulierten SCSI-Controller erkennt. Probleme können bei allen Gastsystemen auftreten, die keinen passenden SCSI-Treiber für die emulierten Controller mitbringen. Der Wizard schlägt bei den unterstützten Gastbetriebssystemen den richtigen Typ deshalb vor.

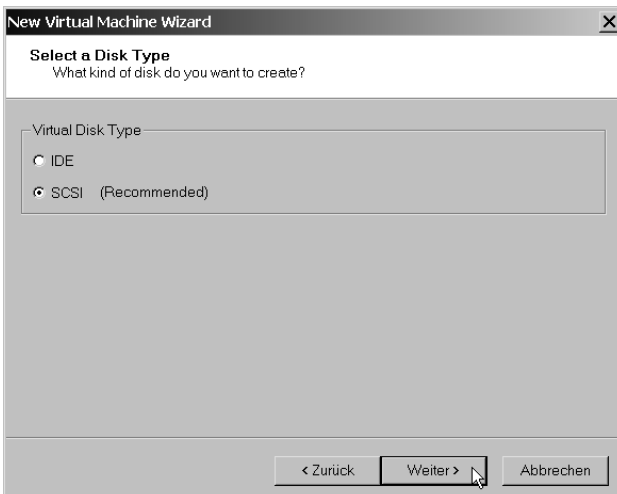


Abbildung 1.8:  
Unabhängig von der  
Hardware im Host  
können SCSI- oder  
IDE-Controller  
emuliert werden

**Zuwachsplatten** Die Größe der virtuellen Platte können Sie freizügig festlegen, da sie auf dem Host nur so viel Platz belegt, wie der Gast wirklich benötigt. Bei Bedarf wächst die Platte bis zur angegebenen Maximalgröße mit. Erst mit einem Haken an **ALLOCATE ALL DISK SPACE NOW** reserviert VMware den gesamten Platz der virtuellen Platte am Stück (Abbildung 1.9). Damit verhindert man zwar das Defragmentieren der Behälterdatei auf dem Host, verschenkt aber meist auch unnötig viel Platz auf den physischen Datenträgern. Noch dazu dauert das Erstellen der Platte sehr lange. Beim Server ist der Haken standardmäßig gesetzt, in Ihrer Testumgebung sollten Sie ihn entfernen, um Zeit und Platz zu sparen.

Abbildung 1.9:  
Die eingestellte  
Plattengröße wird  
normalerweise noch  
nicht reserviert.  
Die virtuelle Platte  
wächst bei Bedarf



Wenn der Host mit einer FAT32-Partition arbeitet, muss unbedingt der Haken an **SPLIT DISK INTO 2 GB FILES** gesetzt sein. Die Datei der virtuellen Platte wird dadurch in 2-GB-Segmente aufgeteilt, um die maximale Dateigröße auf FAT nicht zu überschreiten. Wollen Sie die VMs später auf mehrere DVDs brennen oder zum ESX Server konvertieren, ist diese Aufteilung in Streifen ebenfalls sehr nützlich, weil der Umgang mit mehreren 2-GB-Dateien einfacher ist als mit einer sehr großen zusammenhängenden Datei.

**Ordnung beim Plattennamen** Bei der Wahl des Plattennamens sollten Sie wieder mit System vorgehen, um später leichter auf den Inhalt einer virtuellen Platte schließen zu können. Eine gute Lösung ist es, den Namen der VM mit einem beschreibenden Kürzel zu kombinieren, wie *testvm01\_sys.vmdk* (sys für System). Später können Sie weitere Platten anlegen, etwa für die Daten (*data01*) oder auch für die Auslagerungsdatei (*swap*). Eine Trennung von System und Daten bringt Vorteile beim Klonen, Sichern und bei der Arbeit mit Snapshots (siehe Abschnitt 1.9, „Klonen von Gästen und weitere VMs für die Testumgebung erstellen“).

## Zugehörige Dateien der neu erstellten VM

Damit ist die Erstellung Ihrer VM abgeschlossen und unter FAVORITEN (Workstation) bzw. INVENTORY (Server) erscheint der neue Gast als Eintrag. Schauen Sie zuerst kurz ins Verzeichnis der eben erstellten virtuellen Maschine auf der physischen Festplatte, so sehen Sie dort schon einige Dateien, zur Laufzeit einer VM kommen weitere Dateien hinzu:

- ▶ *testvm01\_sys.vmdk* – Das ist die virtuelle Platte, die noch leer ist. Sie ist später das wichtigste Element der VM. Sie sehen auch, dass sie als Zuwachsplatte noch sehr wenig Platz belegt.
- ▶ *\*.vmx* – Die Datei mit dieser Endung ist die Konfigurationsdatei der VM, die alle Einstellungen, wie zugewiesene Hardware, im Textformat enthält. Die Konfigurationsdatei kann jederzeit ohne viel Aufwand neu erstellt werden. Die Datei wurde vom Wizard automatisch nach dem von Ihnen gewählten Betriebssystem benannt.
- ▶ *\*.vmsd* – Die Datei mit dieser Endung enthält später die Informationen zu den Snapshots der VM.
- ▶ *\*.lck* – Dateien mit dieser Endung zeigen an, dass die VM oder eine bestimmte virtuelle Platte gerade verwendet wird. *\*.lck*-Dateien haben keinen Inhalt und dienen nur dazu, um eine mehrfache Verwendung von Gästen oder virtuellen Platten in verschiedenen VMware-Instanzen zu verhindern.

### 1.3.2 Die Erstellung der ersten VM als Zusammenfassung auf einen Blick

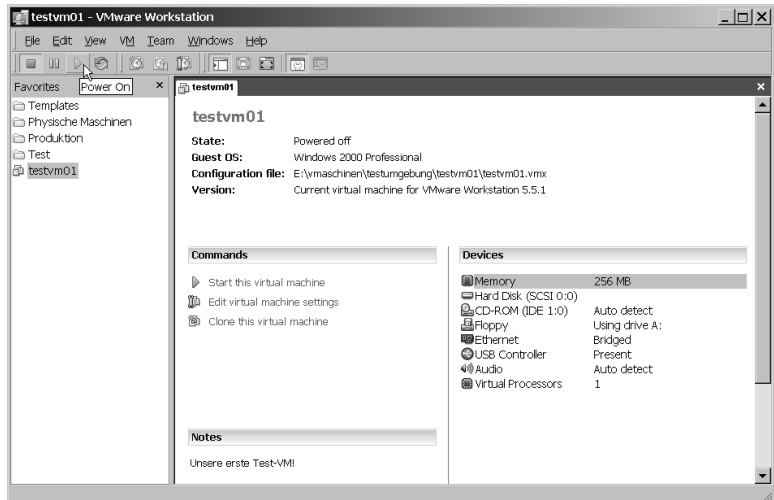
So schnell baut man sich einen neuen virtuellen Rechner – alle Schritte zum übersichtlichen Nachvollziehen hier nochmals auf einen Blick.

1. Wizard starten: FILE/NEW/VIRTUAL MACHINE
2. Virtual machine configuration: *Custom*
3. Virtual machine format (nur Workstation): *New – Workstation 5*
4. Guest operating system: *zukünftiges Betriebssystem in der VM*
5. Virtual machine name: *testvm01*
6. Virtual machine location: *vmaschinen\testumgebung\testvm01*
7. Make this virtual machine private (nur Server): *nein*
8. Startup / Shutdown Options (nur Server): *Vorgaben übernehmen*
9. Number of processors: *One*
10. Memory: *256 MB*
11. Network connection: *Use bridged networking*
12. I/O adapter types: *Vorgaben übernehmen*
13. Disk: *„Create a new virtual disk“*
14. Virtual Disk Type: *Vorschlag übernehmen (bei Problemen IDE)*
15. Disk capacity: *8 GB*
16. Disk file: *testvm01\_sys.vmdk*

## 1.4 Das VMware-Fenster und seine wichtigsten Bedienelemente

Das VMware-Fenster der Workstation oder die Remote-Konsole beim Server ist der Mittelpunkt Ihrer virtuellen Welt (Abbildung 1.10).

Abbildung 1.10:  
Das VMware-Fenster ist die Zentrale, VMware Workstation und VMware Server unterscheiden sich nur in Details



**Bildschirminhalt** Im linken Teil des VMware-Fensters erscheint die eben erstellte Maschine in der Favoritenleiste (beim Server *Inventory*). Hier können zur besseren Übersicht in der VMware Workstation mittels rechter Maustaste und NEW auch Ordner angelegt werden. Rechts im Fenster erreichen Sie alle aktiven VMs über eigene Reiter, unter denen normalerweise der Bildschirminhalt zu sehen ist. Da unsere eben erstellte VM noch ausgeschaltet ist, wird hier die zugewiesene Hardware angezeigt.

**Hardware-Ausstattung** Floppy, CD-ROM, USB und Sound wurden vom Assistenten ohne Nachfrage automatisch hinzugefügt, wenn entsprechende Hardware im Host vorhanden ist. Mit einem Doppelklick auf die Geräteeinträge können Sie spezielle Einstellungen für jedes Bauteil treffen, z.B. die Art der virtuellen Netzwerkkarte, ob das CD-ROM-laufwerk ein- oder ausgeschaltet ist und die RAM-Größe. Über den Menüpunkt VM/SETTINGS bauen Sie weitere virtuelle Hardware in die VM ein und konfigurieren diese.

**PowerOn, PowerOff, Suspend** In der Werkzeugleiste bietet VMware die wichtigsten Funktionen auf einen Blick. Für den Anfang genügen die drei Buttons POWEROFF, POWERON und RESET (Abbildung 1.11). Sie wirken wie die Schalter eines echten PC. Der zusätzliche Button SUSPEND friert eine laufende VM ein, speichert den RAM-Inhalt sowie den Status und schaltet sie dann ab, was dem Ruhezustand eines Laptops entspricht. Später kann die VM an genau dieser Stelle blitzschnell wieder aufgetaut

werden. Das spart Zeit, z.B. nach dem Hochfahren des Host-PC oder wenn man den RAM einer laufenden VM schnell für andere Maschinen benötigt.



Abbildung 1.11:  
Die Schalter der  
virtuellen Maschine

## 1.5 Installation des Betriebssystems in der neuen VM

Die neue Testmaschine könnten Sie schon mit dem grünen Button POWERON einschalten, allerdings ist die virtuelle Platte noch leer. Wie auf einem richtigen PC muss erst ein Betriebssystem installiert werden.

Stellen Sie sich bei allen Aktionen mit Ihrer virtuellen Maschine einfach vor, es wäre ein echter Rechner. Im Prinzip funktioniert Ihre VM nicht anders.



### 1.5.1 Installation von CD oder ISO-Image

Legen Sie die bootfähige Installations-CD Ihres Betriebssystems, z.B. Microsoft Windows XP, in das physische Laufwerk des Host-PC ein. Die VM kann standardmäßig darauf zugreifen und verwendet die eingelegte CD im Laufwerk. Es ist auch möglich, der VM ein ISO-Image direkt als eingelegte CD zu präsentieren, was besonders praktisch bei frisch gesaugten Linux-Distributionen oder Dateien aus der Microsoft MSDN ist. (Abbildung 1.12). Die Art der CD steuern Sie über das Hardware-Menü VM/SETTINGS oder im laufenden Betrieb ganz praktisch über das kleine CD-Symbol unten rechts in der Statusleiste (Abbildung 1.13).

**ISO-Image  
einlegen**

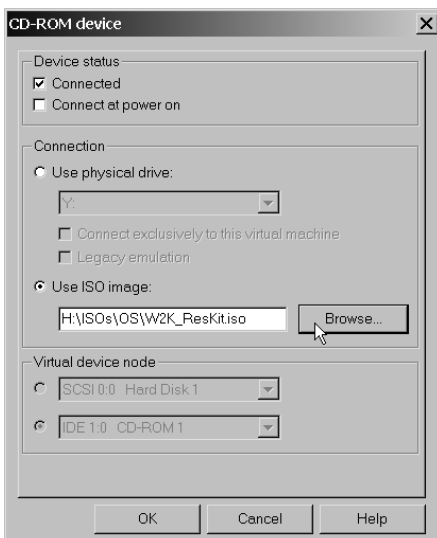


Abbildung 1.12:  
Auch ein ISO-Image  
kann als virtuelle  
CD dienen



Unter VMware Server kann ein Gast zusätzlich über das LAN auf eine CD im lokalen Laufwerk des Clients zugreifen, auf dem die Remote-Konsole läuft. Das erspart Ihnen als Admin den Weg in den Serverraum.

Abbildung 1.13:  
Im laufenden Betrieb  
kann die virtuelle  
Hardware über Sym-  
bole in der Status-  
leiste gesteuert  
werden

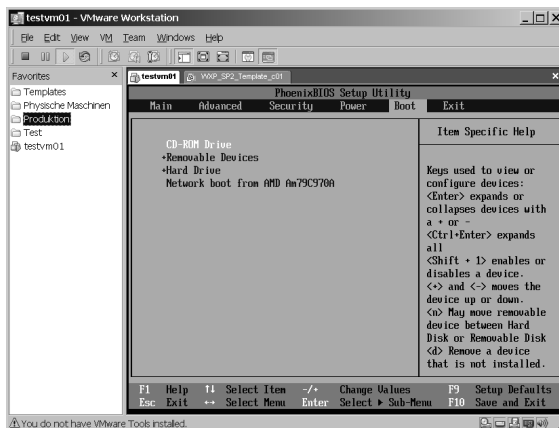


Die VM bootet jetzt von der physischen Installations-CD oder von einem ISO-Image. Die Setup-Routine installiert das Betriebssystem wie gewohnt und kopiert alle Systemdateien auf die virtuelle Festplatte, ohne zu wissen, dass sie nur eine Behälterdatei irgendwo auf dem Host-Datenträger ist. Schließlich findet die Hardware-Erkennung alle emulierten Geräte, als wären diese real.



Sollte die VM nicht von der CD starten, dann können Sie mittels **[F2]** das virtuelle CMOS-Setup aufrufen, um die Reihenfolge der Startgeräte anzupassen. Das ist notwendig, wenn auf der virtuellen Platte schon eine Partition existiert, von der die VM booten will (Abbildung 1.14).

Abbildung 1.14:  
Sogar ein CMOS  
wird in der VM  
emuliert



### 1.5.2 Verwendung von Tastatur und Maus in einem Gast

**Fokuswechsel** Ein paar grundlegende Dinge zur Bedienung Ihrer neuen VM sollten Sie unbedingt wissen. Um während der Installation in der VM die Tastatur verwenden zu können, müssen Sie vorher einmal in den Bildschirm der Maschine klicken. Erst dann landen die Tastenanschläge und Mausbewegungen in der VM und nicht mehr auf dem Host. Mit der Tastenkombination **[Strg] + [Alt]** erhält das Host-System den

Fokus dann wieder zurück. Ist diese Kombination schon anderweitig belegt, lässt sie sich unter EDIT/PREFERENCES/HOT KEYS ändern.

Als weitere Eigenheit wirkt der Griff zu **Strg** + **Alt** + **Entf**, z.B. beim Anmeldebildschirm, immer auf den Host selbst. In einer VM dient als Ersatz dafür **Strg** + **Alt** + **Einf**. Sollten Sie doch einmal (es wird öfter passieren!) versehentlich in einer VM **Strg** + **Alt** + **Entf** betätigen, dann erscheint auf dem Host der Windows-Sicherheitsdialog. Diesen können Sie einfach mit **ABBRECHEN** beenden. Danach sendet VMware nach einer Hinweismeldung die richtige Tastenkombination nachträglich an den Gast.

**Strg** + **Alt** + **Entf**

Sie können die Tastenkombination **Strg** + **Alt** + **Entf** auch über das Menü über VM/SEND **Strg** + **Alt** + **Del** an den Gast übermitteln.



### 1.5.3 Die Funktion der VMware Tools in einem Gast

Irgendwann nach den üblichen Neustarts der Betriebssysteminstallation steht der Gast im Anmeldebildschirm, und Sie werden sich über die eingeschränkte Bildschirmauflösung und die etwas schwergängige Maus wundern. Diese Probleme werden von den *VMware Tools* in einer Maschine gelöst. Die Tools werden über den Menüpunkt **VM/INSTALL VMWARE TOOLS** in den Windows-Gästen problemlos automatisch eingerichtet (Abbildung 1.15). In Linux-Gästen ist je nach Distribution unter Umständen erst die GUI zu beenden und inkl. CD-Mounten, TAR auspacken, Skript ausführen einiges manuell zu erledigen. Weiterhin werden oftmals die Kernel-Header und der Compiler benötigt. Eine ausführliche Beschreibung der VMware Tools finden Sie in *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*.

#### Maus und VGA

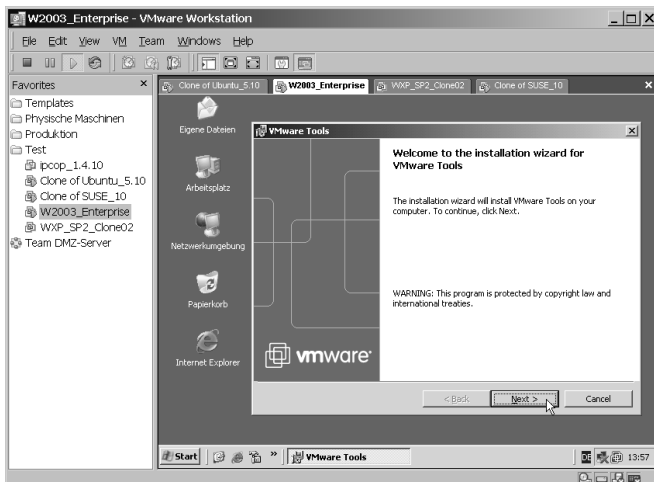


Abbildung 1.15:  
Die Installation der  
VMware Tools in  
den Gästen erleich-  
tert den Umgang  
mit den VMs



**Drag&Drop  
und mehr**

Die Tools bringen unter anderem eigene Treiber für Maus und VGA mit, die für glatte Mausbewegungen und stufenlos skalierbare Bildschirmauflösung bei Änderung der Fenstergröße sorgen. Damit passt sich das Gastsystem mit seiner Bildschirmauflösung dem VMware-Fenster automatisch an und füllt dieses Fenster ohne Scrollbalken oder schwarze Ränder genau aus. Weiterhin wird ein nahtloser Fokuswechsel vom Host in die VM und umgekehrt möglich, ohne umständliches Betätigen von `[Strg]` + `[Alt]` zum Befreien der Maus. Zusätzliche Features der Tools sind Drag&Drop zwischen Host und VMs, Shared Folders zum Datenaustausch (nicht beim Server), Zeitabgleich mit dem Host sowie automatisches Herunterfahren des Betriebssystems in der VM beim Klick auf POWEROFF.



Sollte die Tools-Installation nicht automatisch starten, liegt das am abgeschalteten CD-Autorun im Gast. Die Tools befinden sich auf einem ISO-Image, das von VMware automatisch als virtuelle CD eingebunden wird. Auf der im Gast erscheinenden CD finden Sie eine *Setup.exe*, die Sie im Windows Explorer mit einem Doppelklick starten können.

## 1.6 Mit Snapshots Systemzustände sichern

Im Prinzip ist die Installation des Betriebssystems jetzt abgeschlossen, und der virtuelle Rechner kann zum Testen verwendet werden. Allerdings fehlen noch alle notwendigen Service-Packs und Patches sowie Tools oder die benötigte Software für die Anwendungen im Gast. Bevor Sie am frisch aufgesetzten System Hand anlegen, sollten Sie dessen sauberen Zustand vorher mit einem SNAPSHOT sichern.

### 1.6.1 Zustände sichern und Änderungen verwerfen

**Redo-Logs**

Ein SNAPSHOT speichert den Systemzustand und den RAM-Inhalt einer VM. Festplattenschreibzugriffe landen ab sofort nicht mehr direkt auf der virtuellen Platte, sondern werden in so genannte *Redo-Logs* umgeleitet. Diese Logs sind zusätzliche Dateien, welche die veränderten Sektoren der virtuellen Platte vorläufig puffern.

**Software-Verteilung mit ZEN oder SMS testen**

Ein REVERT stellt den gesicherte Systemzustand in Sekunden wieder her und verwirft alle Änderungen in den Redo-Logs. Wenn die Installation eines Programms oder Patches schief geht, müssen Sie somit nicht alles neu installieren, die VM steht per Mausklick wieder im letzten sauberen Zustand.

Damit testen Sie z.B. sehr komfortabel eine Software-Verteilung, etwa mit ZEN Works oder Microsoft SMS, bevor Sie diese im LAN auf die physischen LAN-Clients anwenden. Sollten Sie mit dem Testergebnis im Gastsystem nicht zufrieden sein, dann setzen Sie die VM mit einem Revert zurück, korrigieren die Verteilungsregeln oder Software-Pakete und starten sofort einen neuen Versuch auf einem sauberen Gastsystem. Erst wenn alles läuft, wenden Sie die Verteilung auf Ihre physischen Rechner an, die Sie bei einem Fehler nicht so komfortabel zurücksetzen könnten.

Bevor Sie den ersten Snapshot in einer virtuellen Maschine gesetzt haben, funktioniert diese wie ein gewöhnlicher Rechner. Alle Änderungen werden unwiderruflich auf die virtuellen Platten geschrieben. Ein Verwerfen von Änderungen wird erst möglich, nachdem Sie einmal die Schaltfläche SNAPSHOT angeklickt haben.



## 1.6.2 Snapshots mit VMware Workstation und VMware Server anlegen und verwalten

Über die Werkzeugleiste (Abbildung 1.16) oder über das Menü VM/ SNAPSHOT sind alle Funktionen der Snapshots zu erreichen. Im VMware Server ist immer nur ein Snapshot möglich. Der nächste Snapshot überträgt alle Änderungen, die in den Redo-Logs zwischengespeichert sind, unwiderruflich auf die virtuelle Platte. VMware beginnt dann mit leeren Redo-Logs von vorn. Damit können Sie vor einem Test den Zustand der VM sichern und sich danach entscheiden, ob Sie alle Änderungen verwerfen wollen, etwa bei einem fehlergeschlagenen Test, oder ob Sie die Änderungen übernehmen wollen, z.B. nach einer erfolgreichen Patch-Aktualisierung.

**Snapshots mit dem VMware Server**

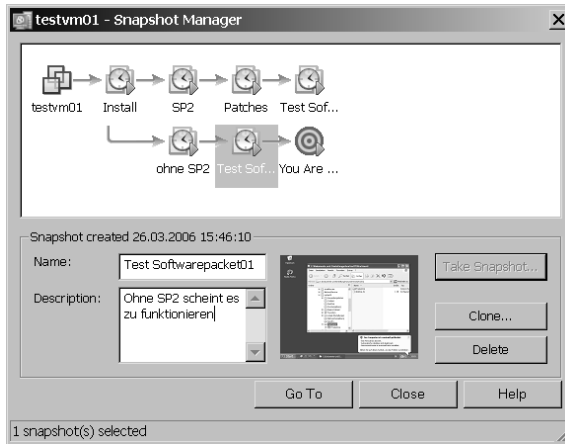


Abbildung 1.16:  
Die Snapshot-Funktionen in der Werkzeugleiste

In der VMware Workstation 5.5 ist die Snapshot-Funktionalität deutlich erweitert. Es ist dort möglich, mehrere Snapshots zu setzen und zwischen diesen unterschiedlichen Zuständen jederzeit beliebig zu wechseln, ohne dass Zustände verloren gehen. Ein grafischer Manager hilft in der Workstation dabei, nicht den Überblick über alle Sicherungen und die entstandenen Verzweigungen zu verlieren (Abbildung 1.17). Zwischen existierenden Snapshots wechseln Sie im Manager mit einem einfachen Doppelklick. So können Sie die Einrichtung und Installation des Systems in mehrere Wiederanlaufpunkte gliedern. Auch Verzweigungen sind möglich, um etwa ein Programm vor und nach einem bestimmten Service-Pack zu testen.

**Snapshot-Manager der Workstation**

Abbildung 1.17:  
Mehrere Wieder-  
anlaufpunkte und  
sogar Verzweigen  
werden mit  
multiplen Snapshots  
der VMware Work-  
station möglich



Beispielsweise können Sie zuerst das Betriebssystem im Gast sauber installieren und gleich darauf den ersten Snapshot setzen. Nach dem Einspielen von Service Pack 1 legen Sie den nächsten Snapshot an, nach Service Pack 2 einen weiteren. Es folgen die aktuellen Patches und dann Stück für Stück alle Programme oder kritische Einstellungen, dazwischen immer wieder ein Snapshot (Abbildung 1.17). Wenn Ihnen während der Installation irgendetwas schief geht, können Sie z.B. zum Zustand ohne Patches wechseln und von vorn beginnen. Oder Sie können ein Programm mit Service Pack 2 testen und dann in einem Zustand, in dem Service Pack 2 noch fehlt.

### Client-Rollout mit einer Master- VM

Der Wechsel zwischen den Systemzuständen erfolgt innerhalb weniger Sekunden. Auf diese Weise bereiten Sie z.B. sehr komfortabel ein komplettes Client-Rollout mit einer Master-VM vor. Snapshots lassen sich im Manager auch gleich kommentieren. Das ist eine wichtige Funktion, die Sie unbedingt ausgiebig nutzen sollten, sonst wissen Sie bald nicht mehr, welche Änderungen ein bestimmter Snapshot enthält.



Zu den Snapshots finden Sie einen eigenen Workshop in *Teil 3, Kapitel 4*, „Die Snapshot- und Clone-Funktion der VMware-Produkte“. Ich gehe in den Praxiskapiteln nicht auf alle Details ein. Für den Anfang genügen ein oder zwei Snapshots während der Installation Ihrer Test-VM.

### Probieren Sie Snapshots einfach in Ihrem Gastsystem aus

Sie haben gerade die Installation des Betriebssystems abgeschlossen und bereits den ersten Snapshot gesetzt. Starten Sie in Ihrer VM den Windows-Explorer, und löschen Sie z.B. den Ordner *Programme*. Benennen Sie andere Dateien um, entfernen Sie Treiber im Geräte-manager, bis nichts mehr geht – trauen Sie sich ruhig!

Unabhängig davon, was Sie im System der VM eingerichtet haben, mit einem einfachen Klick auf REVERT ist alles wieder heil. Ihre VM steht unbeeindruckt an genau der gleichen Stelle wie vor dem Snapshot und kann sich an Ihre Zerstörungswut nicht mehr erinnern. Alle Beschädigungen und alle Änderungen sind vergessen, alle gelöschten Ordner wieder da.

### 1.6.3 Platten vor Datenverlust durch Revert schützen

Bei einem REVERT gehen alle Änderungen seit dem letzten Snapshot verloren, natürlich auch solche an den Daten. Das ist nicht immer erwünscht, weil man zwischenzeitlich in der VM gearbeitet hat. Wollen Sie bestimmte Platten vor einem Datenverlust schützen, so können Sie diese in den Modus *independent-persistent* setzen. Solche Platten sind von den Snapshots ausgenommen und werden immer direkt beschrieben. Die Einstellung erreichen Sie über den Schalter ADVANCED zur entsprechenden virtuellen Platte (Abbildung 1.18). Damit können Sie mit einem Revert das System reparieren, etwa nach einer fehlerhaften Programminstallation, ohne Ihre Datenplatte auf einen früheren Stand zurückzusetzen.

**independent-persistent**

Datenschutz mit *Persistent*-Platten ist einer der Gründe, warum es sinnvoll ist, System- und Datenplatten zu trennen. Der Modus lässt sich allerdings nur einschalten, wenn noch kein Snapshot in der VM existiert, und mit einer solchen Platte sind keine Snapshots im laufenden Betrieb möglich.



Abbildung 1.18:  
Im Modus *independent-persistent* werden alle Änderungen sofort und unwiderruflich geschrieben

## 1.7 Kommunikation und Datenaustausch der Gäste

Nach dem ersten Snapshot beginnen Sie sorgenfrei die weitere Installation und Konfiguration Ihrer Test-VM. An dieser Stelle taucht schnell die Frage auf, wie man Dateien mit der VM austauschen kann bzw. wie die VM ins Internet kommt, um sich dort Patches und Installationspakete abzuholen.

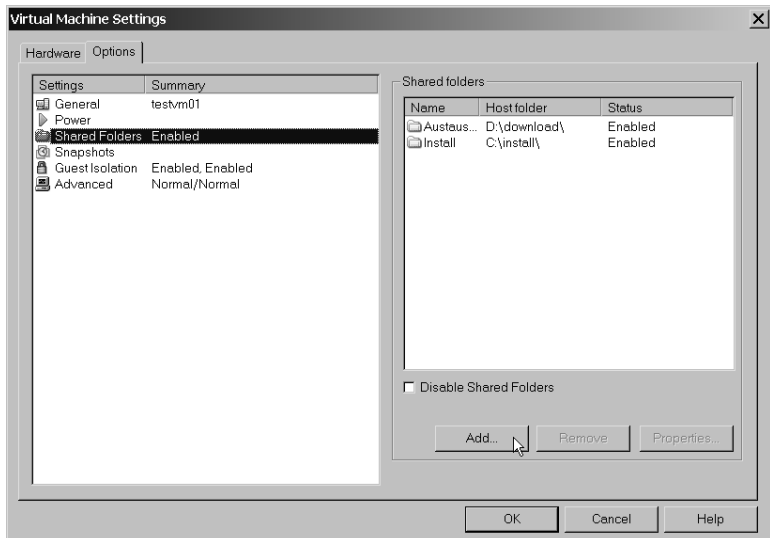
### 1.7.1 Drag&Drop sowie Shared Folders zum Datenaustausch mit dem Host

Die einfachste Methode zum Datenaustausch mit den Gastsystemen ist *Drag&Drop*. Sie ziehen Dateien einfach vom Host in die VM und umgekehrt. Für den Zugriff auf komplette Ordner der Host-Platte bieten sich *Shared Folders* an. Diese lassen sich über VM/SETTINGS/OPTIONS/SHARED FOLDERS einstellen (Abbildung 1.19). Die so freigegebenen Ordner des Hosts sind in der VM unter der Netzwerkumgebung sichtbar. Damit haben Sie z.B. permanenten Zugriff auf ein Host-Verzeichnis und müssen nicht jede Datei erst mittels Drag&Drop in den Gast kopieren.



*Cut&Paste, Drag&Drop und Shared Folders funktionieren nur bei installierten VMware Tools in den Gästen. Der VMware Server unterstützt grundsätzlich keine Shared Folders und kein Drag&Drop.*

Abbildung 1.19:  
Shared Folders der  
VMware Work-  
station ermöglichen  
das Freigeben von  
Host-Ordern in  
eine VM



### 1.7.2 ISO-Images als CD im Gast verwenden

Eine weitere Methode zum Datenaustausch, die allerdings nur einseitig hin zum Gast funktioniert, ist die Verwendung von ISO-Images. Von immer wieder benötigten Dateien oder oft verwendeten CDs können Sie Archive erstellen und in das virtuelle CDROM-Laufwerk einlegen. Sie haben Ihr Betriebssystem in der VM eventuell schon von einem ISO-Image installiert. ISO-Images können Sie im laufenden Betrieb der VM einfach austauschen, wie CDs in einem Laufwerk. Tools zur Erstellung von ISO-Images finden Sie in *Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“*.

### 1.7.3 Netzwerk zum Datenaustausch und zur Kommunikation mit dem Host und dem LAN

Der flexibelste Weg zur unabhängigen Kommunikation ist die ausgereifte Netzwerkunterstützung von VMware. Beim VMware Server bleibt Ihnen nichts anderes übrig, weil er keine Shared Folders und kein Drag&Drop unterstützt. In jede Maschine können Sie bis zu vier virtuelle Netzwerkkarten einbauen (Abbildung 1.20). Sie erscheinen innerhalb der VM als *AMD PCNET-Adapter*, für den jedes Betriebssystem Treiber mitbringt. Diese Adapter können ihre IP-Adresse mittels DHCP erhalten oder manuell konfiguriert werden. Sie funktionieren mit TCP/IP genauso wie mit IPX/SPX oder NETBUI.

#### Virtuelle Netzwerkkarten

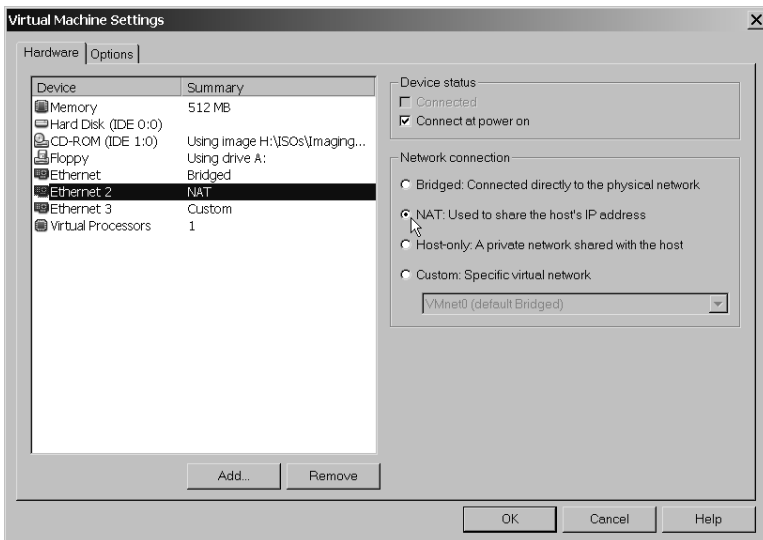


Abbildung 1.20: Drei virtuelle Netzwerkkarten können mit unterschiedlichen Anschlussarten eingebaut werden

VMware stellt vier Konfigurationstypen virtueller Adapter zur Verfügung, und der Typ entscheidet darüber, wie die VM mit dem Rest der Welt kommunizieren kann. Für unsere erste VM genügen vorläufig die beiden Typen *Bridged* oder *NAT*. Eine umfassende Beschreibung der

Netzwerkfunktionalität finden Sie in separaten Workshops in, *Teil 3, Kapitel –1, „Virtuelle Netzwerke Teil 1 – Schnellstart“*, und in *Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“*.

### Netzwerkkarte im Modus Bridged für direkte LAN-Anbindung

**Direkt im LAN** Haben Sie eine virtuelle Netzwerkkarte eingebaut, um Ihre VM in ein LAN zu integrieren oder weil ein Router den Internet-Zugang bereitstellt, dann wählen Sie als Typ der Karte *Bridged*. Ein Adapter mit dieser Konfiguration kann über eine physische Netzwerkkarte des Host-PC mit dem LAN kommunizieren. Der Netzwerkverkehr wird an die physische Karte durchgereicht, und die VM erscheint in der realen Welt wie ein vollwertiger PC mit eigener MAC-Adresse. Die VM hat vollen Zugriff auf das Netz und ist uneingeschränkt zu erreichen. Sie benötigt dazu natürlich eine freie IP-Adresse aus dem LAN oder holt sich diese von einem DHCP-Server.



Alle VMs im Modus *Bridged* sind parallel und unabhängig zum Host-System im LAN sichtbar.

### Netzwerkkarte im Modus NAT für eine indirekte Anbindung

**ISDN, UMTS  
oder Modem**

NAT steht für *Network Address Translation* und wird auch in Routern verwendet, um allen Clients im LAN über eine einzige öffentliche IP eines Routers Zugriff auf das Internet zu geben. Wenn Sie keine Netzwerkkarte im PC haben, sondern ISDN, UMTS, ein Analogmodem oder ein direkt angeschlossenes DSL-Modem für den Internet-Zugang verwenden, dann wählen Sie als Typ der virtuellen Netzwerkkarte *NAT*. Das ist auch sinnvoll, wenn Sie keine freie IP-Adresse im LAN kennen, an dem der Host (z.B. Ihr Laptop) angeschlossen ist.

Eine virtuelle Netzwerkkarte vom Typ *NAT* verwendet einfach die funktionierende Netzwerkverbindung des Hosts mit. Die VM bekommt automatisch eine interne IP-Adresse zugewiesen, ohne dass Sie sich darum zu kümmern brauchen. Der Verkehr gelangt über einen internen Routerdienst mittels NAT zum Host und unter dessen öffentlicher IP nach draußen. Ein NAT-Adapter benutzt die bestehende Internet-Verbindung des Host-PC mit, ohne dass Sie genau wissen müssen, wie diese funktioniert.

### Den Anschlusstyp umschalten oder die Verbindung trennen

Den Anschlusstyp einer Netzwerkkarte schalten Sie im laufenden Betrieb einfach um, entweder über VM/SETTINGS (Abbildung 1.20) oder wieder unten rechts über die Statusleiste des Fensters der VM (Abbildung 1.21). Für das Gastsystem ist das Ändern der Verbindungsart das Gleiche, wie das Umstecken eines Patchkabels. Genauso kann mit dem Entfernen des Hakens an CONNECTED das virtuelle Anschlusskabel abgezogen werden.



Abbildung 1.21:  
Die emulierte Netz-  
werkkarte in einem  
Gast stellt die  
Verbindung mit  
dem LAN her

Als Geschwindigkeit der virtuellen Netzwerkkarte wird im Gast immer nur 10 Mbit angezeigt, das ist normal. Ein AMD-PCNET-Treiber der emulierten Netzwerkkarte kennt nichts anderes. Es wird trotzdem die reale Geschwindigkeit des LAN-Anschlusses verwendet. Bei installierten VMware Tools wird automatisch ein optimierter Treiber verwendet, der immer 1 GBit/s anzeigt (Abbildung 1.21).



## 1.8 Die Betriebssysteminstallation und Konfiguration der VM auf einen Blick

Jetzt lässt sich die VM über eine CD oder über das Netzwerk mit weiterer Software versorgen und kann den eigenen Wünschen entsprechend eingerichtet werden. Snapshots sichern dabei die erreichten Konfigurationsstände und lassen jederzeit den Schritt zurück offen. Den gesamten Prozess der Betriebssysteminstallation können Sie hier auf einen Blick nachvollziehen.

1. Eine bootfähige Betriebssystem-CD ins physische Laufwerk einlegen oder ein ISO-Image über VM/SETTINGS zuweisen.
2. Die VM starten. Bei Bedarf die Bootreihenfolge im Bios mit **[F2]** ändern.
3. Das Betriebssystem in der VM installieren wie auf einem normalen PC. Beachten Sie dabei:
  - ▶ Fokuswechsel zwischen Host und Gast erfolgt mit **Klicken** und **[STRG] + [ALT]**.
  - ▶ Ersatz für **[STRG] + [ALT] + [Entf]** ist im Gast **[STRG] + [Alt] + [Einf]**.
4. Die VMware Tools in der VM installieren mit VM/INSTALL VMWARE TOOLS.
5. Den ersten Snapshot setzen, um den erreichten Stand zu sichern.
6. Eine Netzwerkverbindung für das Gastsystem einrichten:
  - ▶ *Bridged* – für einen Router oder eine LAN-Anbindung.
  - ▶ *NAT* – für Modem, ISDN oder UMTS.
  - ▶ *Alternativen* – Shared Folder oder ISO-Images verwenden.
7. Patches, Service-Packs und Programme im Gast installieren.
8. Einen neuen Snapshot zur Sicherung des erreichten Standes setzen.



## 1.9 Klonen von Gästen und weitere VMs für die Testumgebung erstellen

Wenn Sie mit Ihrer ersten VM genügend Erfahrungen gesammelt haben, möchten Sie vielleicht eine zweite oder dritte Maschine aufsetzen, um ein kleines Netzwerk aufzubauen. Dazu könnten Sie natürlich weitere Maschinen komplett neu installieren. Es geht aber viel komfortabler.

### 1.9.1 Kopieren virtueller Platten zum Klonen eines Gastsystems

#### Auf andere Rechner übernehmen

Durch einfaches Kopieren des gesamten Ordners Ihrer neuen VM können Sie bereits einen vollständigen Klon erzeugen. Über das Menü FILE/OPEN oder noch einfacher mit einem Doppelklick auf die Konfigurationsdatei *\*.vmx* lässt sich die Kopie danach in VMware öffnen. Sie können die *\*.vmx*-Datei auch einfach mit der Maus in die Favoriten des Fensters der VMware Workstation ziehen (nicht am VMware Server). Auf diese Weise haben Sie z.B. die fertig konfigurierte Maschine in Minuten auf einen anderen Host-Rechner übernommen, z.B. vom Laptop auf einen Kundenserver.

#### System und Daten trennen

Manchmal ist es einfacher und schneller, nur die Datei der virtuellen Systemplatte zu kopieren. Wenn Sie separate Platten für das System, die Daten und das Swapfile eingerichtet haben, müssen Sie nicht jedes Mal den gesamten Datenballast mitkopieren. Anschließend erstellen Sie mit dem VMware Wizard eine neue VM im *Custom*-Modus und binden die Kopie der virtuellen Platte mittels USE AN EXISTING VIRTUAL DISK ein, anstelle eine neue Platte zu erstellen (siehe auch Abbildung 1.7).



Wenn Snapshots vorhanden sind, dann müssen Sie immer den gesamten Ordner einer VM kopieren, da der Inhalt des Gastes auch in den Redo-Logs der Snapshots verteilt ist! Oder Sie entfernen alle Snapshots vor dem Klonen und verdichten damit die Redo-Logs auf die Basisplatte (siehe auch Teil 3, Kapitel 4, „Die Snapshot- und Clone-Funktion der VMware-Produkte“).

### 1.9.2 Linked Clones mit VMware Workstation zum schnellen Klonen

Noch komfortabler ist das Klonen auf dem gleichen Host mit dem Clone-Wizard der VMware Workstation 5.5, erreichbar über VM/CLONE (Abbildung 1.22).

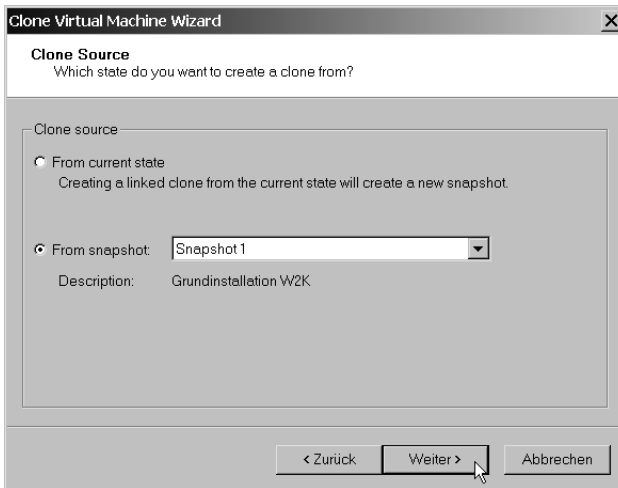


Abbildung 1.22:  
Ein Wizard über-  
nimmt das Klonen  
von einem beliebigen  
Zustand der VM

Neben einem *Full Clone*, der auch wieder nur eine komplette Kopie erstellt, wird mit einem *Linked Clone* nicht die gesamte virtuelle Platte zeit- und platzraubend kopiert. Stattdessen benutzt der erzeugte Klon lesend die Platte der Vorlage und schreibt in ein eigenes Redo-Log, ähnlich wie bei einem Snapshot. Der Klon-Vorgang dauert dadurch nur Sekunden, und die neue Maschine belegt kaum Platz. In wenigen Minuten haben Sie einen ganzen virtuellen Rechnerpark für verschiedene Testszenarien zusammengekllickt (Abbildung 1.23).

#### Full oder Linked Clone

Die Funktion der Linked Clones existiert unter VMware Server nicht, kann aber mit Tricks nachgebildet werden, lesen Sie dazu *Teil 3, Kapitel 4*.

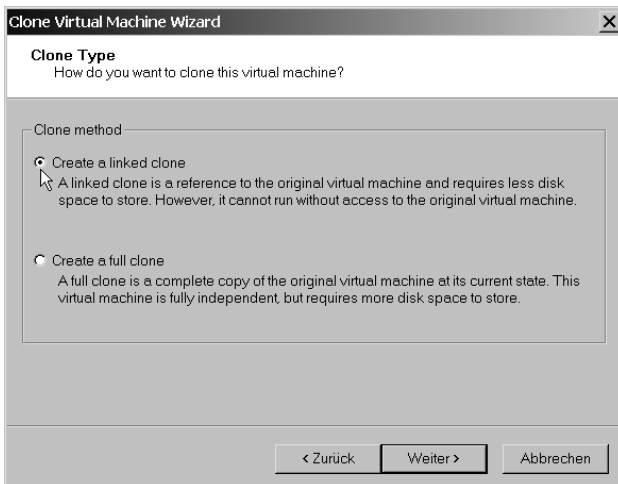


Abbildung 1.23:  
Ein Linked Clone  
funktioniert ähn-  
lich wie eine Ver-  
zweigung in den  
Snapshots, er wird  
aber als neue VM  
angelegt



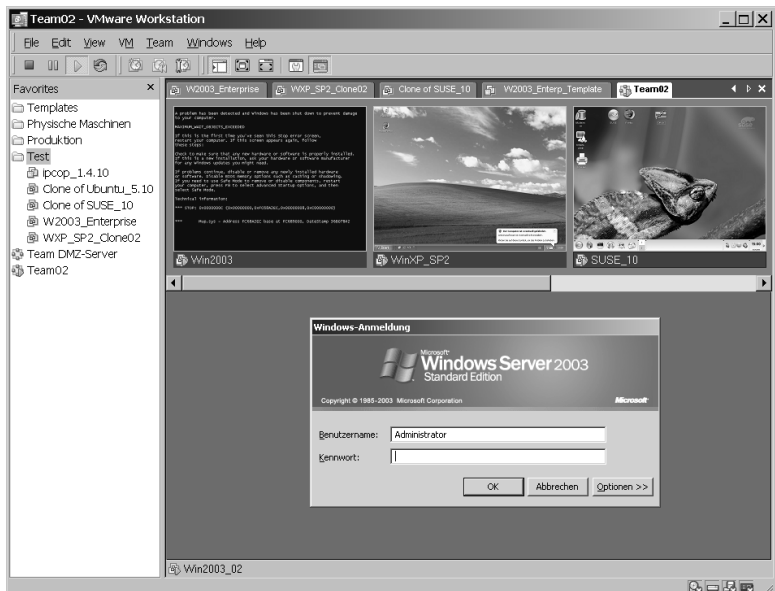
Ein *Linked Clone* benötigt immer die zugrunde liegende Quellmaschine und funktioniert ohne diese nicht mehr! Der Snapshot der Quellmaschine, auf dem der Klon aufsetzt, darf nicht verändert oder gelöscht werden. Am besten Sie verwenden in der Quellmaschine den so genannten *Template-Modus*. Einzelheiten zu Klonen, Snapshots und Redo-Logs finden Sie in *Teil 3, Kapitel 4*.

**Klone anpassen** Wie auf einem physischen Rechner ist in jedem Klon für eine eindeutige IP-Adresse, Rechnernamen und gegebenenfalls *SID* (*Security Identifier*) zu sorgen. Das Verfahren zur Verwendung von Sysprep oder NEWSID in einem Klon, um z.B. SID automatisch anzupassen, ist in *Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“* beschrieben, Sie benötigen diese Funktion für Testumgebungen nicht unbedingt. Das genannte Kapitel beschreibt zusätzlich einige Tipps zur Vorbereitung der Gäste zum Klonen.

## 1.9.3 Teams fassen mehrere VMs zusammen

Mehrere virtuelle Maschinen (auch Linked Clones) kann VMware Workstation 5.5 über FILE/NEW TEAM auch zu einem Team zusammenfassen. Damit lassen sich ganze Testnetzwerke gemeinsam starten, beenden oder in den Suspend-Modus versetzen (Abbildung 1.24).

Abbildung 1.24:  
Ein Team der  
VMware Work-  
station kann aus  
verschiedenen VMs  
bestehen



Im internen Netzwerk zwischen diesen Teams können Sie LAN-Geschwindigkeiten drosseln oder über TEAM/SETTINGS/LAN SEGMENTS verlorene Pakete simulieren. So testen Sie den langsamen Zugriff auf Webseiten oder das Verhalten von Synchronisationsvorgängen über WAN-Verbindungen (Abbildung 1.25).

Teams, mehrere Snapshots und Linked Clones bietet nur die VMware Workstation, nicht der VMware Server oder der Player.

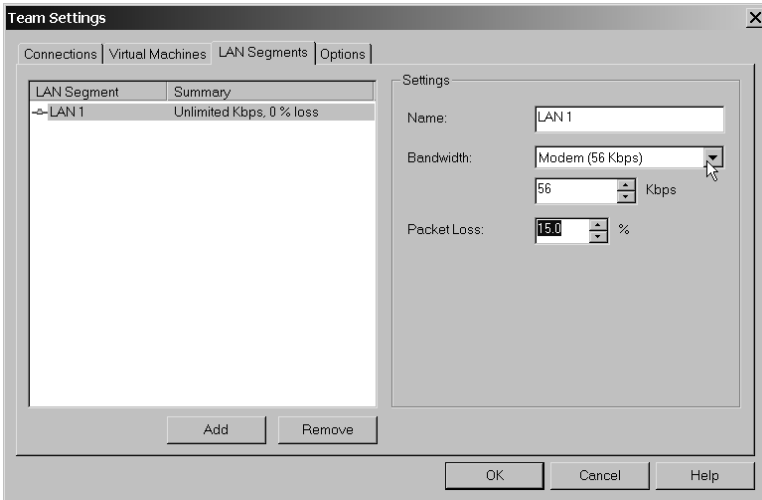


Abbildung 1.25:  
Teams haben eigene  
interne Netze, für  
die sich bestimmte  
Parameter einstellen  
lassen

## 1.10 Wie geht es jetzt weiter?

Ihre virtuelle Testumgebung ist fertig und kann je nach Bedarf mit wenigen Mausklicks weiter ausgebaut werden. Nach ein paar Tagen können Sie sich wahrscheinlich kaum noch vorstellen, wie Sie bisher in Testumgebungen ohne virtuelle Maschinen gearbeitet haben. In *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“* finden Sie noch weitere Features und Hinweise, die Sie aber nicht sofort benötigen, z.B. zur Hauptspeicherverwaltung, zum Vollbildmodus der Gäste oder zur Startreihenfolge der VMs unter dem Server sowie zum Web-Interface. Tiefere Einblicke in Themen wie Netzwerke oder virtuelle Platten erhalten Sie in *Teil 3* des Buches.



# 2 Mobile virtuelle Entwicklungs- und Demo-Umgebung mit Virtual PC

Wir setzen einen virtuellen Web- oder Datenbankserver auf, der als mobile Entwicklungs- und Demo-Umgebung genutzt wird. Der Server ist auf dem Laptop immer mit dabei und steht bei Bedarf sogar den Mitarbeitern im Firmen-LAN zur Verfügung. Beim Kunden kann er für Produkt-Demos eingesetzt werden, ohne zusätzliche Rechner mitzuschleppen. Zum Schluss entstehen noch verschiedene Clients mit unterschiedlichen Browserkonfigurationen.

**Datenbank- oder Webserver**

## Workshop im Überblick

### Hauptprodukt

- ▶ Microsoft Virtual PC 2004
- ▶ Umsetzbar auch auf VMware Workstation und Player

### Praktische Verwendung

- ▶ Entwicklungsumgebung auf verschiedenen PCs und auf dem Laptop.
- ▶ Einfach transportierbare Demo-Umgebung für Kunden oder Messen.
- ▶ Kleiner Intranet- oder Groupware-Server im LAN.

### Schwerpunkte

- ▶ Verwendung einer VM auf unterschiedlichen Rechnern.
- ▶ Verschiedene Netzwerkanbindungen – LAN, lokal, NAT.
- ▶ Schutz von produktiven Daten auf virtuellen Platten.
- ▶ Platzsparendes Betreiben mehrerer VMs.

### Zielgruppe

- ▶ Programmierer, Webdesigner, Datenbankentwickler
- ▶ Trainer, Vertriebsmitarbeiter, Consultants

## 2.1 Virtueller Webserver für Test und Demo

### Produkt-Demo und Entwicklung

Wer kennt das nicht: Die gerade fertig gestellte Webseite muss unter mehreren Browserversionen richtig dargestellt werden oder ein neu entwickeltes Programm soll unter NT genauso laufen wie unter Windows 2000 bzw. XP. Während der Produktvorstellung vor Ort beim Kunden wird ein passend konfigurierter Server samt SQL-Datenbank benötigt. Diesen könnte man auch unterwegs als Entwicklungsumgebung auf dem Laptop gebrauchen. Zusätzliche Rechner möchte man allerdings weder am Arbeitsplatz stehen haben noch herumschleppen. Und für ein Testsystem ständig andere Partitionen zu booten, ist auch sehr unhandlich. Virtuelle Maschinen können solche Probleme auf einen Schlag lösen.



Der Workshop arbeitet mit Microsoft Virtual PC. Eine Umsetzung auf VMware Server/GSX, Workstation oder den VMware Player beschreibe ich am Ende des Kapitels.

Die Folgeversion Virtual PC 2007 unterscheidet sich nur in Details von der Version 2004, mehr Informationen finden Sie im Teil 3, Kapitel 8 – Aktualisierungen, Ergänzungen und Neuerungen.

### Apache oder IIS, Oracle oder SQL

Ziel dieses Workshops ist die Einrichtung eines virtuellen Webserver als Test- und Demo-Umgebung. Dieser Webserver kann abgeschottet auf dem eigenen PC betrieben werden oder für Kunden-Demos öffentlich im LAN zugänglich sein. Auch unterwegs auf dem Laptop ist die eigene Entwicklungsumgebung immer mit dabei.

Linux mit Apache und MySQL kann in der VM genauso laufen wie der IIS unter Windows. Natürlich kann auch ein mobiler Oracle- bzw. SQL-Server realisiert werden oder eine Demo der eigenen Intranet-Lösung. Zum Abschluss erweitern wir die Lösung zu einer kompletten Testumgebung in einem separaten virtuellen Netzwerk. Durch einfaches Klonen erstellter Muster entstehen weitere Maschinen mit verschiedenen Betriebssystemen oder Browserversionen.



Die perfekte Einrichtung und Konfiguration des eigentlichen Webserver in der virtuellen Maschine würde den Umfang des Workshops sprengen. Als Webserver kommt z.B. ein Windows-Gast mit IIS in Frage oder eine Linux-Installation mit Apache – Linux läuft in den VMs von Virtual PC.

Eine komfortable Möglichkeit wäre das Paket XAMPP. Es bietet ohne viel Aufwand einen ApacheServer mit MySQL, Perl und PHP – fix und fertig vorkonfiguriert. Dazu gehört ein komfortables Web-Frontend zur einfachen Bedienung ohne Linux-Know-how. Als dazu passende Betriebssystembasis können Sie den schlanken Linux-Server nach der Anleitung in *Teil 2, Kapitel 4, „Linux-Host mit VMware Server und Integration ins Windows-Netz“* auch in einer VM installieren. Die Kombination aus Linux mit Apache und MySQL ist kompatibel zu den Servern der meisten Hoster und kann gut für die Offline-Entwicklung verwendet werden. XAMPP wird als kostenlose Version für Linux und auch für Windows angeboten:

<http://www.apachefriends.org>

## 2.2 Voraussetzungen für Virtual PC

Der Host-PC sollte eine CPU im GHz-Bereich besitzen und mit mindestens 512 MB RAM bestückt sein, besser mehr. Für jede VM sollten Sie weiterhin, je nach Betriebssystem und installierten Programmen im Gast, mindestens 1–4 GB Plattenplatz einplanen. Als Hostsystem kommt für Microsoft Virtual PC nur Windows in Frage. Offiziellen Support gibt es für Windows 2000 Professionell und XP Professionell. Unter den Server-Versionen, z.B. Windows Server 2003, läuft der Emulator aber trotz Warnmeldung. Weitere Informationen und Grundlagen finden Sie in *Teil 1* des Buches.

Als Gastsystem unterstützt Virtual PC offiziell nur Windows, DOS und OS/2, dennoch läuft Linux unbeeindruckt und stabil in der VM.

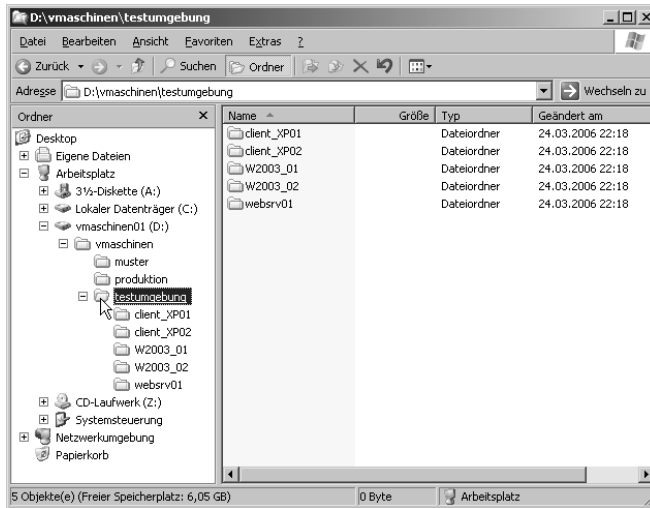
**Linux, OS/2 oder  
Windows**

### 2.2.1 Einrichtung von Virtual PC

Die Installation ist unkompliziert, Näheres dazu und zu weiteren Voraussetzungen finden Sie in *Teil 1, Kapitel 3, „Installation und Konfiguration der einzelnen Produkte“*. Gleich nach der Installation von Virtual PC ist es sinnvoll, für die zukünftigen VMs ein eigenes Verzeichnis *vmaschinen* auf der Festplatte anzulegen. Unterordner wie *testumgebung* und *mustermaschinen* schaffen von Anfang an Überblick in der entstehenden virtuellen Welt (Abbildung 2.1). Ist eine zweite Festplatte im PC eingebaut, sollten Sie die VMs dort ablegen, damit sich deren Plattenzugriffe nicht mit denen des Hostsystems ausbremsen.



Abbildung 2.1:  
Eine sinnvolle  
Ordnerstruktur  
schafft Übersicht in  
der virtuellen Welt



### Standardordner für VMs fest- legen

Damit Sie nicht bei jeder neu zu erstellenden VM oder virtuellen Platte zu Ihrem Ablageordner navigieren müssen, können Sie diesen als Standardverzeichnis für die virtuellen Maschinen einstellen. Das funktioniert etwas umständlich über die Umgebungsvariable `MYVIRTUALMACHINES`, die sich auf dem Host unter `SYSTEMSTEUERUNG/SYSTEM/ERWEITERT/UMGEBUNGSVARIABLEN` als neue Systemvariable festlegen lässt (Abbildung 2.2).

Abbildung 2.2:  
Mit einer Umge-  
bungsvariablen wird  
der Standardordner  
für die VMs fest-  
gelegt



## 2.3 Die erste VM zusammenbauen

Ganz bequem, nur mit wenigen Mausklicks, können Sie jetzt sofort den virtuellen PC für Ihren mobilen Webserver zusammenbauen. Beim ersten Start von Virtual PC erscheint der *Assistent für neue virtuelle Computer* gleich automatisch. Ansonsten können Sie ihn in der Virtual PC-Konsole mit dem Button **NEU** starten.

### 2.3.1 Assistent für neuen virtuellen Computer

Wählen Sie im Assistent bitte nicht den ersten Punkt VIRTUELLEN COMPUTER ERSTELLEN, sondern den zweiten Eintrag STANDARDEINSTELLUNGEN FÜR DAS ERSTELLEN EINES VIRTUELLEN COMPUTERS VERWENDEN (Abbildung 2.3). Auf diesem Weg haben Sie ein wenig mehr Einfluss auf die Konfiguration der virtuellen Platten und liefern sich nicht komplett den Vorgaben des Assistenten aus. Es ist Geschmacksache, aber ich finde diesen Weg übersichtlicher.

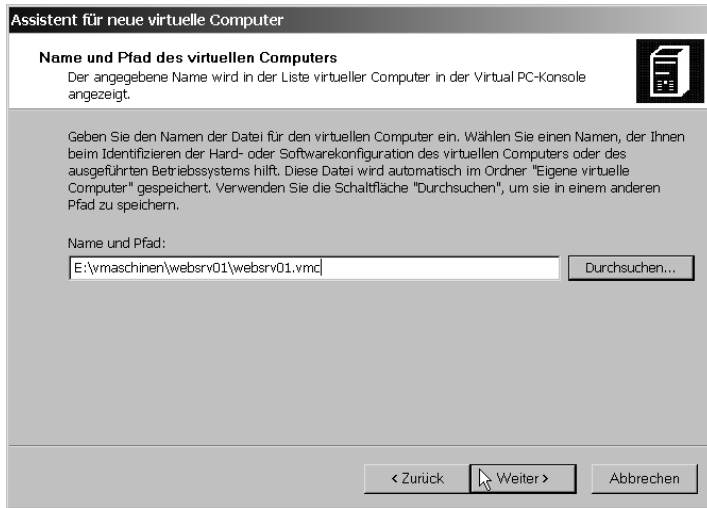


Abbildung 2.3:  
Im Wizard erstellen  
wir vorerst eine VM  
ohne Festplatte

Zuerst fragt der Assistent nach dem Namen und dem Speicherort der neuen Maschine. Mittels DURCHSUCHEN gelangen Sie in Ihren Ordner *vmaschinen*. Wenn Sie ihn bereits per Umgebungsvariable voreingestellt haben, werden neue VMs gleich automatisch dort angelegt, und es genügt, einen Namen in das Feld einzutragen. Im Verzeichnis der VM liegen später alle Dateien zum virtuellen Rechner, z.B. die virtuellen Platten und die Konfiguration. Denken Sie sich für die Ordner und für die Maschinen kurze aussagekräftige Namen aus, um später leichter auf den Inhalt schließen zu können. Als Name des Ordners bietet sich im Beispiel *websrv01* an. Auch die Konfigurationsdatei mit der Endung *\*.vmc* kann gleich so benannt werden, Virtual PC übernimmt automatisch den Namen der VM auch für das Verzeichnis und für die Konfigurationsdatei, wenn Sie nichts anderes festlegen (Abbildung 2.4).

**Ordner  
für die VM**

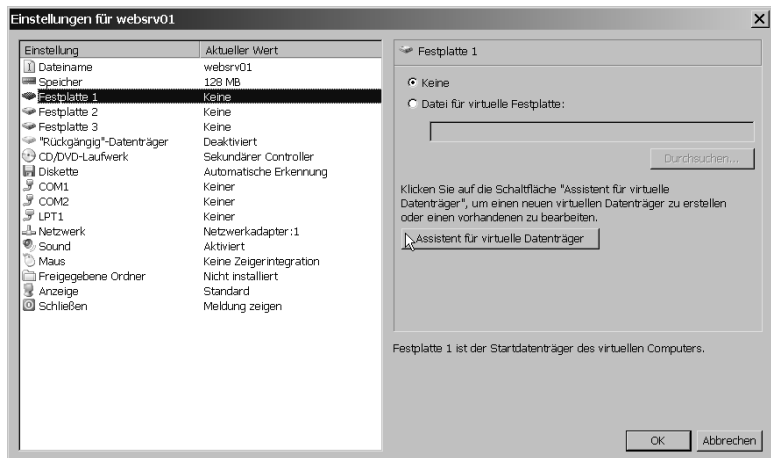
Abbildung 2.4:  
Wählen Sie aussage-  
kräftige Kurznamen  
für Verzeichnisse  
und Konfigurations-  
dateien Ihrer VMs



### 2.3.2 Einstellungen einer VM

Der Assistent erstellt jetzt die neue virtuelle Maschine und wechselt in die Einstellungsübersicht. Hier lässt sich die gesamte Hardware der VM verwalten, vom zugewiesenen RAM bis zu den Netzwerkkarten (Abbildung 2.5). Nachträglich gelangen Sie jederzeit über den Button EINSTELLUNGEN in der Virtual PC-Konsole hierher.

Abbildung 2.5:  
Die Einstellungen  
der VM. Es fehlt  
noch eine virtuelle  
Platte



Links in der Liste lassen sich die zu konfigurierenden Komponenten auswählen. Weitere Hardware integrieren, wie bei VMware, können Sie in der Liste nicht. Das ist auch unnötig, die angebotenen Optionen genügen meist. Was fehlt, sind USB und der direkte Zugriff auf SCSI-Geräte wie einen Streamer. Vorerst interessiert uns nur das fehlende Herzstück der Maschine, die virtuelle Platte. Dort sollen später das Betriebssystem und die Daten des Entwicklungsservers liegen.

### 2.3.3 Die virtuellen Platten einer virtuellen Maschine unter Virtual PC

Virtuelle Platten sind üblicherweise Dateien, die auf der physischen Festplatte des Host-PC angelegt werden. In diese Dateien werden alle Schreib- und Lesezugriffe umgeleitet, wobei das Gastbetriebssystem meint, mit richtiger Hardware zu arbeiten. Die virtuellen Platten können auf dem Host einfach kopiert und in eine andere VM eingebunden werden. Das entspricht dem Umbauen einer echten Festplatte von einem PC in einen anderen. Jeder VM unter Virtual PC können drei virtuelle IDE-Platten zugewiesen werden. SCSI unterstützt nur der große Bruder Virtual Server. Es ist dabei egal, welche echte Hardware im Host steckt. IDE-Platten werden auch emuliert, wenn der Wirt einen SCSI- oder RAID-Controller hat.

Man könnte auch physische Platten direkt einbinden, jedoch darf eine solche Platte nicht von der VM und vom Host gleichzeitig beschrieben werden. Das führt mit Sicherheit zum Daten-GAU. Binden Sie bei Ihren Experimenten deshalb niemals die Systemplatte des Hosts direkt als physische Platte in eine VM ein.



#### Neuen virtuellen Datenträger erstellen

Wählen Sie unter den Einstellungen der VM in der linken Auflistung die *Festplatte 1*. Rechts erscheint dann die Konfigurationsseite zu diesem Eintrag. Ist schon eine Platte vorhanden, kann diese mit DURCHSUCHEN eingebunden werden. Da Sie noch keinen Datenträger erstellt haben, müssen Sie auf den Button ASSISTENT FÜR VIRTUELLE DATENTRÄGER klicken (Abbildung 2.5).

Der Dialog führt über die Option NEUEN VIRTUELLEN DATENTRÄGER ERSTELLEN und danach VIRTUELLE FESTPLATTE direkt zur Frage nach Ort und Namen der Behälterdatei. Mit DURCHSUCHEN navigieren Sie ins Verzeichnis Ihrer neuen VM und legen dort eine Platte mit dem Namen *websrv01\_sys.vhd* an. Auch bei den Datenträgerbezeichnungen zählt sich etwas Ordnung aus. Der Name der VM mit einem Kürzel zum Inhalt der Platte (*sys* für System) hat sich bewährt. Später können weitere Platten für Daten (*data*) oder die Auslagerungsdatei (*swap*) angelegt werden. Die Trennung von System und Daten hat Vorteile, auf die ich weiter unten noch eingehen werden.

**Ordnung beim  
Plattennamen**

Im nächsten Fenster müssen Sie sich für einen Plattentyp entscheiden, vier Optionen stehen dabei zur Verfügung (Abbildung 2.6).

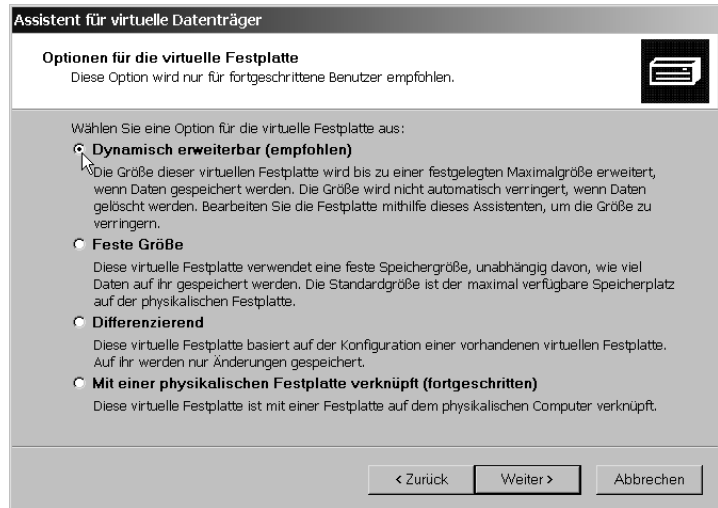
**Plattentypen**

- ▶ *Dynamisch erweiterbar* – Dieser Typ ist für unseren entstehenden Server ideal. Die Platte belegt auf dem Host nur so viel Platz, wie wirklich von Daten verwendet wird, und wächst bei Bedarf mit.
- ▶ *Feste Größe* – Der gesamte Platz wird bereits reserviert. Das kommt etwas der Performance zugute und verhindert das Defragmentie-

ren der Datei der virtuellen Platte auf dem Host, belegt aber auf der physischen Host-Platte meist auch viel unnötigen Platz.

- *Differenzierend* – Auf diesen sehr interessanten Modus werde ich weiter unten noch eingehen. Damit können z.B. mehrere VMs die gleiche Basisinstallation teilen oder mehrere aufeinander aufsetzende Versionsstände erstellt werden, ähnlich den Snapshots von VMware.
- *Mit einer physikalischen Festplatte verknüpft* – Von Versuchen mit diesem Plattentyp rate ich Ihnen vorläufig ab! Sie könnten damit direkt Partitionen echter Festplatten in der VM verwenden.

Abbildung 2.6:  
Vier Arten virtueller  
Platten können Sie  
wählen



Plattengröße und  
Verzeichnis der  
VM

Im nächsten Fenster können Sie bestimmen, wie groß die virtuelle Platte wird. Da Sie eine dynamische Zuwachsplatte verwenden, können Sie großzügig 10 GB bereitstellen. Die Platte wird im Verzeichnis der VM erstellt. Da sie noch keine Daten enthält, belegt die Datei der virtuellen Platte nur einige KB und nicht die kompletten 10 GB. Im Verzeichnis `vmachines\websrv01` existieren jetzt folgende Dateien:

- `websrv01.vmc` ist die Konfigurationsdatei im XML-Format.
- `websrv01_sys.vhd` ist die noch leere virtuelle Festplatte.

### Virtuelle Platte der VM zuweisen

In den Einstellungen der VM können Sie die eben erstellte Platte nun mittels DURCHSUCHEN als Festplatte 1 einbinden. Dazu muss der Punkt an DATEI FÜR VIRTUELLE FESTPLATTE gesetzt sein (Abbildung 2.7).

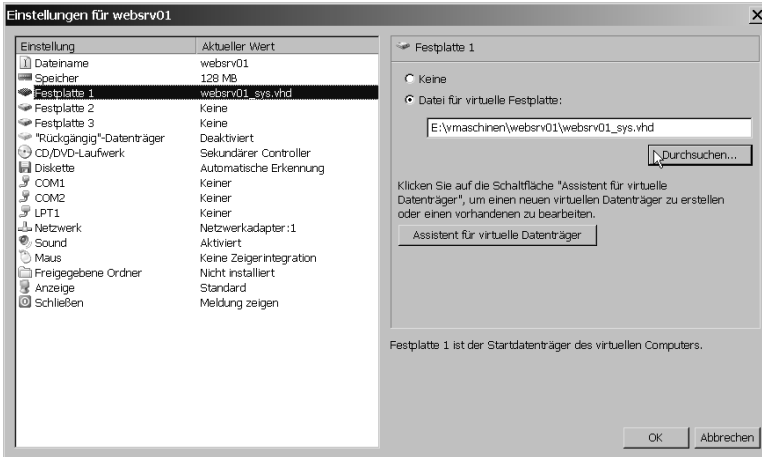


Abbildung 2.7:  
Die VM für den  
Webserver mit  
Festplatte

Wenn der Host mit einer FAT-Partition arbeitet, wird die Platte bei Erreichen der maximalen Dateigröße von 2 GB bzw. 4 GB automatisch in mehrere Einzeldateien aufgeteilt. Auf einer NTFS-Partition entsteht dagegen eine einzige Datei bis zur zugewiesenen Maximalgröße. Umfassende Informationen zu virtuellen und physischen Platten finden Sie in einem eigenen Workshop in Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“.



### 2.3.4 Der Zusammenbau der virtuellen Maschine auf einen Blick

Fertig! Ohne Wollmausattacken unter dunklen Schreibtischen haben Sie ganz bequem Ihren ersten virtuellen PC zusammengeschraubt. Alle Schritte zum schnellen Nachvollziehen hier nochmals auf einen Blick.

#### 1. Neue VM erstellen:

Assistent starten: NEU

Auswahl der Konfigurationsart: *Standardeinstellungen für das Erstellen eines virtuellen Computers verwenden*

Name und Speicherort: *webserv*

#### 2. Virtuelle Platte erstellen:

Einstellungen der VM aufrufen: EINSTELLUNGEN

Eintrag wählen: FESTPLATTE1

Button: ASSISTENT FÜR VIRTUELLE DATENTRÄGER

Auswahl: *neuen virtuellen Datenträger erstellen*

Auswahl: *virtuelle Festplatte*

Name und Pfad: *... \webserv \webserv\_sys.vhd*

Typ: *Dynamisch erweiterbar*

Größe: *10000 MB*

3. Virtuelle Platte einbinden:

Einstellungen der VM aufrufen: EINSTELLUNGEN

Eintrag wählen: FESTPLATTE1

Punkt an: *Datei für virtuelle Festplatte*

Durchsuchen: *websrv\_sys.vhd*

## 2.4 Die Virtual PC-Konsole

**Minimiert in der Taskleiste**

Die Virtual PC-Konsole bietet einen Überblick über alle vorhandenen VMs (Abbildung 2.8). Ist die Konsole minimiert, finden Sie unten rechts in der Taskleiste ein kleines Symbol, über das mit der rechten Maustaste die wichtigsten Funktionen ebenfalls erreicht werden können.

Abbildung 2.8:  
Die kleine Konsole  
ist die Schaltzentrale  
von Virtual PC



Im linken Teil der Konsole erscheint unsere neu entstandene Maschine als Miniatur, in der man später sogar den aktuellen Bildschirminhalt als kleine Vorschau sieht. Rechts daneben befinden sich vier selbst-erklärende Buttons.

- ▶ Mit NEU können Sie weitere VMs erstellen.
- ▶ ENTFERNEN löscht die VM aus der Liste. ENTFERNEN bedeutet dabei nicht von der Festplatte löschen. Die VM kann später jederzeit wieder aufgenommen werden mit NEU/VORHANDENEN VIRTUELLEN COMPUTER HINZUFÜGEN.
- ▶ STARTEN, bzw. SCHLIESSEN startet oder beendet den entsprechenden Gast.
- ▶ Der Button EINSTELLUNGEN bringt Sie zur Konfiguration der VM.



Sollten Sie sich einmal wundern, dass der Button EINSTELLUNGEN ausgegraut ist, dann haben Sie das Einstellungsfenster der VM schon geöffnet. Leider erscheint es nicht in der Taskleiste und verschwindet bei der Arbeit schnell hinter anderen Fenstern. Selbst wenn Sie die Virtual PC-Konsole wieder in den Vordergrund holen, bleiben die Einstellungen verdeckt, bis Sie alle Vordergrundfenster minimieren.

## 2.5 Installation des Betriebssystems in der VM

Den neu zusammengebauten Webserver können Sie schon mit dem Button STARTEN einschalten. Allerdings ist die virtuelle Platte noch leer, weshalb die startende VM nur einen fehlenden Boot-Datenträger reklamiert. Wie auf einem echten PC muss auch hier erst ein Betriebssystem installiert werden.

Dazu legen Sie einfach die bootfähige Installations-CD in das physikalische Laufwerk des Hosts ein, die VM kann ganz normal darauf zugreifen. Es ist auch möglich, der VM ein ISO-Image als eingelegte CD zu präsentieren. Einstellen können Sie die Art der CD nach dem Start der VM über das Menü CD im Fenster der Maschine. Die hier getroffene Zuordnung bleibt auch nach dem Abschalten der VM erhalten (Abbildung 2.9). Nach erfolgter Auswahl der CD können Sie die VM neu booten, und die Setup-Routine des Betriebssystems sollte starten.

**ISO-Image  
verwenden**



Abbildung 2.9:  
Sie können einfach  
von einer virtuellen  
CD booten

Sind bereits Partitionen auf der virtuellen Platte von vorhergehenden Versuchen vorhanden, so kann es sein, dass die VM versucht, von der Platte zu booten und die CD ignoriert. Im virtuellen CMOS-Setup der VM müssen Sie erst die Boot-Reihenfolge ändern (Abbildung 2.10). Sie gelangen ins virtuelle CMOS gleich zu Beginn des Startvorganges mit der Taste **Entf**.





Abbildung 2.10:  
Mit der Taste  
[Entf] gelangen  
Sie ins emulierte  
CMOS-Setup, in  
dem Sie die Boot-  
reihenfolge ändern  
können



## 2.5.1 Das Wichtigste zur Bedienung der VM

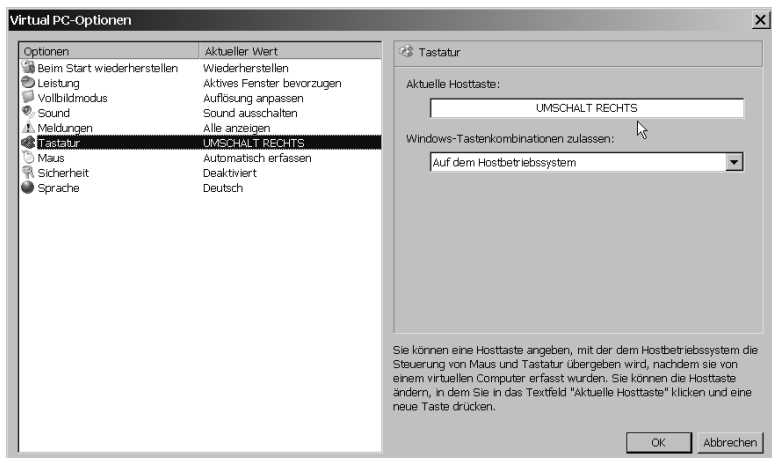
Während die Betriebssysteminstallation läuft, können Sie sich kurz mit ein paar wichtigen Grundlagen zur Bedienung der VM vertraut machen.

### Tastatur und Maus im Gastsystem verwenden

#### Fokuswechsel und Host-Key

Um in der VM die Maus verwenden zu können, muss das Fenster vorher eventuell einmal angeklickt werden. Je nach den Einstellungen in der Konsole unter DATEI/OPTIONEN/MAUS bekommt die VM den Fokus automatisch oder erst durch einen Klick. Mit der rechten Umschalttaste  erhält das Host-System den Fokus zurück. Dieser so genannte Host-Key kann in der Virtual PC-Konsole unter DATEI/OPTIONEN/TASTATUR geändert werden (Abbildung 2.11).

Abbildung 2.11:  
Unter Datei/Optio-  
nen kann z.B. der  
Host-Key angepasst  
werden



Wenn Sie in der VM einen Großbuchstaben oder den Doppelpunkt benötigen, verwenden Sie nicht die rechte Umschalttaste. Damit verlassen Sie die VM. Wenn Sie dieses Verhalten stört, wählen Sie einfach einen anderen Host-Key.



Als weitere Eigenheit wirkt der Griff zu **Strg** + **Alt** + **Entf**, z.B. beim Anmeldebildschirm, immer auf den Host selbst. In einer VM dient als Ersatz dafür die Host-Key-Kombination **→** + **Entf**. Alternativ dazu kann **Strg** + **Alt** + **Entf** auch über das Menü AKTION an die VM gesendet werden (Abbildung 2.12).

**Strg** + **Alt** + **Entf**

## Ausschalten, Suspend, Anhalten

Eine laufende VM können Sie beenden, indem Sie einfach das Fenster schließen. Dabei fragt Virtual PC, ob es die Maschine hart ausschalten soll oder ob der Zustand und RAM-Inhalt gesichert werden (siehe auch Abschnitt 2.6.1, „Rückgängig-Datenträger verwenden“, und Abbildung 2.16). Das Sichern des Zustandes entspricht dem Suspend-Modus eines Laptops, die VM kann später an genau dieser Stelle sehr schnell ohne Booten wieder zum Leben erweckt werden. Dazu wird der Inhalt des Arbeitsspeichers gesichert. Beim erneuten Starten wird der Inhalt wieder zurück in den Arbeitsspeicher geschrieben, so dass die virtuelle Maschine in den gleichen Status versetzt wird wie vor dem Pausieren. Dadurch können Sie sich mit Ihren Gästen den langen Bootvorgang sparen.



Abbildung 2.12:  
Im Menü Aktion  
können Sie die VM  
steuern

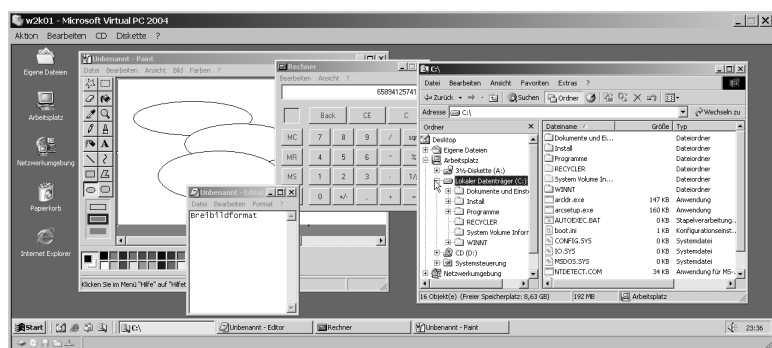
Im Menü AKTION finden Sie weitere Optionen zur Steuerung (Abbildung 2.12).

- ▶ STRG + ALT + ENTF sendet Strg + Alt + Entf an die VM.
- ▶ ANHALTEN friert die VM sofort ein und gibt damit alle Ressourcen für andere Programme auf dem Host frei. Dabei werden aber keinerlei Einstellungen, etwa der RAM-Inhalt, gesichert. Die VM bekommt nur keinerlei CPU-Zeit mehr zugeteilt und verharrt in ihrem letzten Zustand. Nach dem Freigeben arbeitet der Gast sofort an genau der gleichen Stelle weiter.
- ▶ ZURÜCKSETZEN entspricht der Reset-Taste eines physischen PCs.
- ▶ SCHLIESSEN beendet die VM genauso wie das Schließen des Fensters.
- ▶ VOLLBILDMODUS maximiert die VM auf den gesamten Bildschirm. Der Bildschirm des Wirts ist nicht mehr sichtbar. Für den davor Sitzenden wirkt das, als würde der Gast direkt ohne Wirt auf dem PC laufen.

### 2.5.2 Virtual Machine Additions im Gast installieren

Die Setup-Routine von der Installations-CD dürfte inzwischen die Systemdateien klaglos auf die virtuelle Festplatte kopiert haben wie auf einen echten Datenträger. Genauso wird die emulierte Hardware vom Betriebssystem erkannt und verwendet. Nach erfolgter Installation des Betriebssystems sollten als Erstes die *Virtual Machine Additions* in der neuen Maschine eingerichtet werden. Die Additions bringen einige spezielle Treiber für Maus, VGA sowie Controller mit und ermöglichen unter anderem den nahtlosen Fokuswechsel von der VM zum Host auch ohne Lösen der Maus mit dem Host-Key. Weiterhin sorgen die Tools für stufenlose skalierbare Bildschirmauflösungen beim Ändern der Fenstergröße der VM (Abbildung 2.13).

*Abbildung 2.13:  
Durch die stufen-  
lose Skalierung der  
Additions wird  
sogar emuliertes  
Breitbildformat  
möglich*



Drag&Drop zwischen Host und VMs sowie Shared Folders zum Datenaustausch werden von den Additions ebenfalls eingerichtet, und das automatische Herunterfahren des Betriebssystems in der VM wird beim Schließen des Fensters als zusätzliche Option angeboten

(siehe auch Abbildung 2.16). Die Installation der Additions erreichen Sie über den Menüpunkt AKTION/VIRTUAL MACHINE ADDITIONS INSTALLIEREN. In den meisten Gästen erfolgt die Einrichtung dann automatisch (Abbildung 2.14).

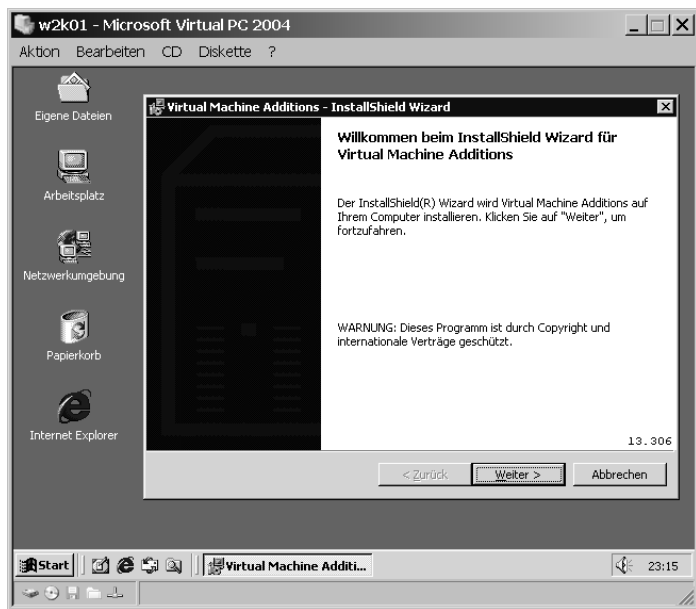


Abbildung 2.14:  
Die Installation der  
Additions startet  
mittels CD-Autorun  
in den VMs automa-  
tisch

Sollte im Betriebssystem der VM CD-Autorun abgeschaltet sein, dann startet die Installation nicht automatisch. Das Setup der Additions befindet sich auf einem ISO-Image, das automatisch zugewiesen wird. In der VM können Sie die *Setup.exe* auch einfach direkt von der emulierten CD starten. Weitere Hinweise zu den Funktionen der Additions finden Sie in *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*.



## 2.6 Zustände des Gastes sichern und Änderungen rückgängig machen

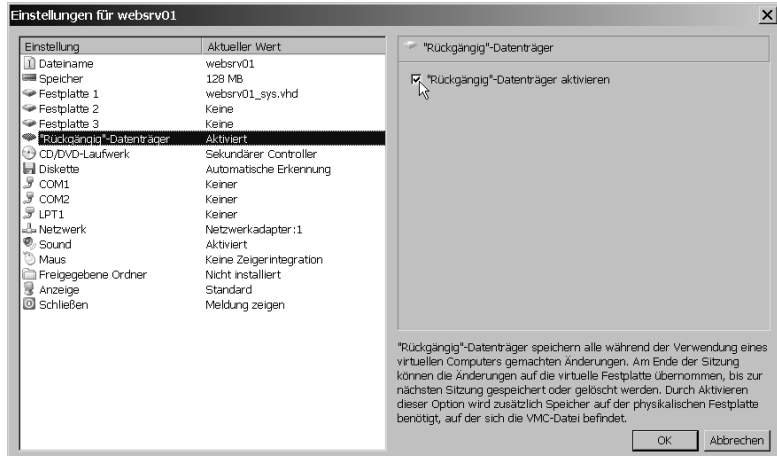
In unserer Maschine fehlen nach der Grundinstallation des Betriebssystems jetzt noch alle notwendigen Service-Packs und Patches sowie die benötigte Software wie Webserver und Datenbanken. Bevor allerdings am frischen System Hand angelegt wird, wäre es schön, wenn man dessen sauberen Zustand sichern könnte. Sollte bei der weiteren Arbeit etwas schief gehen, muss dann nicht alles neu installiert werden. Unter Virtual PC stehen zur Sicherung von Wiederanlaufpunkten zwei Möglichkeiten zur Verfügung.

**Wiederanlauf-  
punkte**

### 2.6.1 Rückgängig-Datenträger verwenden

In den Einstellungen jeder VM gibt es einen Listeneintrag RÜCKGÄNGIG-DATENTRÄGER, den Sie auf der rechten Seite mit einem Haken an RÜCKGÄNGIG-DATENTRÄGER AKTIVIEREN einschalten können (Abbildung 2.15). Das funktioniert nur, wenn die VM ausgeschaltet ist.

Abbildung 2.15:  
Bei aktiviertem Rück-  
gängig-Datenträger  
werden Schreib-  
zugriffe in Undo-  
Logs umgeleitet



**Undo-Logs** Ab jetzt werden alle Schreibzugriffe auf die virtuellen Platten nicht mehr direkt in die Datei der virtuellen Platte geschrieben, sondern in so genannte Undo-Logs gepuffert. Für jede virtuelle Festplatte der VM entsteht automatisch ein solches Undo-Log mit der Endung \*.vud im Ordner des Gastes. Das ermöglicht später jederzeit, diese Änderungen durch einfaches Löschen der Logs zu verwerfen. Die Inhalte der Logs können aber auch irgendwann auf die virtuelle Platte übertragen werden. Damit sind die Änderungen endgültig festgeschrieben und können nicht mehr verworfen werden. Virtual PC beginnt dann wieder mit leeren Undo-Logs für die darauf folgenden Schreibzugriffe.

#### Optionen beim Ausschalten einer VM mit Rückgängig-Datenträger

Änderungen  
verwerfen oder  
aufheben

Die Entscheidung, ob die Logs mit den Änderungen verworfen, festgeschrieben oder erst einmal weiter fortgeführt werden, trifft man beim Beenden der virtuellen Maschine, wobei mehrere Möglichkeiten zur Auswahl stehen (Abbildung 2.16).

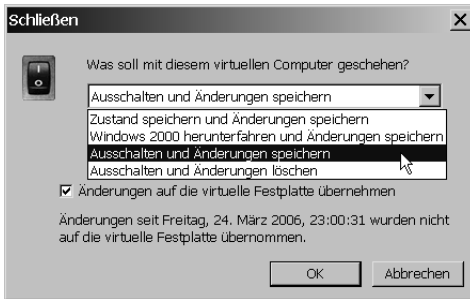


Abbildung 2.16:  
Mit aktiven Rück-  
gängig-Daten-  
trägern können Sie  
beim Abschalten  
entscheiden, was  
mit den Änderun-  
gen geschieht

- ▶ *Zustand speichern und Änderungen speichern* – Diese Option bedeutet, die VM wird nicht abgeschaltet, sondern in den Suspend-Modus versetzt (Zustand speichern), und die Änderungen im Undo-Log bleiben erhalten (Änderungen speichern). Die Änderungen werden aber noch nicht festgeschrieben, sondern bleiben bis auf weiteres in den Undo-Logs. Sie können später immer noch verworfen werden. Beim erneuten Start werden die Undo-Logs einfach weitergeführt.
- ▶ *Ausschalten und Änderungen speichern* – Das ist das Gleiche wie oben, nur dass die VM hart abgeschaltet und nicht in den Suspend-Modus versetzt wird. Änderungen werden in den Undo-Logs aufgehoben und nicht verworfen.
- ▶ *Ausschalten und Änderungen löschen* – Die VM wird hart abgeschaltet, und die Änderungen in den Undo-Logs werden verworfen. Nach dem erneuten Einschalten beginnt die VM mit leeren Logs.
- ▶ *Betriebssystem herunterfahren und Änderungen speichern* – Diese Option existiert nur bei installierten Virtual Machine Additions. Das Betriebssystem in der VM wird vor dem harten Abschalten automatisch heruntergefahren. Die Änderungen in den Undo-Logs werden aufgehoben.

Es noch einen Optionshaken, den Sie bei diesen Aktionen unbedingt im Auge behalten sollten: **ÄNDERUNGEN AUF DIE VIRTUELLE FESTPLATTE ÜBERNEHMEN** (Abbildung 2.16). Sind Sie an dieser Stelle unaufmerksam, werden Sie Änderungen nicht mehr los, die Sie später eigentlich wieder verwerfen wollten. Virtual PC merkt sich immer den letzten gewählten Zustand des Hakens.

**Änderungen  
endgültig über-  
nehmen**

- ▶ *Haken nicht gesetzt* – Ist dieser Haken NICHT gesetzt, passiert auch nichts. Die Änderungen bleiben einfach in den Logs stehen oder werden verworfen, je nach der oben ausgewählten Option.
- ▶ *Haken gesetzt* – Bei gesetztem Haken werden die Änderungen aus den Logs unumkehrbar auf die virtuelle Platte geschrieben und können nicht mehr verworfen werden. Während dieses Vorganges erscheint unten in der Statusleiste die Meldung *Laufwerke werden zusammengeführt*.



Kombinieren Sie die Auswahl *Zustand speichern und Änderungen speichern* mit diesem gesetzten Haken, können erfolgreiche Änderungen zwischendurch auf die Platte übertragen werden, ohne die VM komplett neu booten zu müssen. Nach dem Erwachen aus dem Suspend-Modus stehen leere Undo-Logs für den nächsten Test bereit.

### Auswahl beim Ausschalten automatisieren

Sie können die verfügbaren Optionen beim Abschalten einschränken oder sich auf eine automatisch auszuführende Option festlegen. Die Einstellmöglichkeiten finden Sie unter **EINSTELLUNGEN** ganz unten beim Listeneintrag **SCHLIESSEN**. Das macht die Sache etwas übersichtlicher, birgt aber auch die Gefahr, beim Abschalten der VM ungewollt genau das Falsche mit den vorhandenen Änderungen zu tun.

### Probleme und Nachteile von Rückgängig-Datenträgern

**Es kann nur einen geben**

Der große Nachteil an der Verwendung von Rückgängig-Datenträgern ist die Tatsache, dass damit nicht mehrere Zustände oder Wiederanlaufpunkte gesichert werden können. Entweder man verwirft das Undo-Log oder schreibt es fest. Will man später Änderungen doch noch loswerden, ist das nicht möglich. Schreibt man Änderungen jedoch zu spät fest, kann es passieren, dass eine fehlschlagende Installation die gesamten aufgelaufenen Änderungen kompromittiert.

Außerdem lassen sich Änderungen sehr leicht ungewollt verwerfen oder festschreiben, wenn man nicht sehr gut aufpasst. Zu guter Letzt ist es nicht ohne weiteres möglich, verschiedene Platten, z.B. Daten und System, unterschiedlich zu behandeln. Entweder es wird alles verworfen oder nichts.

## 2.6.2 Differenzierende Platten für die Sicherung des Zustandes und schnelles Klonen

Bei den Nachteilen der Rückgängig-Datenträger setzen die Differenzplatten an. Eine Differenzplatte kann im *Assistent für virtuelle Datenträger* erstellt werden. Differenzplatten können Sie für zwei Einsatzarten verwenden.

### Mehrere Wiederanlaufpunkte mit Differenzplatten erzeugen

**Undo-Logs als eigenständige Platten**

Eine Differenzplatte ist mit einer vorhandenen virtuellen Platte verknüpft. Alle Änderungen werden nur in die Differenzplatte geschrieben, die Basisplatte bleibt unberührt. Lesevorgänge kombinieren den Inhalt beider Platten. Eigentlich ist das die gleiche Funktion wie bei den Undo-Logs der *Rückgängig-Datenträger*. Der Unterschied ist, dass eine Differenzplatte als eigenständige Platte auftritt und der VM als

normaler Datenträger zugewiesen werden muss. Ein einfaches Verwerfen von Änderungen beim Abschalten ist damit nicht möglich, dazu müssen Sie erst wieder eine neue leere Differenzplatte erstellen und einbinden.

Da eine Differenzplatte als normaler Datenträger gilt, kann sie zusätzlich über die Option *Rückgängig-Datenträger* mit einem Undo-Log betrieben werden.



### **Kaskadierung**

Als Besonderheit kann eine erstellte Differenzplatte wieder als Basis für eine weitere Differenzplatte dienen. So können Sie eine Kette von Platten aufbauen, wobei jede jeweils den Änderungsfortschritt eines bestimmten Zeitraumes enthält. Bei Lesezugriffen werden alle Platten der Kette kombiniert, Schreibzugriffe landen nur in der jeweils letzten Differenzplatte.

### **Linked Clones mit Differenzplatten erstellen**

Außerdem können mehrere separate Differenzplatten parallel auf die gleiche Basisplatte aufsetzen, da die Basisplatte ja nur gelesen wird. So kann eine einzige Grundinstallation unabhängig von vielen anderen VMs verwendet werden. Es entsteht eine Art verlinkter Klon. Das spart viel Platz und Zeit beim Vervielfältigen gleicher Betriebssysteme.

Ist die zugrunde liegende virtuelle Platte einer Differenzplatte kaputt oder wurde diese verändert, dann funktionieren alle aufsetzenden Differenzplatten nicht mehr. Versehen Sie die Datei der zugrunde liegenden Platte am besten mit einem Schreibschutz.



### **Differenzplatten und Änderungen zusammenführen**

Die Änderungen in den Differenzplatten können jederzeit mit der Basisplatte oder mit zugrunde liegenden anderen Differenzplatten zusammengeführt werden. Damit lassen sich die verschiedenen gespeicherten Zustände wieder verdichten und erfolgreiche Änderungen endgültig übernehmen. Das Zusammenführen geschieht im *Assistent für virtuelle Datenträger* mit der Option *VORHANDENEN VIRTUELLEN DATENTRÄGER BEARBEITEN*.

### **Verdichten und auf Basisplatte übernehmen**

Eine praktische Anleitung zum Erstellen von Klonen und Wiederanlaufpunkten mit Differenzplatten finde Sie in *Teil 2, Kapitel 7, „Eine virtuelle Pilotumgebung als Testfeld für produktive Einsätze“*.

Mehr Informationen zu virtuellen Platten und dem Aufbau der Undo-Logs finden Sie im ausführlichen Platten-Workshop in *Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“*.



### 2.6.3 Datenplatten vor versehentlichem Verwerfen schützen

**Datenverlust** Bei einem Löschen der Undo-Logs ist nicht immer der Verlust aller Änderungen wünschenswert. Hat man versehentlich das System zerschossen und will diese Modifikationen wieder verwerfen, dann sind dadurch natürlich auch alle Daten betroffen. Bei unserem Webserver sind das die neu entwickelten Seiten und Applikationen. Wenn Sie bestimmte virtuelle Platten vor Datenverlust schützen wollen, so können Sie nur mit Differenzdatenträgern arbeiten und müssen auf die Undo-Logs der rückgängig-Datenträger verzichten. Sie können dann bei Bedarf die Differenzplatte der Systemdisk manuell löschen, die Datendisk aber unangetastet lassen. Vor allem ist so ein versehentliches Verwerfen unmöglich.

**System und Daten trennen** Das ist ein guter Grund, System und Daten zu trennen. Dadurch lässt sich die zerschossene Systemplatte des Webserver mit ein paar Mausklicks reparieren, ohne dabei Änderungen an den Projekten auf der Datenplatte zu verlieren.



Notfalls können Sie auch nur die Undo-Logs einer bestimmten virtuellen Platte manuell löschen. Sie können das im Windows-Explorer bei ausgeschalteter VM tun. Nach dem Neustart beginnt die VM für diese Platte mit neuen leeren Logs.

## 2.7 Klonen von fertig installierten virtuellen Maschinen

Wenn wir gerade bei den Platten sind, lohnt sich ein kleiner Ausflug zum Thema Klonen von virtuellen Maschinen. Benötigen Sie mehrere VMs in einer Testumgebung mit dem gleichen Betriebssystem, dann ist es unpraktisch, jede VM immer wieder neu zu installieren. Es gibt zwei wesentlich komfortablere Möglichkeiten, die ich im Folgenden beschreibe.

### 2.7.1 Ordner einer VM oder nur die virtuellen Platten kopieren

Schon durch eine einfache Kopie des gesamten Ordners einer fertigen VM oder nur der virtuellen Platte mit der Betriebssysteminstallation, können Sie einen kompletten Klon erstellen. So entsteht ohne viel Aufwand z.B. eine Farm aus unterschiedlichen Browser- oder Clientversionen zum Testen. Jede Kopie ist ein komplettes Abbild. In jeder VM muss jetzt nur noch eine andere Browserversion installiert werden. Auch hier ist eine Trennung von System und Daten nützlich, so muss nur die Systemplatte kopiert werden, ohne Datenballast mitzuschleppen.

### 2.7.2 Klonen von virtuellen Systemen mit differenzierenden virtuellen Festplatten

Für eine schnell benötigte, nur temporär verwendete Testumgebung nimmt das Kopieren der virtuellen Platten aber recht viel Zeit und auch Platz in Anspruch. Hier ist eine *Differenzierende virtuelle Festplatte*, kurz *Differenzplatte*, die bessere Lösung.

Zuerst wird eine Basis-VM fertig installiert und eingerichtet. Meistens existiert schon eine VM mit dem benötigten Betriebssystem. Auf die Systemplatte dieser VM werden mehrere Differenzplatten aufgesetzt, die wiederum in unterschiedliche VMs eingebaut werden können. Nur die Änderungen jeder VM liegen in den Differenzplatten, die Basisplatte mit der Grundinstallation wird nur ein einziges Mal benötigt. Auch hier können Sie in allen geklonten VMs völlig unabhängig voneinander unterschiedliche Browser, Service-Packs oder Programme installieren.

**Platz und Zeit sparen**

### 2.7.3 Einbinden der geklonten Platten und Nacharbeit am Klon

Eine komplett kopierte VM können Sie in der Virtual PC-Konsole über NEU/VORHANDENEN VIRTUELLEN COMPUTER HINZUFÜGEN aufnehmen. Bei einer kompletten Kopie der VM müssen Sie der Konfigurationsdatei \*.vmc vorher einen neuen Namen geben. Eine kopierte virtuelle Platte oder einen Differenzdatenträger können Sie dagegen einfach in eine neu erstellte VM einbinden.

Für jeden Klon ist eine eindeutige IP-Adresse, ein Rechnername und gegebenenfalls eine SSID zu sorgen. Und natürlich benötigt man für alle laufenden virtuellen Maschinen auch Lizenzen der darin gestarteten Betriebssysteme, wenn diese nicht freie Software sind.

**IP, Name und SSID**

## 2.8 Kommunikation und Datenaustausch der Gäste mit dem LAN und dem Host

Nachdem Sie nun Ihren erreichten Installationsstand mit einer Differenzplatte oder einem Undo-Log gesichert haben, können Sie sorgenfrei die weitere Installation und Konfiguration des Webservers beginnen. An dieser Stelle taucht die Frage auf, wie man Dateien mit der VM austauschen kann bzw. wie die VM ins Internet kommt, um sich dort Patches und Installationspakete abzuholen.

### 2.8.1 ISO-Images für häufig verwendete CDs

Von häufig verwendeten CDs oder Programminstallationem lassen sich ISO-Images erstellen und in das virtuelle CD-ROM-Laufwerk einlegen. Dies ist die simpelste Art des Datenaustausches. Sie können sich z.B. eine Sammlung aller CDs virtuell an einem zentralen Punkt im Netz ablegen. Tools zum Erstellen von ISO-Images finden Sie in *Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“*.

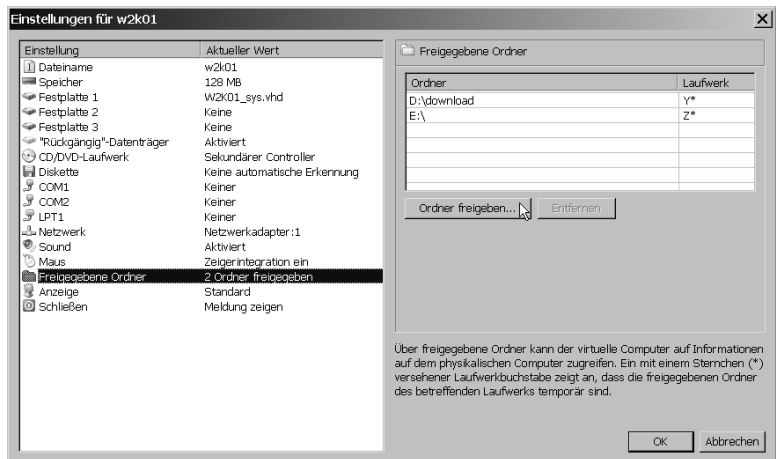
### 2.8.2 Drag&Drop oder freigegebene Ordner zum einfachen Datenaustausch

Die einfachste Methode zum Datenaustausch ist Drag&Drop, man zieht Dateien einfach vom Host in die VM und umgekehrt oder arbeitet mit der Zwischenablage. Für den Zugriff auf komplette Ordner der Hostplatte bieten sich so genannte *Freigegebene Ordner* an. Diese lassen sich über EINSTELLUNGEN/FREIGELEGEBENE ORDNER einstellen (Abbildung 2.17). Die so freigegebenen Ordner des Hosts sind in der VM dann als Laufwerke sichtbar.



Freigegebene Ordner und Drag&Drop stehen nur bei installierten *Virtual Machine Additions* zur Verfügung.

Abbildung 2.17:  
Ordner auf dem  
Host lassen sich  
direkt an die Gäste  
durchreichen



### 2.8.3 Netzwerk zur Kommunikation der Gäste mit dem LAN oder Internet

#### Virtuelle Netzwerkkarten

Der flexibelste Weg zur Kommunikation ist die Nutzung der Netzwerkunterstützung von Virtual PC. In jede Maschine können bis zu vier virtuelle Netzwerkkarten eingebaut werden. Sie erscheinen innerhalb der VM als *Intel Ethernet Adapter*, für den fast jedes Betriebssystem Treiber mitbringt. Diese Adapter können ihre IP mittels

DHCP erhalten oder manuell konfiguriert werden. Das Betriebssystem „denkt“, mit einem echten Adapter zu arbeiten.

Die Konfiguration finden Sie in der Virtual PC-Konsole unter EINSTELLUNGEN zu jeder Netzwerkkarte. Es existieren vier Konfigurationsarten virtueller Adapter, und der Typ entscheidet darüber, wie die VM mit dem LAN oder dem Internet kommunizieren kann (Abbildung 2.18).

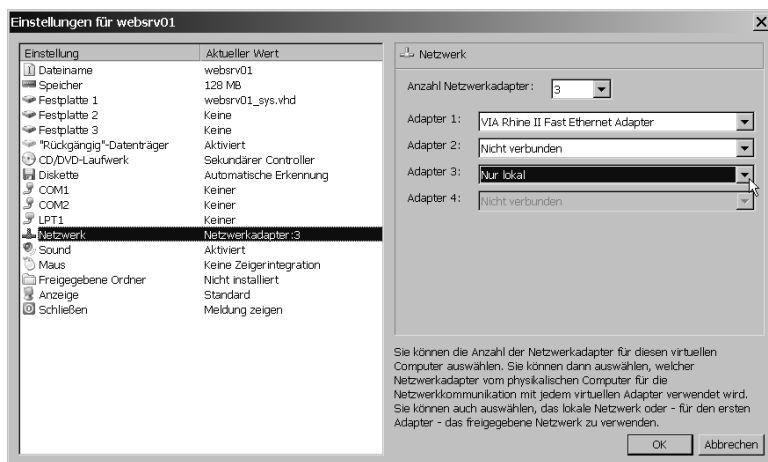


Abbildung 2.18:  
Bis zu vier virtuelle  
Netzwerkkarten mit  
unterschiedlichen  
Anschlüssen stehen  
zur Verfügung

### Nicht verbunden

Die Einstellung *Nicht verbunden* wirkt, als wäre das Kabel von der virtuellen Netzwerkkarte abgezogen worden. Es ist keinerlei Datenverkehr von der VM möglich, obwohl der virtuelle Adapter in der VM weiterhin vorhanden ist. Unser Webserver bleibt isoliert.

### Nur lokal

Alle VMs mit dem Adaptertyp *nur lokal* können nur intern miteinander kommunizieren, ohne jeden Kontakt zur Außenwelt. Unser virtueller Webserver kann so mit virtuellen Testclients arbeiten, ohne dass der PC oder Laptop einen Netzwerkanschluss benötigt und ohne den Betrieb im Unternehmensnetzwerk zu stören.

### Verbunden mit physischer Netzwerkkarte

Aus einer Liste zu jedem Adapter können Sie einfach eine physische Netzwerkkarte auswählen. Der Gast kommuniziert über diese physische Netz Karte im Host-PC mit dem externen Netzwerk. Die VM hat vollen Zugriff auf das LAN und ist uneingeschränkt zu erreichen. Unser Webserver kann damit im Netzwerk des Kunden für Demo-Zwecke zur Verfügung gestellt werden. Er benötigt dazu natürlich eine freie IP-Adresse aus dem LAN. Webserver und Host erscheinen parallel und unabhängig im Netz.

### Gemeinsames Netzwerk (NAT)

Eine virtuelle Netzwerkkarte vom Typ NAT borgt sich sozusagen die Identität des Host-PC. In allen Paketen wird die Absenderadresse mit der Adresse des Wirts ersetzt. Clients im LAN meinen, der Host selbst sendet die Pakete. Wie bei NAT üblich, ist ein direktes Ansprechen der Maschine vom LAN aus nicht möglich. Der Vorteil ist, dass keine freie IP aus dem LAN benötigt wird. NAT-Adapter sind sinnvoll, um die ISDN-, Modem- oder UMTS-Verbindung des Host-PC zu nutzen oder um im Kunden-LAN unbemerkt zu bleiben. Sehr praktisch ist der virtuelle DHCP-Dienst, der auch gleich die passenden IP-Adressen an die VMs verteilt. Für unseren Webserver ist NAT nicht sinnvoll, da er dann nicht von außen erreichbar ist.

### Host-only mit Microsoft Loopback Adapter

Die Kommunikation vom Host-PC zur VM ist nur über eine Netzwerkkarte auf dem Host möglich. Wenn Sie z.B. im Zug oder im Hotel vom Laptop auf den Webserver in der VM zugreifen wollen, geht das nicht, weil kein Link vorhanden ist und die Netzwerkkarte im Host deaktiviert ist. Hier hilft der *Microsoft Loopback Adapter*, der über SYSTEMSTEUERUNG/HARDWARE/NEUES GERÄT/HINZUFÜGEN als Netzwerkkarte auf dem Host installiert werden kann. Er gehört zum Lieferumfang von Windows. Diesen Netzkartentreiber können Sie wie einen physischen Adapter auf dem Host verwenden und unter Virtual PC auswählen. Er stellt die Verbindung von den Gästen zum Host her. Darauf und auf weitere Details zum Netzwerk gehe ich im ausführlichen Netzwerk-Workshop in Teil 3, Kapitel 2, „*Virtuelle Netzwerke Teil 2 – die ganze Wahrheit*“ ein.

## 2.9 Webserver fertig stellen und weitergeben

Unser Webserver ist fertig und kann als Demo- oder Entwicklungsumgebung verwendet werden. Natürlich müssen Sie noch die Software, wie Apache oder IIS, einrichten. Wenn der Host ans LAN angeschlossen ist und die virtuelle Netzwerkkarte des Webserver mit einer physischen Netzwerkkarte verbunden wurde, sollte ein Ping vom Host zum Webserver schon funktionieren. Verfügt das LAN über keinen DHCP-Server, so muss im Gastbetriebssystem eine freie IP-Adresse aus dem LAN-Bereich fest eingestellt werden.



Wenn Sie sich bei der weiteren Installation im Gast an irgendeiner Stelle unsicher sind, können Sie vorher eine weitere Differenzplatte anlegen, um den Konfigurationsstand zu sichern.

Nachdem der Webserver funktioniert und per HTTP und FTP ansprechbar ist, kann er durch eine einfache Kopie des gesamten Ordners auf jedem beliebigen PC laufen. Damit können Sie ihn an Kollegen weitergeben, an Kunden versenden oder auf dem Laptop und dem Firmen-PC vorhalten. Auch hier macht sich wieder eine Trennung von Datenplatten und System bezahlt, weil Sie dadurch immer die gleiche Systemplatte mit unterschiedlichen Datenplatten verteilen können. So hat der Kunde eine Demo-Umgebung, und Sie arbeiten mit den Entwicklungsdaten.

**VMs weitergeben**

Zum Weitergeben eignet sich sogar die Konkurrenz, der kostenlose VMware Player, der auch VMs von Virtual PC laufen lässt (siehe Teil 2, Kapitel 5, „*Virtuelle Umgebungen mit dem VMware Player weitergeben*“). Dadurch benötigt Ihr Kunde nicht einmal eine Lizenz von Virtual PC.

**Kostenloser  
VMware Player**

## 2.10 Weitere VMs in der Testumgebung erstellen und vernetzen

Sie können problemlos weitere VMs zur Testumgebung hinzufügen, entweder durch Neuinstallation oder durch einfaches Klonen angefertigter Mustervorlagen. So lässt sich ein Browser-Park mit Differenzplatten aufbauen oder ein Archiv verschiedener Clients und Betriebssystemversionen installieren. In einem Testnetzwerk hängen dann alle erstellten VMs am internen Netz *lokal*. So können Sie z.B. mit verschiedenen Browsern auf den virtuellen Webserver zugreifen. Wie viele Gäste Sie parallel laufen lassen können, hängt hauptsächlich vom RAM im Host ab.

**Komplettes  
Testnetz**

Gewöhnen Sie sich an, in jedem Verzeichnis einer VM eine Textdatei *Änderungen.txt* anzulegen, in der Sie genau dokumentieren, was Sie wann an diesem Gast geändert haben, wann Änderungen verworfen wurden und wann Sie eine neue Differenzplatte aufgesetzt haben. Sie verlieren sonst bald den Überblick in Ihrer wachsenden virtuellen Welt.



## 2.11 Umsetzung der Testumgebung mit VMware

Unter VMware werden viele Funktionen anders bezeichnet als bei Microsoft, aber alle sind vorhanden. So kann unser Entwicklungsserver auch ohne weiteres unter VMware laufen. Die wichtigsten Unterschiede finden Sie hier:

- ▶ *Tastatur und Maus* – Die Tastenkombination zum Lösen des Fokus ist unter VMware standardmäßig **[Strg] + [Alt]**. Der Griff **[Strg] + [Alt] + [Entf]** wird durch **[Strg] + [Alt] + [Einf]** ersetzt.
- ▶ *Virtual Machine Additions* – Unter VMware heißen die Virtual Machine Additions *VMware Tools* und bieten ungefähr die gleiche Funktionalität. Die Tools gibt es unter VMware auch für Linux-Gäste.
- ▶ *Rückgängig-Datenträger* – Unter VMware übernehmen die Snapshots die Funktionen zum Sichern der Konfigurationszustände. Vorteil: Es gibt in der Workstation 5 nicht nur einen Snapshot, sondern mehrere in einem sehr komfortablen Snapshot-Manager. Die VMware Server kennen nur einen Snapshot, unter dem Player ist die Funktion stark eingeschränkt.
- ▶ *Differenzplatten* – Mehrere Snapshots und Linked Clones bieten unter VMware Workstation die gleichen Funktionen wie mehrere kaskadierte Differenzplatten unter Virtual PC. VMware bietet einen komfortablen Manager für Snapshots und einen Wizard zur Erstellung von Klonen.

### Netzwerk

Obwohl die Netzwerkfunktionalität unter VMware wesentlich umfangreicher ist, ähneln sich die grundsätzlichen Funktionen:

- ▶ *Verbunden mit physischer Netzwerkkarte* – Unter VMware ist eine Netzwerkkarte im Bridged-Modus mit einer physischen Netzwerkkarte verbunden.
- ▶ *nur lokal* – In VMwares Custom-Modus kann eine Netzwerkkarte an eine freien VMnet-Switch (z.B. VMnet4) angeschlossen werden. Alle Netzwerkadapter an einem freien VMnet hängen an einem internen Netz ohne Kontakt zur Außenwelt. Es gibt unter VMware mehrere interne Netze (VMnet0–VMnet9).
- ▶ *NAT-Modus* – Den NAT-Modus gibt es auch bei VMware. Es existiert zusätzlich die Möglichkeit zum Port-Forwarding. Damit kann unser Webserver trotz NAT auf bestimmten Ports auch von außen erreicht werden.
- ▶ *Microsoft Loopback-Adapter* – Im Modus HostOnly verwendet VMware einen eigenen virtuellen Host-Adapter zur Kommunikation vom Host zur VM, ohne dass eine physische Netzwerkkarte notwendig ist. Die Konfiguration dieses Adapters übernimmt VMware automatisch, ein Microsoft Loopback-Adapter ist nicht notwendig.

# 3 Virtuelle DMZ mit Firewall und Webserver im Internet

In diesem Workshop lernen Sie die Anwendung virtueller Netzwerkkarten und Anschlusstypen an einem praktischen Beispiel kennen. Der Workshop eignet sich als Lernbeispiel oder für den produktiven Einsatz. Zuerst sichern Sie mittels einer Firewall-VM, mit IPCop bzw. ISA Server, den Internet-Zugang für Ihren Host-PC und für ein komplettes LAN ab. Im nächsten Schritt entsteht in einem internen virtuellen Netzwerk eine DMZ (*demilitarisierte Zone*), in der Webserver oder Terminalserver als VMs laufen. Diese Server sind, abgesichert über die Firewall, vom Internet aus erreichbar. Die Anbindung kann als Testumgebung über eine DSL-Flatrate oder produktiv über eine vollwertige Standleitung mit fester IP-Adresse erfolgen. Ohne zusätzliche Hardware und Kabelverlegung betreiben Sie öffentlich zugängliche Server in einer virtuellen DMZ.

**DMZ und sicherer Internet-Zugang**

## Workshop im Überblick

### Hauptprodukt

- ▶ VMware Server, VMware Workstation, VMware Player
- ▶ Umsetzung des Konzeptes auch mit Microsoft Virtual PC/Server

### Praktische Verwendung

- ▶ Für das LAN oder den Host-PC einen sichereren Internet-Zugang über eine Firewall realisieren
- ▶ Den eigenen Webserver per DSL sicher im Internet bereitstellen
- ▶ Für Außendienstler einen Terminalserver betreiben
- ▶ Mailserver oder Outlook Web Access ans Internet anbinden

### Schwerpunkte

- ▶ Virtuelle Netzwerke ausreizen und verstehen
- ▶ Sicherheit virtueller Maschinen und virtueller Netzwerke

### Zielgruppe

- ▶ Firmen und Arbeitsgruppen
- ▶ Ambitionierte Laien und Privatanwender, Netzwerkinteressierte



### 3.1 Praktische Anwendung virtueller Netzwerke

Wenn Sie sich heutzutage im Internet bewegen, sollten Sie an die eigene Sicherheit denken. Schon beim Surfen ohne Firewall tummeln sich schnell ungebetene Gäste auf Ihrem PC. Spätestens wenn Sie eigene Server im Internet bereitstellen, kommen Sie um eine so genannte *demilitarisierte Zone*, kurz *DMZ*, nicht herum. Nur so lässt sich Ihr LAN sicher vor Angriffen schützen, wenn Würmer oder Hacker auf die öffentlichen Server durch Sicherheitslücken Zugriff erlangen sollten.

#### Hardware und Platz sparen

Eine echte DMZ benötigt einiges an Hardware: ein oder zwei Firewall-Geräte, zusätzliche Server, ein separater Hub oder Switch sowie jede Menge Kabel, Platz und Strom. Wie Sie schon ahnen, lässt sich einiges davon sparen, wenn Sie auf virtuelle Maschinen setzen.

Abbildung 3.1:  
Geplanter Aufbau  
der virtuellen DMZ  
im Überblick

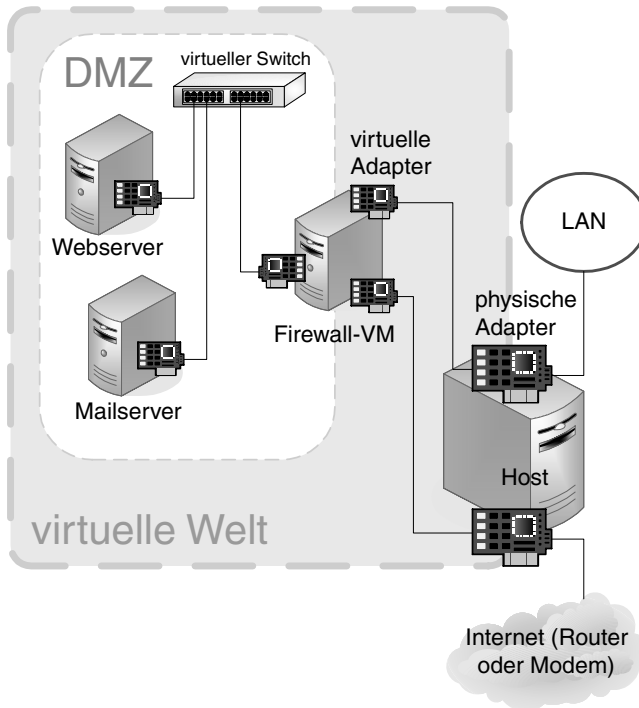


Abbildung 3.1 zeigt den geplanten Aufbau einer virtuellen DMZ. Hinter der Firewall-VM existiert als DMZ ein abgeschottetes virtuelles Netzwerk, in dem die virtuellen Server angeschlossen sind. Die Firewall kontrolliert den Zugang vom LAN ins Internet und vom Internet in die DMZ. Die Kommunikation der virtuellen Firewall mit dem LAN und mit dem Internet erfolgt über physische Netzwerkkarten im Host-Rechner.

### Was ist eine DMZ?

Sinn einer DMZ ist es, einen abgesicherten Bereich zu schaffen, in dem solche Rechner stehen, die direkt vom Internet aus zu erreichen sind. Rechner aus der DMZ haben keinen direkten Zugriff aufs LAN. Dazu hängen sie an einem abgetrennten Netzwerk. Sollte trotz aller Sicherheitsvorkehrungen auf diesen Servern ein Angreifer die Kontrolle erlangen, so befindet sich der Hacker oder der Wurm nur im geschützten Bereich der DMZ und kann im richtigen Firmennetz keinen Schaden anrichten. Vom eigenen LAN aus sind die Server in der DMZ, zwecks Administration und Datenaustausch, dagegen uneingeschränkt erreichbar. Welches Netzwerkpaket wohin darf, entscheidet eine Firewall. Diese trennt Internet, DMZ und LAN voneinander. Pakete werden anhand von Regeln in bestimmte Richtungen weitergeleitet oder blockiert.

Eine DMZ kann mit zwei separaten Firewalls arbeiten, zwischen denen sich das abgesicherte Netzwerk befindet. Als Alternative verfügen viele Firewalls über drei Netzwerkschnittstellen. Die erste ist mit dem LAN verbunden, die zweite stellt die Verbindung zum Internet her. An der dritten lässt sich ein separates Netzwerksegment betreiben, das die DMZ bildet. Wir verwenden im Workshop die Lösung mit nur einer Firewall, ein Ausbau zur zweistufigen DMZ ist aber möglich.

### 3.1.1 Mehrstufiger Ausbau des Workshops vom einfachen Surfschutz bis zur vollwertigen DMZ

Der folgende Workshop beschreibt den mehrstufigen Ausbau einer Firewall in einer virtuellen Maschine. Wir beginnen mit einem einfachen Surfschutz für den Host-PC und steigern uns bis zur kompletten DMZ mit zusätzlichen virtuellen Web- oder Terminalservern. So dürfte jeder Anwender eine passende Lösung für seinen Einsatzbereich finden.

**Einfacher Surfschutz oder DMZ**

Das Beispiel zeigt die ganze Flexibilität virtueller Netzwerke und schöpft alle Konfigurationsmöglichkeiten direkt im praktischen Einsatz aus. Es ist nicht unbedingt ein Einsteiger-Workshop. Wenn Sie noch nie etwas mit virtuellen Netzwerken zu tun hatten und während des Workshops nicht weiterkommen, empfehle ich Ihnen als Vorbereitung die Lektüre *Teil 3, Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“*.

Die Beschreibung arbeitet mit dem VMware Server, der Workshop eignet sich aber genauso für eine Testumgebung unter VMware Workstation, da sämtliche Netzwerkeinstellungen gleich sind. Im VMware Player können Sie die DMZ ebenfalls umsetzen. Zur Netz-

**VMware Player und Microsoft-Produkte**

werkkonfiguration (*Custom-Netzwerk*) sind allerdings einige Kenntnisse aus Teil 2, Kapitel 5, „*Virtuelle Umgebungen mit dem VMware Player weitergeben*“ notwendig. Auch auf die Microsoft-Produkte kann die DMZ problemlos umgesetzt werden, ich gehe am Ende des Kapitels detailliert darauf ein.



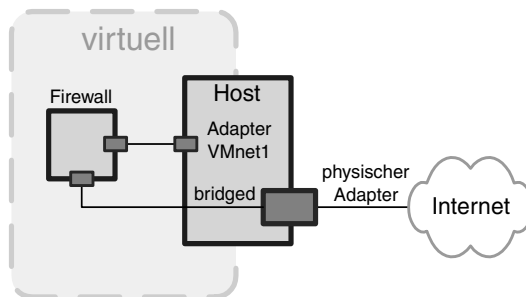
Die im Workshop verwendete Menüeinstellung *HOST/VIRTUAL NETWORK SETTINGS* existiert nicht bei einem Linux-Host. Um die Beschreibung nicht unnötig kompliziert zu machen, beschränke ich mich auf die Windows-Konfiguration. Zusätzliche Hinweise zur Netzwerkkonfiguration unter einem Linux-Host finden Sie in Teil 3, Kapitel 2.

#### Die Ausbaustufen der Firewall und der DMZ

Der Workshop sieht mehrere Ausbaustufen vor, durch die Sie sich Stück für Stück durcharbeiten können:

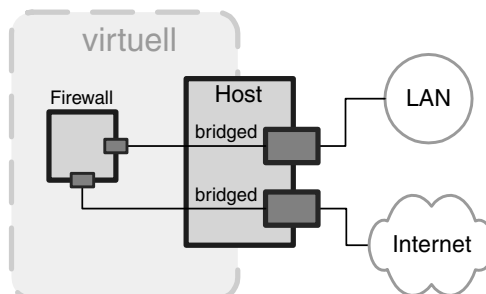
- **Stufe 1:** *einfache Absicherung des Host-PC* – Sie beginnen mit der einfachen Absicherung des Host-PC als Einzelplatz. Die Firewall-VM ermöglicht über eine physische Netzwerkkarte im Host einen sicheren Internet-Zugang mit einem DSL-Modem oder einem Router. Es ist kein LAN angeschlossen, nur der Host hat über die Firewall-VM Internet-Zugriff (Abbildung 3.2).

Abbildung 3.2:  
Ausbaustufe 1 –  
Nur der Host kann  
über einen virtuellen  
Host-Adapter die  
Firewall und das  
Internet erreichen



- **Stufe 2:** *zusätzliche Anbindung eines LAN* – In der Ausbaustufe 2 ist die Firewall-VM auch vom LAN aus zu erreichen. Das ermöglicht den abgesicherten Internet-Zugang für alle Client-PCs und für den Host (Abbildung 3.3).

Abbildung 3.3:  
Ausbaustufe 2 – Der  
Host und das LAN  
können über einen  
physischen Host-  
Adapter die Firewall  
und das Internet  
erreichen



- **Stufe 3:** einen virtuellen Webserver in der DMZ ins Internet bringen – Als Ausbaustufe 3 setzen Sie neben der Firewall eine weitere VM auf, die als Webserver dient. Dieser Server ist in einem virtuellen Netz angeschlossen, welches die DMZ bildet. Er ist vom Internet aus über Port 80 und Port 443 erreichbar (Abbildung 3.4). Die Ausbaustufe 3 lässt sich mit Stufe 1 oder Stufe 2 kombinieren.

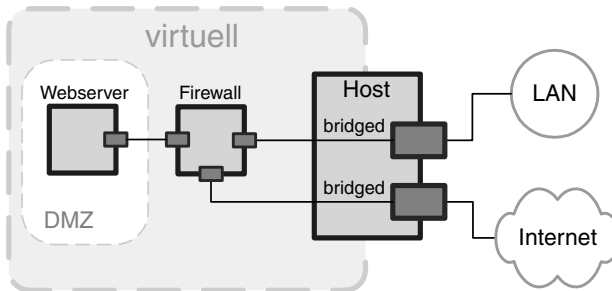


Abbildung 3.4:  
Ein dritter virtueller Adapter in der Firewall-VM bildet den Anschluss der DMZ

- **Stufe 4:** weiterer Ausbau der DMZ – Sie können weitere Server zur DMZ hinzufügen und den gesamten Funktionsumfang der Firewall ausnutzen. So lässt sich z.B. ein SSL-Tunnel oder ein VPN zu einem Remotedesktop oder Terminalserver in der DMZ aufbauen. Das ermöglicht den sicheren Zugriff von jedem Platz der Welt aus über das Internet.

Die einzelnen Stufen gehen teilweise ineinander über oder lassen sich kombinieren. So kann eine DMZ mit einem öffentlich erreichbaren Webserver für Testzwecke auch nur auf dem eigenen Arbeitsplatz-PC mit *Ausbaustufe 1* laufen, ohne dass eine zusätzliche LAN-Anbindung erfolgt.

**Mit oder ohne LAN**

## 3.2 Anforderungen an den Host-PC

Als Host-PC, auf dem die virtuellen Maschinen laufen, genügt in den einfachen Ausbaustufen der eigene Arbeitsplatzrechner. Die VM kann als Firewall für den Internet-Zugang des Host-PC dienen, und Sie verwenden die DMZ zum Experimentieren.

**Nur Firewall**

Für eine sichere DMZ mit öffentlichen Servern ist dagegen eine separate Maschine als Host empfehlenswert. Diese kann sogar mit abgezogenem LAN-Kabel isoliert als DMZ laufen und nur mit einem dedizierten Internet-Zugang verbunden werden. So ist eine optimale Trennung vom Firmennetz gegeben, und alle Maschinen, inkl. Firewall, laufen auf einem kompakten Server.

**Isolierte Maschine als DMZ**

Für den Betrieb einer Firewall und einiger virtueller Server in der DMZ muss der Host über genügend RAM und Plattenplatz verfügen, an die CPUs werden nur geringe Anforderungen gestellt. Hinweise zur Installation von VMware oder Microsoft Virtual Server sowie zu den Host-Voraussetzungen finden Sie in *Teil 1* des Buches.

### 3.2.1 Die physischen Netzwerkkarten im Host-PC

**DSL oder Router** Eine wichtige Voraussetzung für die virtuelle DMZ ist die Ausstattung des Hosts mit den notwendigen physischen Netzwerkkarten. Wenn kein LAN vorhanden ist oder wenn Sie das LAN nicht anbinden wollen, genügt im Host nur eine physische Netzwerkkarte zum DSL-Modem oder zum Router. Neben den Gästen in der DMZ hat nur der Host selbst über ein internes virtuelles Netzwerk (Host-only) Zugriff auf das Internet. Das entspricht der Ausbaustufe 1 mit zusätzlicher DMZ. Nur über den Host können Sie die Server in der virtuellen DMZ verwalten.

Wenn Sie zusätzlich ein vorhandenes LAN über die Firewall-VM ans Internet anbinden möchten oder wenn Sie aus dem LAN auf Server in der DMZ zugreifen wollen, dann benötigt der Host mindestens zwei physische Netzwerkkarten.



Die physische Netzwerkkarte zum Internet sollte explizit nur für die Verbindung zum Router oder Modem reserviert sein. Eine Mitbenutzung für die LAN-Kommunikation des Hosts oder für andere Gäste ist aus Sicherheitsgründen nicht zu empfehlen, da sonst das LAN und die Schnittstelle zum Internet eine physische Verbindung haben. Das widerspricht dem Konzept einer DMZ und kann höchstens in einer Testumgebung kurzzeitig verwendet werden.

## 3.3 Der Aufbau der Firewall-VM in Ausbaustufen

Die Firewall-VM ist ein Gast, der mit mehreren virtuellen Netzkarten als Schnittstelle vom physischen LAN zum Internet und zur virtuellen DMZ dient.

### 3.3.1 Die Software in der Firewall-VM

**IPCop oder ISA-Server** In der VM läuft die zur Firewall optimierte Linux-Distribution *IPCop*. Genauso könnten Sie natürlich auch einen ISA-Server oder jede andere Firewall-Software in der VM installieren. Ich möchte vordergründig die Schritte zur Einrichtung der virtuellen Netzwerke und Adapter vermitteln. Dazu habe ich als Beispiel IPCop gewählt, damit Sie den Workshop auch nachvollziehen können, wenn Sie keine kostenpflichtige Lösung wie den Microsoft ISA Server zur Verfügung haben. Sollten Sie eine andere Firewall bevorzugen, dann können Sie diese auf der hier vorgestellten virtuellen Infrastruktur problemlos einsetzen.

## Was ist IPCop?

IPCop ist eine kostenlose Linux-Distribution, die sich als Firewall-Lösung bereits seit langer Zeit etabliert hat. Für die Einrichtung und Verwendung von IPCop sind keinerlei Linux-Kenntnisse notwendig. Bis auf die unkomplizierte Installation erfolgt die Bedienung größtenteils über ein komfortables Web-Interface, in dem Sie vom LAN aus alle Einstellungen, wie Filterregeln oder Zugangsdaten, vornehmen können. Wenn Sie sich den Installationsvorgang von IPCop sparen wollen, können Sie das Programm bereits als fertig installierte Appliance von den VMware-Webseiten herunterladen. Mit einer eigenen Installation lernen Sie aber das Konzept besser kennen.

IPCop stellt mehrere Netzwerkschnittstellen zur Verfügung, an die jeweils das Internet, das LAN oder eine DMZ angeschlossen werden kann. Dabei wird die Gefährlichkeit der angeschlossenen Netzwerke von IPCop durch unterschiedliche Farben dargestellt (siehe auch Abbildung 3.5):

- **Grün:** *das lokale abgesicherte LAN* – Internet-Verkehr gelangt vom grünen Netz nur mittels NAT (*Network Address Translation*) nach draußen. Auf die DMZ und ins Internet kann vom grünen Netz (LAN) voll zugegriffen werden. Von der DMZ oder vom Internet aus ist dagegen keinerlei Zugriff aufs grüne Netz möglich.
- **Orange:** *die DMZ* – Hier stehen später die virtuellen Rechner, die auf explizit freigegebenen Ports vom Internet aus erreicht werden können. Dazu gehört unser Webserver, der z.B. auf Port 80 von jedem Browser der Welt erreicht werden soll. Ein Zugriff von der DMZ (Orange) ins LAN (Grün) ist nicht möglich.
- **Rot:** *das Internet* – Von der roten Schnittstelle lässt IPCop nur Antwortpakete auf die Anfragen der LAN-Clients zurück ins LAN (Grün) passieren, damit diese im Internet surfen können. Der Administrator kann zusätzlich bestimmte Ports der Firewall nach innen öffnen (z.B. Port 80 für einen Webserver) und damit eine Kommunikation vom Internet (Rot) in die DMZ (Orange) oder ins LAN (Grün) zulassen.

Den Download von IPCop finden Sie auf der offiziellen IPCop-Webseite:

[www.ipcop.org](http://www.ipcop.org)

Es existiert auch ein deutsches Forum zum Thema:

[www.ipcop-forum.de](http://www.ipcop-forum.de)

IPCop als fertig installierte Appliance finden Sie auch auf den VMware-Seiten:

[www.vmware.com/vmtn/appliances/directory](http://www.vmware.com/vmtn/appliances/directory)

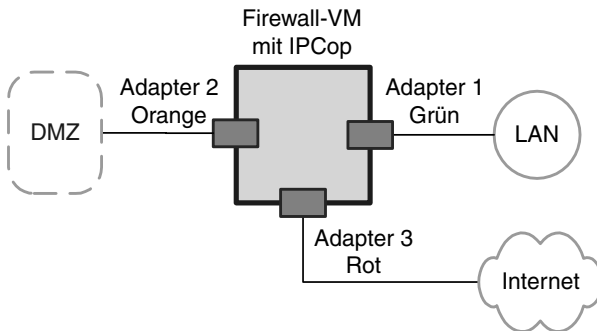
### 3.3.2 Die virtuellen Netzwerkkarten der Firewall-VM

Virtuelle Netzwerkkarten werden von VMware in den Gästen vollständig emuliert. Dazu muss nicht einmal eine physische Netz Karte im Host vorhanden sein. Das Gastbetriebssystem in der VM sendet seine Pakete ganz normal an den virtuellen Adapter, ohne zu wissen, dass dieser keine echte Hardware ist. Ob die Pakete auch ins physische LAN bzw. ins Internet gelangen oder ob die VM nur in der virtuellen Welt kommunizieren kann, ist abhängig von den Einstellungen der jeweiligen virtuellen Netzwerkkarte. Tiefere Grundlagen zu den Netzwerkfunktionen finden Sie in *Teil 3, Kapitel 1* und *Kapitel 2*. Alles, was Sie zum Aufbau der virtuellen DMZ benötigen, vermittele ich direkt hier im Workshop.

#### Die Funktion der drei virtuellen Netzwerkkarten der Firewall-VM

Die Firewall-VM wird mit ihren virtuellen Netzwerkkarten zum Vermittler zwischen LAN, DMZ und Internet.

Abbildung 3.5:  
Die Firewall-VM  
wird mit drei virtuel-  
len Netzwerkadap-  
tern zum Vermittler  
zwischen LAN,  
Internet und DMZ



Egal welche Ausbaustufe Sie wählen, wir bauen immer drei virtuelle Adapter in die Firewall-VM ein. Wenn die Netzwerkkarte für die DMZ nicht benötigt wird, bleibt sie einfach unbenutzt. Die virtuelle Hardware-Ausstattung ist damit bereits für alle Ausbaustufen vorbereitet und muss später nicht mehr verändert werden. Die einzelnen virtuellen Adapter der Firewall-VM haben folgende Funktionen (siehe auch Abbildung 3.5):

- **Der virtuelle Adapter1** bildet den *LAN-Anschluss* (grünes IPCop-Netzwerk) der Firewall. Er wird in der Ausbaustufe 2 mit jener physischen Host-Netzwerkkarte verbunden, an der auch das LAN angeschlossen ist. Die Firewall ist darüber uneingeschränkt aus dem Firmennetz erreichbar. Nutzer können darüber sicher im Internet surfen und auf die Server in der DMZ zugreifen.

Wenn kein LAN angeschlossen ist (Ausbaustufe 1), dann konfigurieren Sie Adapter1 als so genanntes *Host-only-Netz*. Für solch ein Netz ist keine physische Netzwerkkarte im Host notwendig. Über dieses virtuelle Netz kann der Host auch ohne LAN auf die Fire-

wall, die DMZ und auf das Internet zugreifen. Der Host stellt in Ausbaustufe 1 sozusagen als einziger PC das LAN dar. An der Konfiguration der Firewall ändert sich dadurch nichts.

- **Der virtuelle Adapter2** wird zum *DMZ-Anschluss* (oranges IPCop-Netzwerk) und ist an ein internes virtuelles VMware-Netz (*VMnet2*) angeschlossen. Dieses virtuelle Netzwerk bildet die eigentliche DMZ und ist in sich abgeschottet ohne direkten Kontakt zur Außenwelt. Es kann nur über die Firewall erreicht werden. Am gleichen Netzwerk schließen Sie in Ausbaustufe 3 auch den virtuellen Webserver an. Wollen Sie die Lösung nur als Firewall ohne DMZ und ohne virtuellen Webserver verwenden, dann bleibt der Adapter2 einfach unbenutzt.
- **Der virtuelle Adapter3** ist der *Internet-Anschluss* der Firewall (rotes IPCopNetz). Sie weisen ihm später die physische Host-Netzwerkkarte zu, die am DSL-Modem oder am Router angeschlossen ist. Über Adapter3 hält die Firewall die Internet-Verbindung, egal ob mit einer DMZ oder nur als einfacher Surfzugang. Der virtuelle Adapter3 und die zugehörige physische Netzwerkkarte im Host werden unbedingt benötigt.

### 3.3.3 Zusammenbauen der Firewall-VM

Die virtuelle Maschine für die IPCop-Installation können Sie jetzt ganz bequem in der VMware Server Console oder direkt im Fenster der VMware Workstation mit dem Wizard unter FILE/NEW/VIRTUAL MACHINE zusammenklicken. Als Konfigurationstyp genügt TYPICAL.

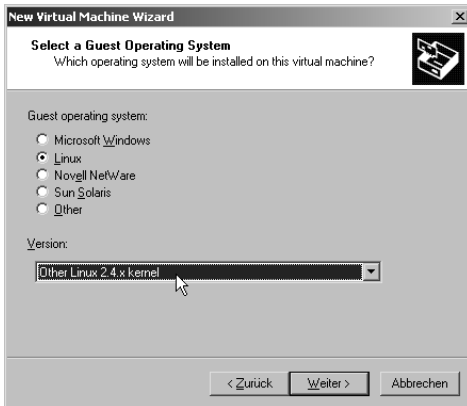


Abbildung 3.6:  
In der VM läuft  
IPCop mit Linux-  
Kernel 2.4

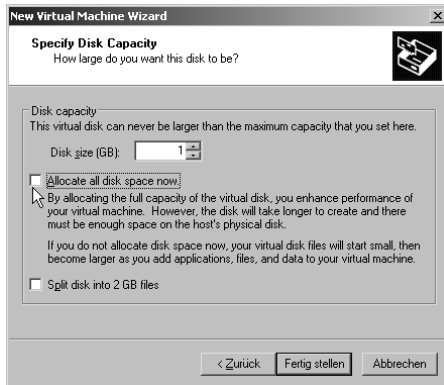
Wählen Sie als Gastbetriebssystem *Other Linux 2.4x Kernel* (Abbildung 3.6), vergeben Sie den Namen *firewall1*, und legen Sie für die VM ein eigenes Verzeichnis auf dem Host an. Die weitere Konfiguration der virtuellen Hardware erfolgt nach den Vorgaben des Wizards. Lassen Sie im Fenster zur Netzwerkkarte die Einstellung vorerst auf *Bridged*.



**Virtuelle Festplatte anpassen**

Nur bei der virtuellen Festplatte sollten Sie die Vorgaben des Wizards anpassen. IPCop benötigt wenig Platz, weshalb eine 1GB-Platte genügt. Beim VMware Server ist der Haken an *Preallocate all Disk Space now* zu entfernen, um keinen unnötigen Platz auf dem Host zu verschwenden (Abbildung 3.7). Mit dem Haken wird sonst der gesamte Plattenplatz der virtuellen Platte bereits reserviert, auch wenn der Gast ihn später nicht benötigt. Weitere Informationen zu virtuellen Festplatten finden Sie in Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“.

Abbildung 3.7:  
IPCop benötigt nur  
wenig Plattenplatz



Nachdem die VM zusammengebaut wurde, fällt vor der Installation der Software im Gast noch etwas Nacharbeit an. Im Menü VM/SETTINGS/HARDWARE entfernen Sie überflüssige Geräte. Unsere Firewall benötigt kein USB und kein Audio, außerdem genügen 16 MB RAM. Da VMware den Speicher zwischen Host und VMs aufteilen muss, sollten Sie nicht zu verschwenderisch damit umgehen (siehe auch Abbildung 3.10 weiter unten).

### 3.3.4 Netzwerkkonfiguration der Firewall-VM

#### Zusätzliche virtuelle Adapter hinzufügen

Zwei ganz essenzielle Dinge fehlen noch – die restlichen Netzwerkkarten. Die Firewall benötigt in der Endausstattung drei davon. Wie ich schon erwähnt habe, werden wir immer alle drei Netzwerkkarten zuweisen, egal bei welcher Ausbaustufe. Also setzen Sie schnell den virtuellen Schraubenzieher an und bauen mittels VM/SETTINGS/HARDWARE/ADD zwei weitere Ethernet-Adapter ein. Dabei übernehmen Sie die vorgegebene Einstellung *Bridged*, Sie passen die Adapter später an.



Sollten Sie noch den GSX Server im Einsatz haben, wählen Sie unter ADAPTER TYPE unbedingt *vlan* und nicht *vmxnet* (Abbildung 3.8). Sonst erkennt die IPCop-Installation keine Netzwerkkarten. Beim VMware Server existiert diese Auswahl nur noch bei *legacy*-Maschinen, also VMs aus älteren VMware-Versionen.

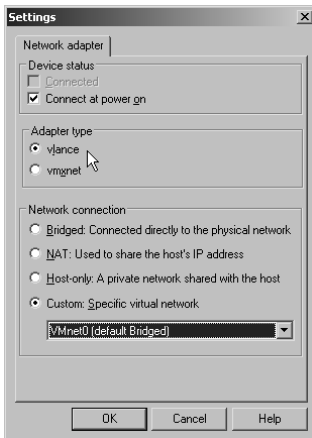


Abbildung 3.8:  
Nur ein vlance-  
Adapter wird ohne  
zusätzliche Treiber  
in einer der VM  
erkannt. Die Aus-  
wahl gibt es nur noch  
beim GSX Server

## Die virtuellen Adapter der Firewall-VM den richtigen virtuellen Netzen (VMnet) zuweisen

Welcher virtuelle Adapter der Firewall-VM mit dem LAN bzw. Internet kommunizieren kann und welcher Adapter dagegen in der DMZ isoliert bleibt, das bestimmen Sie mit der Zuweisung dieser Adapter zu bestimmten virtuellen Switches, den *VMnets*.

### VMnet-Switches und virtuelle Adapter

Ein *VMnet* bildet unter VMware intern ein virtuelles Netz, in dem sich standardmäßig nur die Gäste sehen, die am gleichen VMnet angeschlossen sind. Das entspricht dem Verhalten physischer Rechner an physischen Switches, weshalb die VMnets auch als *virtuelle Switches* bezeichnet werden. Normalerweise ist ein solches virtuelles Netz vom Host und vom LAN isoliert, kein Paket gelangt nach draußen.

Wurde einem solchen VMnet zusätzlich eine physische Netzwerkkarte des Host-PC zugewiesen, dann bezeichnet man das virtuelle Netz als *bridged*. Das bedeutet, es verfügt über eine Brücke ins physische LAN. Alle virtuellen Adapter an diesem VMnet funktionieren dadurch wie echte Netzwerkkarten. Der gesamte Netzwerkverkehr der Gäste erscheint am Ausgang der zugewiesenen physischen Karte und damit im LAN. Die VMs sind voll erreichbar wie echte PCs und benötigen eigene IP-Adressen.

Virtuelle Adapter, die am *VMnet1 (Host-only)* angeschlossen sind, können zwar nicht mit dem LAN kommunizieren, aber mit dem Host selbst. Sie benötigen dafür keine physische Netzwerkkarte, wodurch die Kommunikation vom Host zur VM über VMnet1 auch ohne LAN funktioniert. Wir verwenden VMnet1 z.B. in der Ausbaustufe 1 ohne LAN-Anbindung.

Tiefere Grundlagen zu den Netzwerken finden Sie in *Teil 3, Kapitel 2*, „*Virtuelle Netzwerke Teil 2 – die ganze Wahrheit*“.

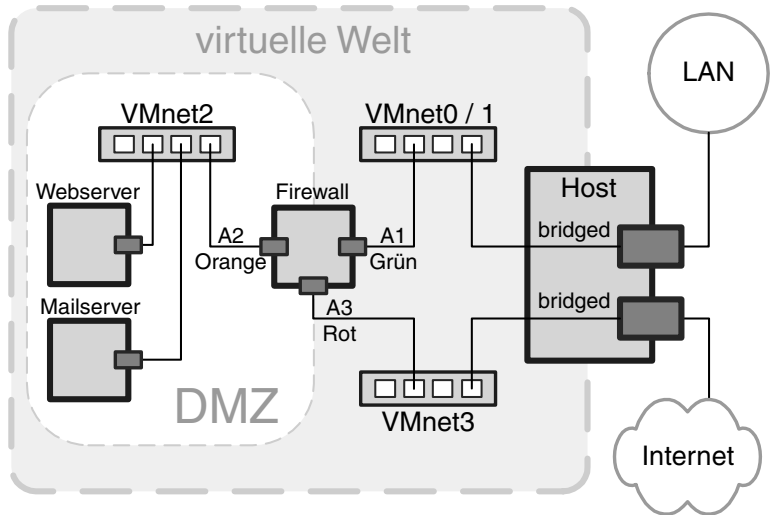


**Isoliertes Netz**

**Brücke ins LAN**

**Nur mit dem Host**

Abbildung 3.9:  
Die endgültige  
Ausbaustufe mit  
LAN-Anbindung  
über einen Bridged-  
Adapter an VMnet0  
und mit Servern in  
der DMZ an  
VMnet2



**Custom-Adapter** Alle drei Adapter der Firewall-VM konfigurieren Sie über VM/SETTINGS/HARDWARE als Adapter vom Typ *Custom*, und schließen Sie jeweils an ein bestimmtes virtuelles VMware-Netz (VMnet) an (Abbildung 3.10). Halten Sie dabei folgende Reihenfolge unbedingt ein, denn jede Netzwerkkarte hat später in der Firewall eine bestimmte Aufgabe zu erfüllen (siehe zur Übersicht die Zeichnung in Abbildung 3.9).

- **Adapter1:** LAN oder nur Host – grünes IPCop-Netz – Den ersten virtuellen Adapter schließen Sie für Ausbaustufe 1 (kein LAN vorhanden) an das VMnet1 (Host-only) an. Nur der Host kann darüber mit der Firewall kommunizieren (Abbildung 3.10). Für die Ausbaustufe 2 mit LAN-Anbindung gehört der Adapter dagegen an VMnet0 (default Bridged). Darüber kommuniziert später das LAN über eine physische Host-Netzkarte direkt mit der Firewall.
- **Adapter2:** DMZ – oranges IPCop-Netz – Völlig unabhängig von der Ausbaustufe binden Sie den zweiten Adapter immer an das interne abgeschottete Netz VMnet2, die DMZ.
- **Adapter3:** Internet – rotes IPCop-Netz – Der dritte Adapter gehört an VMnet3. Diesem Netz weisen Sie später die physische Netzwerkkarte zu, an der das Modem oder der Router angeschlossen ist. Der Adapter3 kommuniziert mit dem Internet.

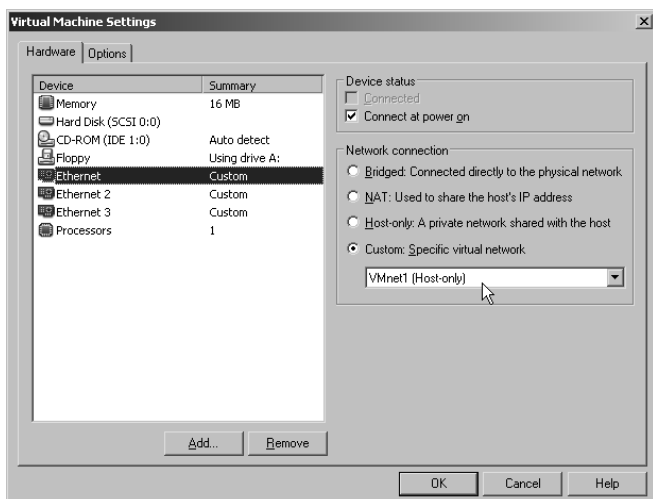


Abbildung 3.10:  
Jeder der drei Adapter gehört an ein bestimmtes VMnet

## Die physischen Netzwerkkarten die richtigen VMnets zuweisen

Jetzt erfolgt die Zuweisung der eben angeschlossenen VMnet-Switches zu den physischen Netzwerkkarten im Host. So legen Sie fest, welche virtuelle Netzwerkkarte der Firewall Kontakt zur Außenwelt hat und welche nicht. Unter dem Reiter HOST/VIRTUAL NETWORK SETTINGS/ HOST VIRTUAL NETWORK MAPPING (oder EDIT/VIRTUAL NETWORK SETTINGS bei der Workstation) konfigurieren Sie die VMnet-Switches manuell (Abbildung 3.11). Dabei ergeben sich folgende Zuweisungen:

### Kontakt zur Außenwelt

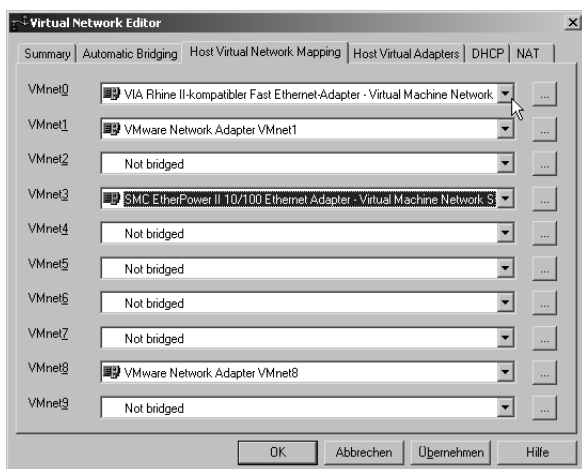


Abbildung 3.11:  
Wurde einem virtuellen Switch ein physischer Adapter zugewiesen, sind alle VMs in diesem Netz mit dem LAN verbunden

- **VMnet0 in der Ausbaustufe 1** – wird von der Firewall nicht verwendet. Sie müssen also bei Ausbaustufe 1 an VMnet0 nichts verändern oder einstellen, egal welcher Eintrag bereits vorhanden ist. Stattdessen haben Sie den Adapter1 (IPCop grün) für die reine Host-Kommunikation an *VMnet1 (host-only)* angeschlossen (siehe auch Abbildung 3.10).

- ▶ **VMnet0 (LAN, grün)** in der Ausbaustufe 2 – weisen Sie jene physische Netzwerkkarte des Host-PC zu, an der das LAN angeschlossen ist. Der virtuelle Switch VMnet0 und alle angeschlossenen Gäste sind dadurch mit dem LAN verbunden, und ein LAN-Client erreicht über den Adapter1 (IPCop grün) die Firewall.
- ▶ **VMnet2 (DMZ, orange)** – bleibt immer *not bridged*. Alle hier angeschlossenen virtuellen Netzwerkkarten haben somit keinerlei Verbindung zur realen Welt. Sie können intern nur mit anderen virtuellen Maschinen am selben virtuellen Switch kommunizieren. Das interne Netzwerk VMnet2 bildet später die abgeschottete DMZ, egal ob diese verwendet wird oder nicht.
- ▶ **VMnet3 (Internet, rot)** – weisen Sie der physischen Netzwerkkarte zu, die am DSL-Modem oder am Router steckt. VMs am VMnet3 (in unserem Falle nur die Firewall) kommunizieren über diesen physischen Adapter mit angeschlossenen Geräten, z.B. dem Router.



Überprüfen Sie unbedingt, ob die Reihenfolge der Adapter und die Zuweisungen in Ihrer Konfiguration stimmen. Sonst funktioniert später kein einziges Element der Firewall!

#### 3.3.5 Installation von IPCop in der Firewall-VM

In der vorbereiteten VM installieren Sie IPCop. Dabei weisen Sie die verschiedenen Netze *Grün*, *Orange*, *Rot* den vorbereiteten virtuellen Netzwerkkarten zu. Diese Adapter haben Sie bereits mit den richtigen virtuellen Switches verbunden, so dass IPCop nach der Installation sofort mit dem LAN, mit dem Internet und mit der DMZ kommunizieren kann.

##### Grundinstallation von IPCop von einem ISO-Image

Das ISO-Image von der IPCop-Webseite binden Sie vor dem Start über VM/SETTINGS/CD-ROM/USE ISO IMAGE gleich als emulierte CD ein. So sparen Sie sich das Brennen einer CD (Abbildung 3.12). Sobald Sie die VM einschalten, erscheint nach dem Booten die Begrüßungsmeldung von IPCop, die mit  zu bestätigen ist.

##### Tastatur und Maus verwenden

Navigieren lässt sich während der IPCop-Installation mit . Vergessen Sie nicht, dass Tastatur und Maus in einer VM erst dann funktionieren, wenn einmal in das Fenster geklickt wurde. Mit  +  wird die Maus dann wieder freigegeben. Die VMware Tools lassen sich unter IPCop nicht installieren, weshalb Sie die permanent unten links angezeigte Warnung *You do not have VMware Tools installed!* ignorieren.

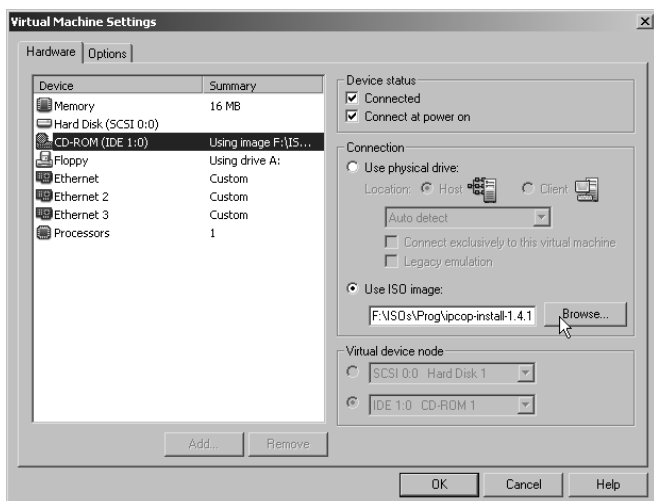


Abbildung 3.12:  
Ein ISO-Image  
kann direkt als CD  
verwendet werden

In der virtuellen Maschine beginnt die Installation mit der Sprachauswahl und dem Willkommensbildschirm, die Grundinstallation ist selbsterklärend. Nach der Auswahl von CD-ROM als Programmquelle (Abbildung 3.13) partitioniert das Setup automatisch die virtuelle Festplatte und installiert IPCop. Die Frage nach der Diskette mit gesicherten Systemeinstellungen überspringen Sie.

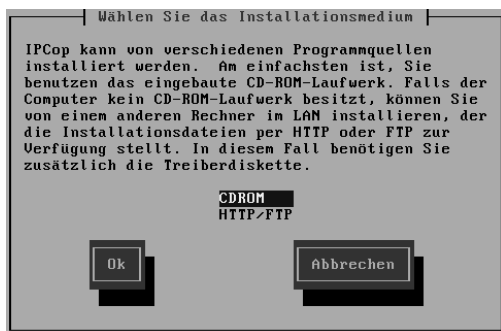


Abbildung 3.13:  
Sie können die Fire-  
wall direkt vom  
ISO-Image instal-  
lieren

## Die erste Netzwerkkarte während des IPCop-Setups

Bei der Netzwerkkonfiguration der Installationsroutine wählen Sie AUTOMATISCHE ERKENNUNG. Es sollte ein Adapter vom Typ AMD PCNet32 gefunden werden (Abbildung 3.14). Den ersten Adapter macht IPCop automatisch zur grünen Schnittstelle. Er stellt damit das sichere LAN dar, in unserem Falle VMnet0 oder VMnet1.

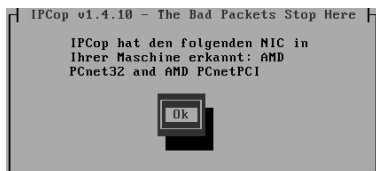


Abbildung 3.14:  
Adapter1 wird von  
der Setup-Routine  
automatisch erkannt

Als IP-Adresse weisen Sie exemplarisch die 192.168.1.1 (Abbildung 3.15) zu. Diese Adresse muss bei Ausbaustufe 2 im Netzwerkbereich Ihres LAN liegen und dort frei sein. In Ausbaustufe 1 (ohne LAN-Anbindung) kann eine Adresse aus einem beliebigen nicht-öffentlichen Netz gewählt werden, z.B. 192.168.1.1, 192.168.5.1 oder auch 172.16.1.1.



Alle IP-Adressen des Workshops sollten Sie Ihren Gegebenheiten anpassen. Ich gehe davon aus, dass Ihr LAN den Adressbereich 192.168.1.x verwendet und dort die Adresse 192.168.1.1 noch frei ist. Das wird in den wenigsten Fällen der Realität entsprechen, weshalb Sie die verwendeten Adressen ändern müssen. Zusätzlich sollten Sie darauf achten, dass sich die weiter unten vorgeschlagenen internen Netzwerkadressen (z.B. für die DMZ) nicht mit Netzwerkbereichen überschneiden, die bei Ihnen bereits im Einsatz sind. Einen Überblick über die gesamten Adressen der Beispielkonfiguration liefert Ihnen die Tabelle 3.1).

Abbildung 3.15:  
Adapter 1 wird die  
grüne Schnittstelle  
der Firewall und  
damit der Anschluss  
zum abgesicherten  
LAN

GREEN Schnittstelle

Geben Sie die IP-Adressinformationen für die GREEN Schnittstelle ein.

IP-Adresse: 192.168.1.1

Subnetzmaske: 255.255.255.0

Ok Abbrechen

#### IPCop-Konfiguration

Damit ist die Grundinstallation abgeschlossen, das IPCop-Setup startet gleich anschließend automatisch. Nach der Auswahl des Tastaturlayouts *de* und der Zeitzone *Europe/Berlin* bekommt Ihre Firewall den Hostname *firewall1* und den Domännennamen *localdomain*. Im nächsten Fenster wählen Sie **ISDN DEAKTIVIEREN** (Abbildung 3.16). Der direkte Zugriff auf eine ISDN-Karte im Host ist aus der VM heraus sowieso nicht möglich.

Abbildung 3.16:  
Auch wenn Sie eine  
ISDN-Karte im Host  
eingebaut haben,  
wird diese Hardware  
nicht in eine VM  
durchgereicht

ISDN-Konfigurationsmenü

ISDN ist momentan Deaktiviert.

Protokoll: NICHT GESETZT

Karte: NICHT GESETZT

Lokale Telefonnummer: NICHT GESETZT

Wählen Sie aus, was Sie konfigurieren möchten, oder verwerfen Sie die aktuellen Einstellungen.

Protokoll/Land

Zusätzliche Modulparameter angeben

ISDN-Karte

Lokale Telefonnummer (MSN/EA2)

Ok ISDN aktivieren ISDN deaktivieren

3.3.6      **Netzwerkconfiguration von IPCop**

Jetzt beginnt die eigentliche Netzwerkconfiguration der Firewall. Alle Einstellungen der Netzwerke und Adapter sehen Sie in der Tabelle 3.1 auf einen Blick. Vor allem zur Fehlersuche können Sie sich damit einen besseren Überblick verschaffen. Vorausgreifend habe ich die Umsetzung mit MS Virtual PC/Server ebenfalls mit eingefügt. Beachten Sie als Ergänzung auch die Zeichnung in Abbildung 3.9.

**Auch mit MS  
Virtual PC/Server**

| Virtueller Adapter | Adapter 1, grün                                        | Adapter 2, orange                  | Adapter 3, rot                                     |
|--------------------|--------------------------------------------------------|------------------------------------|----------------------------------------------------|
| Netzwerk           | LAN/nur Host                                           | DMZ                                | Internet                                           |
| IPCop Farbe        | GREEN, eth0                                            | ORANGE, eth1                       | RED, eth2                                          |
| IPCop Adresse      | 192.168.1.1                                            | 192.168.2.1                        | PPPoE/Router                                       |
| Vmware VMnet       | VMnet0/1                                               | VMnet2                             | VMnet3                                             |
| Vmware Typ         | bridged/host-only                                      | not bridged                        | Bridged                                            |
| MS VPC/Server      | Physische Netz-<br>werk-karte oder<br>Loopback-Adapter | Nur lokal/<br>internes<br>Netzwerk | externes Netz-<br>werk/physische<br>Netzwerk-karte |

*Tabelle 3.1:  
Die Netzwerkkon-  
figuration unter  
VMware und VPC/  
Server auf einen Blick*

Gehen Sie das Menü der Netzwerkconfiguration während des IPCop-Setups einfach der Reihe nach durch. Sie können später den Vorgang jederzeit wiederholen. Um nachträglich Änderungen an der IPCop-Konfiguration zu machen, melden Sie sich an der Konsole mit `root` an und geben den Befehl `setup` ein.



- 1. Der TYP DER NETZWERKKONFIGURATION ist in unserem Beispiel **GREEN + ORANGE + RED** (Abbildung 3.17).

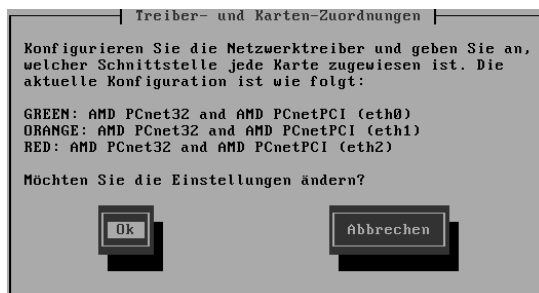


*Abbildung 3.17:  
Die Gefährlichkeit  
der Netze stellt  
IPCop übersichtlich  
durch Farben dar*



- eth0, eth2, eth3**
- In der TREIBER- UND KARTEN-ZUORDNUNG von IPCop weisen Sie die Netzfarben *Orange* und *Red* den beiden verbleibenden Schnittstellen zu. Sie müssen dazu nur zweimal  drücken. Das grüne Netz wurde vom Setup bereits an die Schnittstelle *eth0* vergeben.
  - Die IPCop-Netze sind damit den richtigen virtuellen Netzwerkkarten zugeordnet. Ein nochmaliger Kontrollblick in die TREIBER- UND KARTEN-ZUORDNUNG zeigt das Ergebnis. Orange gehört an *eth1* und Red an *eth2* (Abbildung 3.18). Sie verlassen die Übersicht nach der Kontrolle mit ABBRECHEN.

Abbildung 3.18:  
Die Treiber und  
Kartenzuordnung  
zeigt die Konfigura-  
tion noch einmal im  
Überblick



### IP-Adressen der Adapter in der IPCop-Firewall

Nach erfolgter Zuordnung der farbigen IPCop-Netze zu den *eth*-Schnittstellen und damit zu den virtuellen Adaptern der VM vergeben Sie die IP-Adressen. Grün haben Sie bereits die Adresse 192.168.1.1 zugewiesen. In den ADRESS-EINSTELLUNGEN vom IPCop-Setup konfigurieren Sie den Rest, es ergibt sich folgende Zuordnung:

- ▶ **Grün (eth0)** – 192.168.1.1
- ▶ **Orange (eth1)** – 192.168.2.1
- ▶ **Rot (eth2)** muss PPPoE verwenden, wenn ein DSL-Modem angesprochen wird (Abbildung 3.19). Bei einer Anbindung an einen Router bekommt *Rot* eine IP-Adresse aus dem Bereich, den der Router auf seinem internen LAN-Interface verwendet. Zu den verschiedenen Möglichkeiten der Anbindung eines Routers lesen Sie bitte den Abschnitt 3.4.4.

Bestätigen Sie zum Abschluss die Adresseinstellungen mit FERTIG.

Abbildung 3.19:  
PPPoE wird für ein  
DSL-Modem ver-  
wendet. Für einen  
Router muss hier  
eine passende IP-  
Adresse eingetragen  
werden



## DNS, Gateway und DHCP-Server konfigurieren

DNS- UND GATEWAY-EINSTELLUNGEN sind bei einem DSL-Modem nicht notwendig, da der Provider diese Daten beim Verbindungsaufbau liefert. Dient dagegen ein Router als DSL- oder Standleitungsabschluss, dann müssen Sie dessen Adresse im Feld für DNS-SERVER und GATEWAY eintragen. Bestätigen Sie die Netzwerkkonfiguration anschließend mit FERTIG.

**DSL-Modem oder Router**

Die Setup-Routine fragt nun, ob IPCop auch einen DHCP-Server bereitstellen soll. In unserem Workshop ist das nicht der Fall, also müssen Sie hier nichts ausfüllen.

**DHCP-Server**

Wählen Sie an dieser Stelle im DHCP-Menü unbedingt immer OK und nicht ABBRECHEN, weil die Setup-Routine sonst einfach die Installation beendet!



### 3.3.7 Abschluss der IPCop-Installation

Zum Schluss fragt das Setup noch die Passwörter für zwei spezielle IPCop-Nutzer ab. Der Nutzer *root* erhält die volle Kontrolle über das System an der Kommandozeile, und mit dem Nutzer *admin* melden Sie sich später am Web-Interface von IPCop an. Eine nachträgliche Änderung der gesamten Konfiguration ist möglich, indem Sie sich als *root* an der Konsole anmelden und das Kommando `setup` eingeben.

**Passwort für admin und root**

Die Eingabe der Passwörter während des IPCop-Setup erfolgt im völligen Blindflug. Tastenanschläge werden nicht angezeigt, und es bewegt sich auch kein Cursor. Keine Angst, Ihre Tastatur funktioniert! Schreiben Sie das Passwort einfach blind, und navigieren Sie mit  zur Bestätigung.



Nach erfolgreichem Abschluss der Installation und nach dem automatischen Neustart von IPCop ist es Zeit für den ersten *Snapshot* (Abbildung 3.20). Damit sichern Sie den momentanen Systemzustand Ihrer virtuellen Maschine und können jederzeit durch ein *Revert* zu diesem Stand zurückkehren. Wenn im weiteren Verlauf der Konfiguration etwas schief gehen sollte, müssen Sie nicht wieder ganz von vorn anfangen. Ausführliche Hinweise und Verfahren zur Verwendung von Snapshots finden Sie in *Teil 3, Kapitel 4, „Die Snapshot- und Clone-Funktion der VMware-Produkte“*.

**Der erste Snapshot**



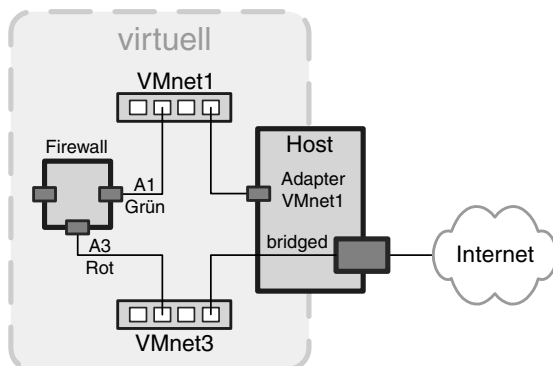
Abbildung 3.20:  
Ein Snapshot sichert den Konfigurationsstand

## 3.4 Ergänzungen zu den ersten beiden Ausbaustufen

Die Installation der Software ist damit abgeschlossen. Um das Netzwerk zu vervollständigen, sind noch einige Handgriffe und ein abschließender Testlauf notwendig.

### 3.4.1 Ausbaustufe 1, Kommunikation mit der Firewall ohne LAN-Anbindung

Abbildung 3.21:  
Der Host kann über den VMware Network-Adapter VMnet1 mit dem virtuellen Netz und der Firewall kommunizieren



Bei der Ausbaustufe 1 ohne LAN-Anbindung ist keine zweite physische Netzwerkkarte im Host-PC vorhanden. Der einzige physische Adapter wird ausschließlich für die Internet-Verbindung genutzt (Abbildung 3.21). Das kann der Fall sein, wenn Sie eine völlig abgeschottete DMZ auf einem dedizierten Host ohne LAN-Anbindung betreiben wollen oder wenn Sie auf Ihrem normalen PC den Workshop zu Testzwecken nachvollziehen. Eigentlich kann in dieser Konfiguration niemand auf die Firewall zugreifen, um sie zu konfigurieren oder um Server in der DMZ anzusprechen. Der Host gelangt auch nicht ins Internet, da er mit IPCop nicht kommunizieren kann.

#### Host-only-Netz ohne physische Netzwerkkarte an VMnet1

Damit der Host in Ausbaustufe 1 die Firewall trotzdem erreicht, benötigt er irgendeine Netzwerkkarte. VMware installiert für solche Fälle zwei virtuelle Adapter auf dem Host, die auch funktionieren, ohne dass eine physische Netzwerkkarte vorhanden ist. In den Netzwerkeinstellungen eines Windows-Hosts sind diese Adapter als normale Netzwerkkarten sichtbar (Abbildung 3.22).

Der Adapter *VMware Network Adapter VMnet1* ist standardmäßig immer mit dem virtuellen Switch *VMnet1* verbunden (siehe auch die Zeichnung in Abbildung 3.21).

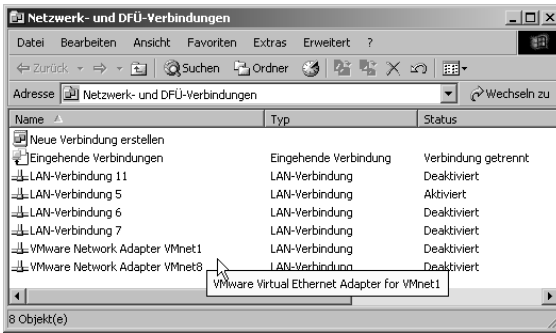


Abbildung 3.22:  
Der virtuelle Host-Adapter VMnet1 wirkt für den Host wie eine echte Netzwerkkarte

Alle VMs an VMnet1 und der Host bilden damit das so genannte *Host-only-Netz*. Der virtuelle Host-Adapter benötigt nur noch die richtige IP-Adresse, um mit der Firewall kommunizieren zu können, wenn diese an VMnet1 angeschlossen ist. In den Netzwerkeinstellungen des Host-PC weisen Sie dem Adapter die Adresse 192.168.1.2 zu. Als Standard-Gateway und als DNS-Server definieren Sie die grüne Adresse der IPCop-Firewall 192.168.1.1 (Abbildung 3.23 und Abbildung 3.24).

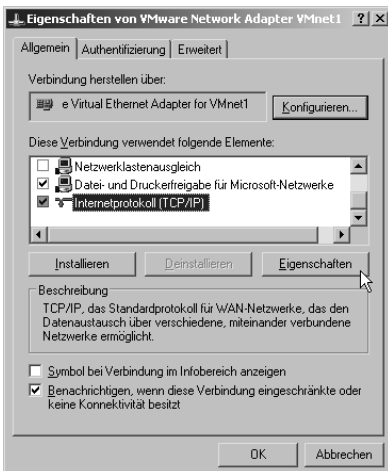
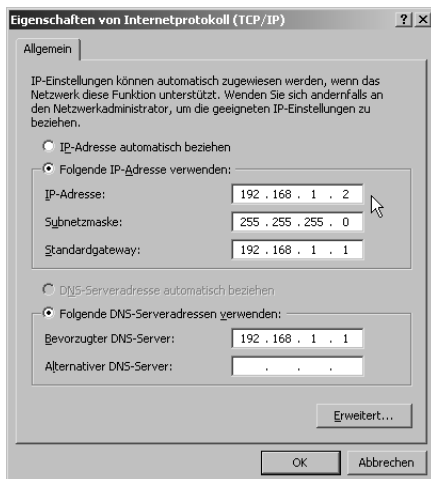


Abbildung 3.23:  
Der virtuelle Host-Adapter VMnet1 kann auf dem Host wie eine normale Netzwerkkarte verwendet werden

Ein Hinweis nur für diejenigen Leser, die bereits die Netzwerk-Kapitel in Teil 3 durchgearbeitet haben: Sie werden sich fragen, warum wir den *VMware Network Adapter VMnet1* nicht über die Subnet-Einstellung der virtuellen Switches (siehe Teil 3, Kapitel 2) im Netzwerkmenü von VMware konfigurieren. Zum einen möchte ich hier nicht auf die gesamten Netzwerk-Features eingehen, dazu existieren die ausführlichen Workshops. Zum anderen würde der Adapter dann automatisch die Adresse 192.168.1.1 bekommen und damit im Konflikt mit der im Workshop verwendeten Adresse von IPCop stehen.



Abbildung 3.24:  
Der virtuelle Host-  
Adapter VMnet1  
dient zur direkten  
Kommunikation vom  
Host mit IPCop ohne  
physisches LAN



**Adapter1 gehört  
an VMnet1**

Sobald Sie den virtuellen Adapter1 der Firewall-VM unter VM/SETTINGS/HARDWARE mit *VMnet1* verbinden (siehe auch Abbildung 3.10 weiter oben), dann befindet er sich im gleichen virtuellen Netzwerk wie der *VMware Network Adapter VMnet1* des Host-PC. Dadurch kann der Host-PC mit der Firewall in einem internen virtuellen Netz kommunizieren, ohne eine physische Netzwerkkarte zu benutzen.



Alle IP-Adressen des *Host-only-Netzes* sollten in einem Netzwerk-bereich liegen, der weder auf dem Host-PC noch irgendwo anders in Ihrer vorhandenen Umgebung verwendet wird, damit keine Konflikte entstehen.

### 3.4.2 Ausbaustufe 2, LAN-Anbindung über das Bridged-Netz VMnet0

**Zwei physische  
Netzwerkkarten**

In der Ausbaustufe 2 verfügt der Host über zwei physische Netzwerkkarten. Eine davon dient wieder als dedizierte Verbindung für das rote IPCop-Interface zum Internet. Über den anderen Adapter sind der Host selbst und die grüne Schnittstelle von IPCop ans LAN angeschlossen (Abbildung 3.25). Ausbaustufe 2 entspricht damit fast schon der Ausbaustufe 3, es fehlt nur noch die DMZ.

**Physische Adap-  
ter gemeinsam  
nutzen**

Nur zum besseren Verständnis – lassen Sie sich von der LAN-Anbindung bei Ausbaustufe 2 nicht verwirren! Ihr Host ist gleichzeitig normales Mitglied im LAN, und zusätzlich kommuniziert das grüne Interface der Firewall ebenfalls über dieselbe Netzwerkkarte. Der Host und die virtuelle Maschine teilen sich im *Bridged-Modus* den gleichen Netzwerkadapter, ohne sich dabei gegenseitig zu behindern. Von außen betrachtet sind das zwei getrennte Rechner.

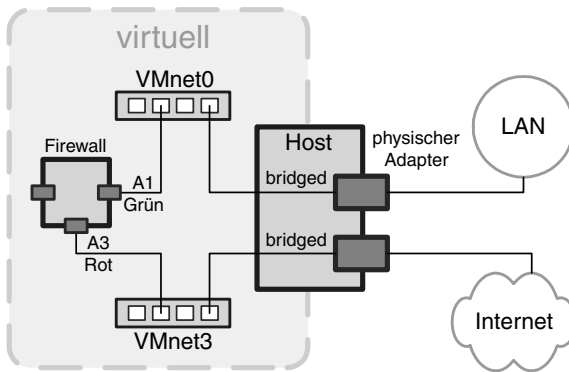


Abbildung 3.25:  
Eine physische  
Netzkarte ist am  
VMnet0 angeschlos-  
sen. Darüber können  
LAN-Clients und  
der Host die Firewall  
erreichen

Der Host-PC kommuniziert also über eine physische Netzwerkkarte ganz normal mit dem LAN und hat eine eigene IP-Adresse, z.B. die 192.168.1.125. Parallel dazu kommuniziert auf der gleichen physischen Netzwerkkarte auch der grüne Adapter der virtuellen IPCop-Maschine mit der IP-Adresse 192.168.1.1 und ist ebenfalls aus dem LAN erreichbar. Auch der Host erreicht über das LAN (also über die eigene Netzwerkkarte) die virtuelle Maschine, in der IPCop läuft. Damit können alle LAN-Clients und der Host die grüne Schnittstelle von IPCop über das LAN ansprechen.

Wird am Host das Netzkabel zum LAN abgezogen, dann deaktivieren einige Betriebssysteme diesen physischen Netzwerkadap-  
ter. Dadurch ist auch keine Kommunikation vom Host zur Fire-  
wall-VM mehr möglich. Sie müssten dann auf Ausbaustufe 1  
(Host-only mit VMnet1) ausweichen.



### 3.4.3 Testen der Ausbaustufen 1 und 2

Bevor wir fortfahren, sollten Sie Ihre Konfiguration mit ein paar Ping-Befehlen testen:

#### ► Ausbaustufe 1:

- Ping vom Host-PC auf 192.168.1.2 (Network Adapter VMnet1)
- Ping vom Host-PC auf 192.168.1.1 (IPCop, Grün, host-only)
- Ping vom Host-PC auf 192.168.2.1 (IPCop, Orange)

#### ► Ausbaustufe 2:

- Ping vom Host auf 192.168.1.1 (IPCop, Grün, bridged)
- Ping vom Host-PC auf 192.168.2.1 (IPCop, Orange)
- Ping von einem LAN-Client auf 192.168.1.1 (IPCop, Grün)
- Ping von einem LAN-Client auf 192.168.2.1 (IPCop, Orange)

Funktioniert das Ping auf die DMZ (192.168.2.1) nicht, dann hat der LAN-Client (bzw. der Host) bzw. hat wahrscheinlich noch nicht das

passende Default-Gateway auf das grüne Interface der Firewall. Anpassen können Sie den Eintrag in der Netzwerkumgebung des Clients (bzw. des Hosts) am Netzwerkadapter, der die Verbindung zum LAN herstellt. Bei Ausbaustufe 1 (ohne LAN) haben Sie bereits am Host den Adapter *VMware Network Adapter VMnet1* richtig konfiguriert (Abbildung 3.24).



Machen Sie an dieser Stelle erst weiter, wenn jedes Ping funktioniert. Überprüfen Sie gegebenenfalls alle Zuweisungen der virtuellen Adapter an die richtigen VMnets (Abbildung 3.10), weiterhin die Zuweisung der physischen Netzkarten an die richtigen VMnets (Abbildung 3.11) und die gesamte IPCop-Konfiguration (Abbildung 3.18).

### 3.4.4 Verwendung eines Routers am roten Interface von IPCop

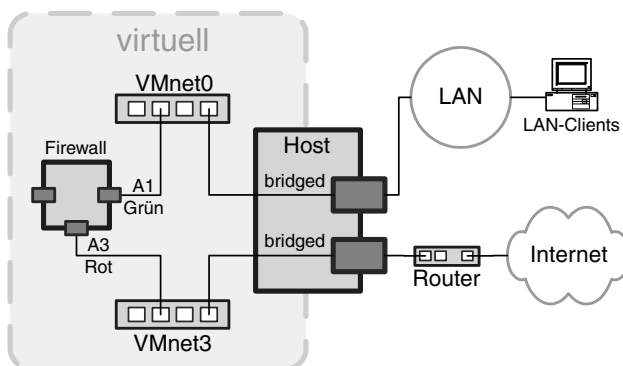
Heutzutage wird eher im Privatbereich oder bei älteren Internet-Anbindungen noch ein DSL-Modem vorhanden sein. Weitaus häufiger ist ein Router mit integriertem Modem am DSL bzw. an der Standleitung angeschlossen. Zur Verwendung eines Routers anstelle eines DSL-Modems muss ich hier noch etwas ausholen, denn es gibt grundsätzlich zwei Möglichkeiten, den Router mit der Firewall zu verbinden.

#### Router direkt an die Firewall anschließen

##### Sicherer abgeschotteter Betrieb

Die angestrebte saubere Lösung ist natürlich, den Router physisch vom LAN zu trennen und ausschließlich mit dem roten Interface von IPCop zu verbinden. Wenn Ihr Router nicht bereits über eingebaute Ethernet-Ports verfügt, an die Sie IPCop direkt anschließen können, dann benötigen Sie ein Crossover-Kabel oder einen kleinen Hub. Im Host sollte eine dedizierte Netzwerkkarte nur für diese Verbindung benutzt werden (Abbildung 3.26).

Abbildung 3.26:  
Im Normalfall wird der Router ausschließlich an die dedizierte Netzkarte für VMnet3 (rotes IPCop-Interface) angeschlossen



Damit führen alle Wege zum physischen Router nur über die Firewall-VM. Der Router, der an seinem LAN-Interface bisher eine Adresse aus dem LAN-Bereich hatte, muss allerdings umkonfiguriert werden. Er benötigt eine neue Adresse aus einem nicht verwendeten Netz, z.B. die 192.168.5.1. Dem roten Interface von IPCop weisen Sie eine dazu passende Adresse, z.B. 192.168.5.2, aus dem gleichen Netz zu (Abbildung 3.27). Sie gelangen zu den IPCop-Einstellungen, indem Sie sich in der Firewall-VM mit dem Benutzer *root* anmelden und den Befehl *setup* eingeben. Im Setup-Menü wählen Sie NETZWERK/ADRESSEINSTELLUNGEN/RED.



Abbildung 3.27:  
Bei der Verwendung eines Routers benötigt das rote Interface von IPCop eine statische Adresse aus dem richtigen Bereich

Die Einträge für den DNS-Server und für das Default-Gateway von IPCop sollten auf die Adresse des Routers 192.168.5.1 zeigen (Abbildung 3.28). Sie finden die Einstellungen unter NETZWERK/DNS- UND GATEWAY-EINSTELLUNGEN.



Abbildung 3.28:  
IPCop sollte den Router als Default-Gateway und als DNS-Server verwenden

Der Host und das gesamte LAN müssen über die grüne Schnittstelle von IPCop geroutet werden, um auf das Internet zuzugreifen. Dazu ändern Sie im LAN an jedem Client, manuell oder mittels DHCP, das Default-Gateway und eventuell auch den DNS-Eintrag auf die Adresse des grünen IPCop-Interface (in diesem Workshop ist das als Beispiel immer die 192.168.1.1). Wenn Sie bereits über ein zentrales Default-Gateway im LAN verfügen, dann genügt es, nur dort die Route ins Internet auf 192.168.1.1 (IPCop) zu ändern. Wenn Sie einen zentralen DNS-Server im LAN verwenden (z.B. in Active Directory-Domänen), dann genügt es, auf diesem eine DNS-Weiterleitung auf 192.168.1.1 (IPCop) zu konfigurieren. Sie können damit beide Einstellungen zentral ändern und müssen das nicht an allen Clients tun.

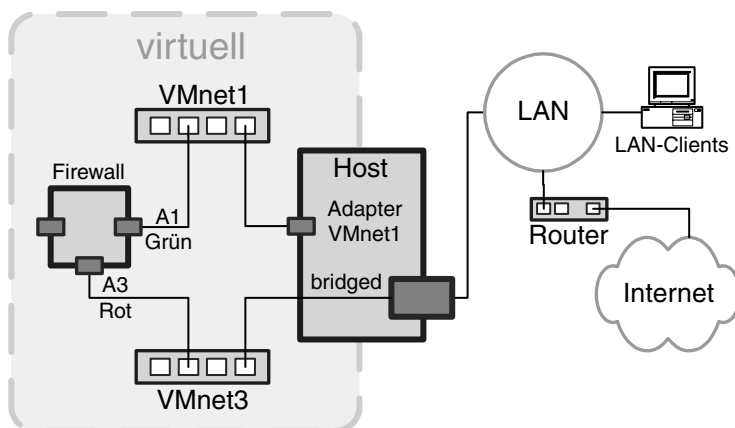


### Router und Firewall parallel im LAN betreiben (Testszenario)

#### Testen, ohne das LAN zu stören

Für einen bloßen Test sind all diese Änderungen im Netzwerk natürlich kaum durchzuführen. Aber es gibt eine Lösung, bei der Sie am Router und im LAN nichts verändern müssen. Der physische Router wird dabei von allen LAN-Clients weiterhin ohne Umwege verwendet, die Clients surfen sozusagen an IPCop vorbei (Abbildung 3.29). Parallel dazu kann IPCop den Router ebenfalls als Internet-Zugang und für die DMZ mitbenutzen, IPCop verhält sich dabei wie ein normaler LAN-Client. Der Host benutzt weiterhin den physischen Router als Internet-Zugang und greift nur zur Konfiguration über ein internes virtuelles Host-only-Netzwerk auf IPCop zu.

Abbildung 3.29:  
Zu Testzwecken  
kann die Firewall als  
normaler LAN-  
Client parallel zum  
restlichen Netzwerk  
auf den Router  
zugreifen



Die grüne Schnittstelle von IPCop (Adapter1) binden Sie dazu unter VMware über VM/SETTINGS/HARDWARE ans VMnet1 (Host-only). Die Konfiguration ähnelt damit der Ausbaustufe 1. Sie geben dem Host-Adapter *VMware Network Adapter VMnet1* die Adresse 192.168.1.2 mit Gateway und DNS auf die Adresse des grünen IPCop-Interface 192.168.1.1 (siehe auch Abbildung 3.24 weiter oben). Der Host kann dadurch über diesen virtuellen Adapter auf IPCop zugreifen, was der Ausbaustufe 1 ähnelt.

Den Unterschied zur Ausbaustufe 1 macht das rote Interface von IPCop (Adapter3 an VMnet3), dem Sie eine freie Adresse aus Ihrem physischen LAN mit Gateway- und DNS-Eintrag auf den physischen Router geben (siehe auch Abbildung 3.27 und Abbildung 3.28). Ihr physischer Host-Adapter bleibt ganz normal mit dem LAN verbunden. IPCop und Ihr Host kommunizieren über diesen Adapter als Clients im LAN. Für Ihren Host ändert sich an seiner LAN-Anbindung nichts. Unter HOST/VIRTUAL NETWORK SETTINGS/HOST VIRTUAL NETWORK MAPPING müssen Sie Ihren physischen Host-Adapter VMnet3 zuweisen (siehe auch Abbildung 3.11 weiter oben), VMnet0 wird nicht verwendet und kann auf *Bridged to an automatically chosen adapter* stehen bleiben.

Da der Host weiterhin über seine Netzwerkkarte im LAN angeschlossen ist, darf der virtuelle Adapter der grünen IPCop-Schnittstelle nur noch *Host-only* sein und muss einen freien Netzwerkbereich verwenden. Sollte Ihr LAN bereits den Bereich 192.168.1.x benutzen, dann müssen Sie für IPCop grün und den *VMware Network Adapter VMnet1* Adressen aus einem anderen Bereich verwenden, z.B. 192.168.7.x. Mit dieser Konfiguration hat IPCop Zugriff auf den Router und auf das Internet, wie jeder andere Client im LAN auch. IPCop verwendet den Router also parallel zu allen PCs im Netzwerk, der Router muss nicht umkonfiguriert werden. Der rote Adapter von IPCop ist allerdings nicht mehr direkt und abgeschottet mit dem Internet-Zugang verbunden. Sie können damit die DMZ sogar aus dem LAN testen.

Der physische Adapter für VMnet3 darf in dieser Testkonfiguration auch die Netzwerkkarte sein, über die der Host selbst am LAN hängt. Dann kann der Host weiterhin normal im LAN kommunizieren, und die Firewall-VM spricht parallel dazu über den gleichen Adapter mit dem Router. Aus Sicht des Routers sind das zwei völlig unterschiedliche Geräte. Damit können Sie den Workshop testweise auch von Ihrem normalen LAN-PC mit der VMware Workstation oder dem VMware Server nachvollziehen.



Wollen Sie mit dieser Konfiguration auch Ausbaustufe 3 (die DMZ) testen, dann müssen Sie auf dem physischen Router eine Portforwarding-Regel für Port 80 und 433 auf die LAN-Adresse des roten Interface von IPCop festlegen. Der Router leitet damit Anfragen aus dem Internet an IPCop weiter, und IPCop schickt wiederum diese Anfragen in die virtuelle DMZ. Hier sollten Sie allerdings sehr gut aufpassen, was Sie tun, weil Sie damit Anfragen aus dem öffentlichen Internet direkt ins interne LAN durchlassen. In einer produktiven Umgebung ist es sicherer, von einem internen Testplatz den Zugriff auf IPCop und die DMZ zu simulieren, dazu bietet sich sogar eine zusätzliche virtuelle Maschine an VMnet3 an.

Wollen Sie in dieser Konstellation vom Host aus nicht nur zur Konfiguration auf die IPCop-Firewall zugreifen, sondern auch auf Server in der DMZ, dann müssen Sie am Host eine explizite Route in die DMZ setzen (im Beispiel hat IPCop grün die 192.168.1.1). Geben Sie dazu an einer Eingabeeinforderung am Host-PC folgenden Befehl ein:

```
route add 192.168.2.0 mask 255.255.255.0
192.168.1.1 -p
```



## 3.5 Internet-Zugang der Firewall einrichten

Die grundlegende Infrastruktur haben Sie damit entsprechend Ihren Gegebenheiten aufgebaut. Es fehlt noch die Konfiguration des Internet-Zuganges.

### 3.5.1 Konfiguration mit dem Web-Interface von IPCop

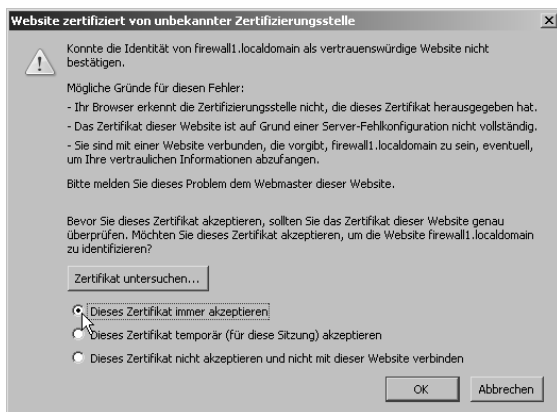
Die weitere Konfiguration der Firewall erfolgt mit IPCops Web-Interface, das Sie vom LAN oder vom Host aus bereits im Browser über die Adresse der grünen IPCop-Schnittstelle erreichen sollten:

*http://192.168.1.1:81*



Die Anmeldung am Web-Interface von IPCop funktioniert nur mit dem Nutzer *admin* und nicht als *root*!

Abbildung 3.30:  
Das Web-Interface  
von IPCop arbeitet  
mit einer SSL-  
Verbindung. Das  
Zertifikat können  
Sie akzeptieren



#### PPPoE oder Router

Nach dem Bestätigen des IPCop-Zertifikates im Browser konfigurieren Sie im Menüpunkt NETZWERK/EINWAHL die PPPoE-Verbindung des DSL-Modems zum Internet-Provider mit Ihren Zugangsdaten. Bei einer DSL-Flatrate können die Haken an *Verbinden bei IPCop-Neustart* und *Dauerhafte Verbindung* gesetzt werden. Unter SYSTEM/STARTSEITE lässt sich dann der Status der Verbindung prüfen bzw. mittels VERBINDEN ein Test durchführen (Abbildung 3.31).

Verwenden Sie einen Router, entfällt die Konfiguration der Zugangsdaten und auch der manuelle Verbindungsaufbau zum Testen, da diese Daten auf dem Router eingetragen sind. IPCop dient in diesem Fall nicht zum Aufbau der Internet-Verbindung, sondern ausschließlich nur als zusätzliche Firewall hinter dem Router.

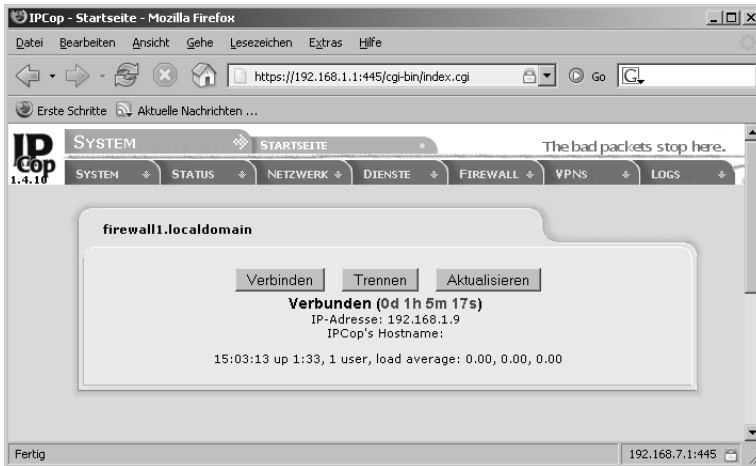


Abbildung 3.31:  
Die Startseite vom  
Web-Interface gibt  
einen schnellen  
Überblick über den  
Verbindungsstatus

Der Verbindungsaufbau erfolgt innerhalb weniger Sekunden. Wenn er fehlschlägt, sollten Sie überprüfen, ob Adapter 3 wirklich an die richtige physische Host-Netzwerkkarte zum DSL-Modem bzw. zum Router gebunden ist. Weiterhin sind unter LOGS/SYSTEMLOGDATEIEN/RED auch detaillierte Fehlermeldungen ersichtlich, etwa ein falsch eingegebenes Passwort.

### Log-Dateien

### 3.5.2 Einstellungen an den LAN-Clients

Nach erfolgter Zugangskonfiguration können Sie Ihre Firewall bereits als sicheren Internet-Zugang verwenden. Dazu ist bei Ausbaustufe 2 auf dem Host und an den LAN-PCs als Default-Gateway sowie als DNS-Server die grüne IPCop-Adresse (im Beispiel 192.168.1.1) einzutragen (siehe auch Abschnitt 3.4.4, „Verwendung eines Routers am roten Interface von IPCop“). Für die Ausbaustufe 1 (kein LAN) müssen Sie das nur im VMware Network Adapter VMnet1 auf dem Host tun. Funktioniert alles, ist es wieder Zeit, für einen Snapshot den Konfigurationsstand zu sichern.

### DNS und Default-Gateway

Alle Nutzer können jetzt über die Firewall auf das Internet zugreifen, ohne dass Würmer wie Sasser oder Blaster, die Sicherheitslücken schon bei einer bloßen Verbindung zum Internet ausnutzen, zur Gefahr werden. Wichtig ist das vor allem, wenn das DSL-Modem ohne Router ungesichert an der Leitung angeschlossen ist. Auch Hackern bleibt der direkte Weg verwehrt. Natürlich macht eine Firewall keinen Virenschutz auf den Clients überflüssig und regelmäßige Sicherheitsupdates bleiben weiterhin Pflicht.

## 3.6 Die Server in der DMZ installieren

Bei der Konfiguration und Einrichtung der virtuellen Server in der DMZ beschränke ich mich auf die grundlegende Netzwerkfunktionalität. Als potenzielle Server kommen verschiedenste Konfigurationen in Frage, auf die ich hier unmöglich eingehen kann. Ob Linux mit Apache oder Windows mit IIS verwendet wird, ist nicht von Bedeutung, wenn man die Netzwerkkonfiguration durchschaut. Auch ein Terminalserver oder ein Windows XP Professional mit Remote-Desktop können in der DMZ laufen. Genauso lässt sich ein Mailserver betreiben.

### 3.6.1 Netzwerkkonfiguration in der DMZ

Nach so viel Schweiß bei der Konfiguration der Firewall ist der Ausbau der DMZ einfach. Die virtuellen Server in der DMZ benötigen jeweils nur eine einzige virtuelle Netzwerkkarte mit der Einstellung *Custom* an *VMnet2* (Abbildung 3.9). Sie müssen mit IP-Adressen aus dem Netz 192.168.2.x und mit dem Default-Gateway 192.168.2.1 konfiguriert werden.

Vom LAN oder vom Host-PC aus sollten Sie einen Server in der DMZ dann bereits mittels Ping erreichen. Maschinen in der DMZ können allerdings kein Ping ins LAN oder zum Host senden, das ist normal. Schließlich soll ein Hacker, der den Webserver geentert hat, in keiner Weise auf das Firmen-LAN zugreifen können.



Auch ins Internet blockt IPCop aus der DMZ ein Ping. Zum Verbindungstest von einem Server aus der DMZ ins Internet können Sie als Ersatz ein `telnet` auf *port 80* eines bekannten Webserverns verwenden:

```
telnet www.vmware.com 80
```

Im erscheinenden schwarzen Bildschirm geben Sie den Befehl `quit` oder `get` ein, dabei sollten ein paar wirre Zeilen HTML-Code des angesprochenen Webserverns ausgegeben werden.

### 3.6.2 Zugriff auf die DMZ vom Internet aus zulassen

#### Portweiterleitung

Für den Zugriff vom Internet auf einen Webserver innerhalb unserer DMZ können Sie im Web-Interface von IPCop unter **FIREWALL/PORTWEITERLEITUNG** Weiterleitungen für die TCP-Ports *80* und *443* konfigurieren. Das Ziel ist die IP-Adresse 192.168.2.x des Servers in der DMZ (Abbildung 3.32). Dadurch reicht IPCop alle Pakete, die an die

genannten Ports der öffentlichen IP-Adresse adressiert sind, nach innen in die DMZ zum Webserver durch. Alle anderen Verbindungsversuche aus dem Internet blockiert die Firewall.

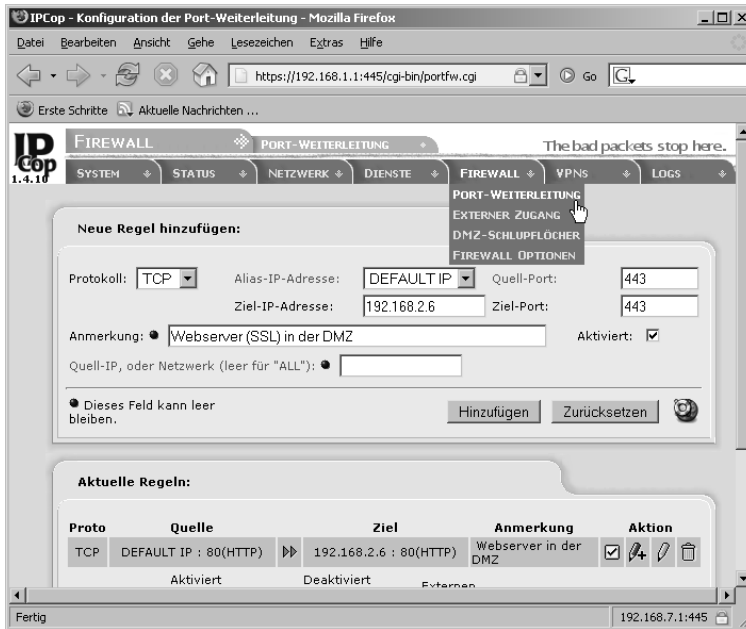


Abbildung 3.32:  
Um vom Internet  
aus Server in der  
DMZ anzuspre-  
chen, müssen expli-  
zite Ports weiterge-  
leitet werden

Wenn IPCop nicht direkt an ein DSL-Modem angeschlossen ist, sondern an einen Router, muss bereits der Router die entsprechenden Ports an IPCop weiterleiten.



Sollte ein Hacker einen Server auf einem der geöffneten Ports knacken, dann gelangt er aus der DMZ im VMnet2 trotzdem nicht ins grüne Netzwerk. Friedliche Nutzer aus dem grünen Netz können den Webserver aber jederzeit für Wartungszwecke oder zum Datenaustausch erreichen.

**Hacker bleiben  
draußen**

### 3.6.3 DynDNS für DSL-Anschlüsse ohne feste IP-Adresse einrichten

Wenn Sie nicht über eine Standleitung mit fester IP-Adresse als Internet-Zugang verfügen, dann gelingt ein Verbindungsaufbau mit einem Server in der DMZ noch nicht. Woher soll der potenzielle Besucher des Webserver die dynamisch zugeteilte IP-Adresse des DSL-Zugangs kennen?

### Wie funktioniert DynDNS?

Wenn IPCop eine neue DSL-Verbindung aufgebaut hat, bekommt er automatisch eine neue IP-Adresse vom Provider. Zusätzlich werden die meisten DSL-Zugänge auch bei einer Flatrate einmal am Tag kurz getrennt. Bei erneuter Verbindung wechselt dann wieder die IP-Adresse. IPCop übermittelt die neue Adresse automatisch an den Server des DynDNS-Anbieters. Dort wird die Adresse in einer DNS-Datenbank einer von Ihnen reservierten Sub-Domain zugewiesen, z.B. *mein-server.dyndns.com*. Unter dieser Adresse ist jetzt der DSL-Anschluss, und damit der Server in der DMZ, jederzeit erreichbar, solange IPCop die neuen IP-Adressen beim Anbieter immer wieder aktualisiert.

Arbeiten Sie mit einem Router, dann sollte dieser das Handling von DynDNS beherrschen, weil er die öffentliche dynamische IP-Adresse vom Provider bekommt. Notfalls gibt es separate Programme, die auf einem Client im LAN installiert werden können und welche die Aktualisierung des DynDNS-Eintrages übernehmen. Beispiele dafür sind DirectUpdate oder RouterControl.

*[www.directupdate.net](http://www.directupdate.net)*

*[www.routercontrol.de](http://www.routercontrol.de)*

#### Dynamische IP-Adresse auflösen

Zwar können Sie die vom Provider zugeteilte IP-Adresse zum Testen der Konfiguration vorerst im Web-Interface von IPCop anschauen. Unter SYSTEM/STARTSEITE wird sie bei aktiver Verbindung angezeigt (Abbildung 3.31). Für eine permanente Erreichbarkeit sollten Sie sich aber eine Sub-Domain bei einem Weiterleitungsdienst, wie z.B. DynDNS, registrieren. IPCop unterstützt eine ganze Liste der üblichsten Anbieter. Im Menü DIENSTE/DYNAMISCHER DNS können Sie die Parameter konfigurieren, und mit AKTUALISIERUNG ERZWINGEN können Sie die Funktion testen. Im Abschnitt *IPCop* der Log-Dateien sollte dann ein ähnlicher Eintrag wie folgender erscheinen:

```
Dynamic DNS ip-update for mein-server.dyndns.com:
success
```

Wenn Sie jetzt von irgendeinem beliebigen PC mit Internetzugang ein Ping auf Ihren registrierten Hostnamen (z.B. *mein-server.dyndns.com*) machen, dann sollte die Adresse ordentlich aufgelöst werden, und Sie sehen die derzeitige IP-Adresse Ihres DSL-Zuganges.

### 3.7 Abschließende Einstellungen am Host und an den VMs

Mit abschließenden Snapshots aller VMs sichern Sie den erreichten Stand der Firewall und der Server in der DMZ. Zusätzlich kann VMware Workstation 5 alle VMs als ein Team zusammenfassen, um sie auf Knopfdruck gemeinsam zu starten oder zu beenden.

**Snapshots,  
Teams**

Für die VMs in der DMZ, etwa den Webserver, können Sie mehrere virtuelle Platten verwenden; mindestens eine für das System und eine zusätzliche im Modus *Independent Persistent* nur für die Daten. Mit einem *Revert* lässt sich somit eine Beschädigung des Systems wieder rückgängig machen, ohne Daten auf der Persistent-Platte zu verlieren. Weitere Hinweise zu Snapshots und Platten finden Sie in *Teil 3, Kapitel 4, „Die Snapshot- und Clone-Funktion der VMware-Produkte“*.

**Wichtige Daten  
und Snapshots**

Beim VMware Server können Sie in der Server-Konsole unter VM/SETTINGS/OPTIONS/STARTUP SHUTDOWN den automatischen Start der VMs beim Hochfahren des Host-PC und ein automatisches Herunterfahren vor dem Abschalten des Hosts einstellen. Nützlich ist das z.B. bei angeschlossener USV-Steuerung (*USV – Unterbrechungsfreie Stromversorgung*). Dazu muss ein Anmeldekonto hinterlegt werden, unter dem der Gast auf dem Host-System dann als Dienst startet (Abbildung 3.33). Dadurch laufen die Gäste unabhängig davon, ob ein Nutzer am Host angemeldet ist.

**Autostart und  
USV-Steuerung**

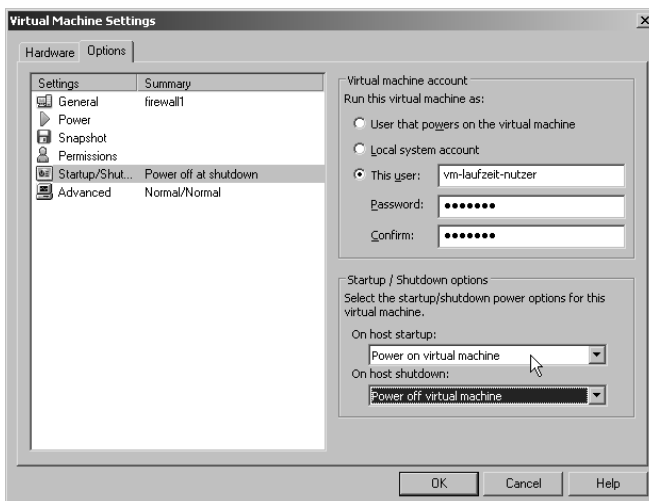


Abbildung 3.33:  
Damit VMs am  
Server als Dienst  
laufen, kann ein  
Nutzerkonto hinter-  
legt werden. Damit  
wird auch ein Auto-  
start möglich

Ebenfalls beim Server ist eine Steuerung des Zugriffs auf die virtuellen Maschinen mittels Dateirechten unbedingt zu empfehlen. Damit können nur berechtigte Nutzer die VMs bedienen, verändern oder löschen. Mehr zur Rechteverwaltung finden Sie in *Teil 3, Kapitel 5, „Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs“*.

**Rechte**



## 3.8 Ausblick auf die Möglichkeiten von Ausbaustufe 4 der DMZ

Sie können jetzt weitere VMs in der DMZ installieren. Auch die Netzwerkeinstellungen von VMware bieten noch einiges zum Experimentieren. Zusätzlich verfügt IPCop über weitere interessante Funktionen, mit denen Sie die Möglichkeiten der DMZ voll ausreizen können. Komplette Anleitungen würden den Umfang des Buches allerdings sprengen und haben auch nichts mehr vordergründig mit virtuellen Maschinen zu tun. Deshalb möchte ich Ihnen nur einige Anregungen geben.

### 3.8.1 Beispiele für den weiteren Ausbau der DMZ

#### Mailserver in der DMZ

Ein weiteres Paradebeispiel neben dem Webserver ist ein Mailserver in der DMZ. Vom Internet aus muss nur der SMTP-Port 25 für eingehende Mails in die DMZ weitergeleitet werden. Nutzer aus dem LAN können problemlos, z.B. mittels POP3, auf Ihre Mailkonten zugreifen. Potenzielle Angreifer kommen aus der DMZ aber nicht ins LAN.

#### Terminalserver in der DMZ

In der DMZ kann als Server auch ein virtueller Terminalserver oder im einfachsten Falle ein Windows XP Professionell mit aktiviertem Remotedesktop laufen. Damit kann ein Außendienstmitarbeiter jederzeit von jedem Ort der Welt auf bestimmte Anwendungen, wie Kundenadressen, zugreifen. Problematisch ist nur der Datenaustausch mit dem LAN, weil dazu Ports geöffnet werden müssten, über die aus der DMZ ins LAN zugegriffen werden kann. Am sichersten bleibt eine abgeschottete Lösung in der DMZ, wobei die Daten nur vom LAN aus zyklisch mit dem Server in der DMZ aktualisiert werden.

#### SSH-Tunnel in die DMZ oder ins LAN

Im einfachsten Falle könnte man für das Beispiel eines Terminalservers eine Portforwarding-Regel für den RDP-Port 3389 in IPCop einrichten (RDP, *Remote Desktop Protocol* – das Protokoll, das Terminalserver- und Remotedesktop-Verbindungen verwenden). Damit ist unser Rechner in der DMZ auf diesem Port aber unkontrolliert erreichbar, und der gesamte RDP-Verkehr wird im Internet übertragen. Um den Zugang sicherer zu machen, sollte der Zugriff über ein VPN oder über einen SSL-Tunnel erfolgen.

#### Citrix Secure Gateway

Ein professionelles Produkt für genau diesen Einsatzzweck wäre z.B. das Secure Gateway der Firma Citrix. Damit kann über einen SSL-Tunnel das ICA-Protokoll (*ICA, Independent Computing Architecture* –

das Protokoll, das Citrix u.a. für seine Terminalserververbindungen verwendet) sicher im Internet transportiert werden. Weil die Kommunikation ausschließlich über den Port 443 erfolgt, der auch von Webservern verwendet wird, funktioniert das sogar über Proxy-Server und durch die meisten Firewalls hindurch ([www.citrix.com](http://www.citrix.com)).

Es geht aber auch einfacher. Im Web-Interface von IPCop können Sie unter SYSTEM/SSH-KONFIGURATIONSSSEITE/SSH ZULASSEN den SSH-Zugriff auf Port 222 freischalten und die TCP-WEITERLEITUNG zulassen. Der frei verfügbare SSH-Client *Putty* kann eine Verbindung in die DMZ aufbauen, über die sich jedes Protokoll, z.B. RDP, auf einen Rechner in der DMZ (oder auch direkt ins LAN) tunneln lässt. Es gibt diverse HowTos zum Thema SSH-Tunnel mit IPCop im Internet, z.B. [ipcop.gutzeit.ch/pdf/ssh\\_lan.pdf](http://ipcop.gutzeit.ch/pdf/ssh_lan.pdf). Zusätzlich bietet IPCop auch VPN-Funktionalität.

**SSH mit IPCop und Putty**

### **3.9 Sicherheit – sind Löcher in der VM möglich?**

Zum Abschluss taucht natürlich die Frage auf, wie sicher eine virtuelle DMZ ist. Sicherheitslücken werden immer wieder entdeckt, egal ob in einer teuren Hardware-Firewall oder in einer Software-Lösung wie IPCop oder ISA-Server. Der Unterschied zu einer physischen Firewall ist die Isolation des Systems.

Sollte ein Angreifer einen der Server in der virtuellen DMZ oder gar die Firewall-VM selbst übernehmen, dann ist die letzte Barriere die Sandbox der virtuellen Maschine. Als *Sandbox* (engl. für Sandkasten) wird ein abgeschotteter Bereich bezeichnet, in dem eine Applikation zwar vollen Zugriff hat, ohne diese Umgebung jedoch verlassen zu können. Im Gegensatz zu einem echten isolierten Hardware-Rechner befindet sich der Angreifer in einer VM schon auf dem Host-System, parallel zu anderen VMs. Wenn es ihm gelingen sollte, aus der virtuellen Maschine auszubrechen, kann er theoretisch den Host und auch andere Gäste kompromittieren oder sogar übernehmen. Steht der Host direkt im Firmen-LAN, dann ist der Angreifer auch gleich am Ziel. Sicherheitslücken der Emulationssoftware, wie mögliche Buffer Overflows, kommen somit zusätzlich zu den Risiken hinzu, die offene Ports und öffentliche Server im Internet sowieso schon darstellen.

**Sandbox oder Hardware?**

Bisher sind keine Schwachstellen im Virtualisierungslayer der Produkte oder im *VMware Bridge Protocol* bzw. in Microsofts *Virtual Machine Network Services* bekannt. Allerdings wurde im NAT-Netzwerk von VMware (das im Projekt nicht verwendet wird) bereits eine Möglichkeit zu Buffer-Overflow-Attacken gefunden. Diese Lücke wurde vom Hersteller aber schnell geschlossen.

**Buffer Overflow**

**Restrisiko** Ein Hacker oder ein Virus muss auf jeden Fall bewusst auf virtuelle Maschinen testen und Schwachstellen ausnutzen. Die Emulationssoftware darf keine Schwachstellen aufweisen. Wenn doch, müssen diese vom Hersteller schnellstens behoben werden, dann ist die virtuelle DMZ fast gleichwertig zu physischen Rechnern. Ob Sie das Restrisiko tragen wollen, hängt von der Sicherheitsstufe Ihrer Anwendungen ab!



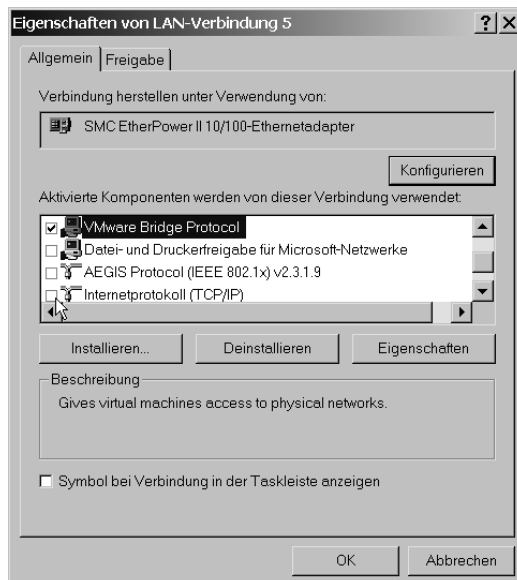
Dieser Workshop ist als Test- und Lernumgebung konzipiert. Vor einer Anwendung für sicherheitsrelevante Umgebungen muss ich ausdrücklich warnen!

### 3.9.1 VMs in der DMZ optimal isolieren

Um die VMs optimal zu isolieren, sind zusätzlich noch folgende Tipps zu empfehlen:

- An der physischen Netzwerkkarte zum DSL-Modem bzw. Router ist am Host nur das *VMware Bridge Protokoll* oder bei Microsoft das Protokoll *Virtual Machine Network Services* zu binden. Nichts anderes, auch kein TCP/IP (Abbildung 3.34)! Dadurch ist der Router oder das DSL-Modem ausschließlich mit der virtuellen Maschine verbunden und bleibt isoliert.

Abbildung 3.34:  
Um die Netzwerkkarte zum Internet dediziert der Firewall zuzuweisen, müssen alle Protokolle auf dem Host entbunden werden



- Überprüfen Sie die Bindungen nach Änderungen der Netzwerkkonfiguration am Host. In manchen Konstellationen fügt Windows einfach selbstständig die Bindung von TCP/IP wieder allen Adaptern hinzu.

- ▶ In der Konfiguration der virtuellen Maschinen sollten Sie unter VMware Workstation bei VM/SETTINGS/OPTIONS die *Shared Folders* und alle Optionen unter GUEST ISOLATION abschalten.
- ▶ Im Disketten- und CD-ROM-Laufwerk kann die Option *Connect at power on* deaktiviert werden.
- ▶ Zusätzlich können Sie unter EDIT/PREFERENCES/INPUT noch *Copy&Paste* generell unterbinden.
- ▶ Benötigen Sie zu den VMs in der DMZ keinen permanenten Zugriff aus dem LAN, dann können Sie einen dedizierten Host ohne LAN-Anbindung ausschließlich als DMZ laufen lassen. Dieser Rechner verfügt nur über ein einziges Patch-Kabel zum Modem bzw. zum Router. Vom Host aus können Sie über einen virtuellen Host-Adapter (VMnet1) zu Wartungszwecken auf die DMZ zugreifen. Damit ist der gesamte Host samt virtueller DMZ physisch vom LAN isoliert.

Höchste Sicherheitsstufe

### 3.10 Umsetzung mit Microsoft Virtual PC 2004/2007 und Virtual Server 2005 R2

Die virtuelle Firewall lässt sich auch problemlos unter den Produkten von Microsoft realisieren. Dazu sollten Sie folgende Hinweise beachten.

#### Linux (IPCop) in Gästen unter Microsoft betreiben

Linux wird seit Microsoft Virtual Server 2005 R2 von Microsoft in einer VM offiziell unterstützt. Aber auch in allen anderen Versionen, z.B. Virtual PC 2004, läuft der Pinguin ohne Probleme. Der Installation von IPCop in einer VM unter Virtual PC/Server steht damit nichts im Wege. Als Alternative kann auch der Microsoft ISA Server dienen.

#### Netzwerkconfiguration der DMZ

Für die im Workshop verwendeten VMware-Anschlusstypen der virtuellen Netzwerkkarten können Sie folgende Konfigurationen verwenden (beachten Sie zum Überblick auch Tabelle 3.1):

- ▶ **Adapter1** – Für Ausbaustufe 2 mit LAN-Anbindung ist die Umsetzung einfach. In den Einstellungen der VM wird beim Adapter 1 aus der Liste einfach die physische Netzwerkkarte ausgewählt, die am LAN angeschlossen ist (externes Netzwerk).

Für Ausbaustufe 1 ohne LAN ist wieder eine Verbindung vom Host zur VM ohne physische Netzwerkkarte notwendig. Ähnlich dem Host-only-Netzwerk von VMware wird das mit dem *Microsoft Loopback-Adapter* erreicht. Dieser muss allerdings erst auf dem Host installiert werden (siehe Teil 3, Kapitel 2). An diesen Adapter

müssen Sie manuell unter den Netzwerkeinstellungen des Host-PC das Protokoll *Virtual Machine Network Services* und zusätzlich TCP/IP binden. Auf dem Host erhält der *Microsoft Loopback-Adapter* dann die IP-Adresse 192.168.1.2 mit Gateway und DNS auf die 192.168.1.1 (IPCop grün).

- ▶ **Adapter2** – Bei Virtual Server ist ein so genanntes *internes Netzwerk* genauso isoliert wie ein *not bridged VMnet* unter VMware. Unter Virtual PC dient der Modus *nur lokal* zur Isolation aller Gäste in der DMZ.
- ▶ **Adapter3** – Zum Verbinden der virtuellen Netzwerkkarte mit der physischen Netzwerkkarte zum DSL-Modem oder Router wird der entsprechende Host-Adapter (unter Virtual Server *external Network*) einfach aus der Liste beim virtuellen Adapter3 ausgewählt. Er bildet damit das rote Netz und ist direkt am Internet angeschlossen.

So können Sie nun den gesamten Workshop einfach in die Sprache von Microsoft Virtual PC 2004 und Virtual Server 2005 R2 übersetzen.

# 4 Linux-Host mit VMware Server und Integration ins Windows-Netz

Sie setzen den kostenlosen VMware Server auf einer Linux-Basis auf. Damit erhalten Sie eine stabile und etablierte Virtualisierungslösung zum Nulltarif – für Test, Schulung, Entwicklung und auch für Produktionsumgebungen. Die Bedienung erfolgt hauptsächlich vom Windows-Client aus, Basiswissen für die Linux-Verwaltung vermittelt der Workshop. Für den produktiven Einsatz sollten zur Sicherheit Linux-Kenntnisse vorhanden sein.

**Auch für Linux-Neulinge**

## Workshop im Überblick

### Hauptprodukt

- ▶ VMware Server auf Linux-Basis (Debian oder SUSE)
- ▶ Bedienung erfolgt vom Windows-Client aus

### Praktische Verwendung

- ▶ Stabile Basis für eine Vielzahl von Virtualisierungsanwendungen
- ▶ Test- und Pilotumgebung
- ▶ Produktive Server virtualisieren
- ▶ Dedizierter Host für die virtuelle DMZ in *Teil 2, Kapitel 3*

### Schwerpunkte

- ▶ Linux als Host-System, VMware unter Linux installieren
- ▶ Komfortable Anbindung an die Windows-Welt
- ▶ PAE, Kernel kompilieren, Probleme unter Linux lösen

### Zielgruppe

- ▶ Alle IT-Abteilungen
- ▶ Ambitionierte Laien und Privatanwender

## 4.1 VMware unter Linux als kostenlose Einstiegslösung

**Kostenfrage** So manches Virtualisierungsprojekt scheitert gerade im Mittelstand an der Kostenfrage. Als Einstiegslösung stellt VMware aber eine komfortable, stabile und praxisbewährte Plattform zur Verfügung, die nicht gleich das Controlling schockt – der kostenlose VMware Server. Dessen Installation ist auf einem Windows-Host völlig unkompliziert und nicht der Rede wert. Wie Sie auch einen schlanken Linux-Host ins Windows-Netzwerk integrieren und damit sogar die Host-Lizenz sparen, beschreibt dieser Workshop.

Ein Linux-Host lohnt sich vor allem dann, wenn auf vorhandenen 32-Bit-Systemen mehr als 4 GB RAM mittels PAE (*Physical Address Extension*) genutzt werden sollen, was neben Linux nur der teure Windows Server 2003 unterstützt. Beachten Sie allerdings in diesem Zusammenhang auch das vereinfachte Lizenzierungsmodell von Microsoft für virtuelle Maschinen, das unter bestimmten Voraussetzungen den Betrieb von bis zu fünf Windows-Instanzen mit einer Enterprise Edition-Lizenz ermöglicht und den Aufpreis damit relativieren kann (siehe Teil 1, Kapitel 3, „Installation und Konfiguration der einzelnen Produkte“).

**Mut zum Einstieg!** Für bis zu zehn laufende virtuelle Maschinen, je nach Auslastung und Hardware, bietet die hier im Workshop vorgestellte Lösung durchaus Platz, für eine zentrale Test- oder Schulungsumgebung oder produktiv. Und der überschaubare Aufwand macht Mut zum Einstieg. Später ist die Lösung jederzeit mit dem ESX Server bis auf Datacenter-Niveau ausbaufähig, alle VMs lassen sich unkompliziert übernehmen.

## 4.2 Beschreibung des Projekts

**Pilotumgebung, Schulung oder produktiv** Wenn Sie den Produktivbetrieb noch scheuen, können Sie sich in einer Pilotumgebung stressfrei von allen Vorteilen der Virtualisierung überzeugen. An virtuellen Kopien Ihrer Produktionsserver lassen sich Migrationen, Updates und neue Software originalgetreu mit Benutzerkonten und Daten testen, inklusive virtueller Clients. Das geschieht völlig abgeschottet ohne Risiko für die heiße Produktionsumgebung. Ganz nebenbei lernen Sie so das Konzept virtueller Maschinen kennen und machen sich mit deren Bedienung vertraut. Auch in einer Schulungsumgebung kann der Host als zentraler Server einige Schüler bedienen.

Genauso ist die produktive Virtualisierung von File- und Printservern oder von Diensten wie Domänencontrollern, DHCP, DNS und Lizenzierungsservern möglich. Nicht zuletzt finden ganze Intranet- und Groupware-Lösungen von fünf bis 500 Mitarbeitern Platz im neuen virtuellen Zuhause.

### 4.2.1 Windows-Integration des Linux-Hosts

Das Ziel dieses Workshops ist der Aufbau eines kompakten Linux-Hosts mit dem VMware Server, ohne X und GUI, also ohne grafische Benutzeroberflächen wie KDE oder GNOME. Der Verzicht auf eine grafische Oberfläche macht das System schlank und genügsam, weniger fehleranfällig und für den Linux-Laien unkomplizierter.

Die Bedienung erfolgt komfortabel vom Windows-Client aus über die VMware Server Console und über das Web-Interface. Wenige zusätzliche Tools, wie Samba, ermöglichen einen unkomplizierten Zugriff auf die Dateien der VMs. So integriert sich der Server in eine Windows-Umgebung auch für in Linux unerfahrene Anwender.

**Komfortable  
Bedienung vom  
Windows-Client**

Bevor Sie mit dem produktiven Betrieb beginnen, sollten Sie allerdings erst einige Erfahrungen sammeln. Wenn Sie den Schritt mit Linux nicht wagen wollen, dann bleibt immer noch die Installation auf einem Windows-Host, VMs lassen sich unkompliziert übernehmen.



### 4.2.2 Debian als Host-System

Die freie Linux-Distribution Debian hat sich vor allem im Serverbereich als sehr stabile Plattform einen Namen gemacht. Dazu kommt das komfortable und ausgereifte Paketmanagement, mit dem notwendige Module ganz einfach direkt von CD oder aus dem Internet nachinstalliert werden können. Dadurch entsteht eine sehr schlanke Installation. Debian gehört zwar nicht zu den von VMware empfohlenen Host-Betriebssystemen, eignet sich aber trotzdem sehr gut als Basis. Der Workshop steht damit exemplarisch als Beispiel für die Verwendung anderer Linux-Distributionen.

### 4.2.3 SUSE als unterstütztes Host-System

Wenn Sie bereits eine Version von SUSE Linux besitzen, sollten Sie diese verwenden, vor allem auf 64-Bit-Hardware. SUSE Linux wird von VMware offiziell als Host-System unterstützt. Ich gehe in einem eigenen Abschnitt auf die Installation unter SUSE Linux ein (siehe Abschnitt 4.10, „Installation des VMware Servers unter SUSE Linux“). Bis auf die Möglichkeit der Installation mit RPM-Paketen bleibt das vorgestellte Konzept grundlegend gleich und kann sowohl mit Debian als auch mit SUSE umgesetzt werden.



## 4.3 Vorbereitung der Installation des Host-Systems

Vor der Installation des Hosts sind noch einige Vorbereitungen zu treffen, z.B. die Software zu besorgen und Hardware einzubauen.

### 4.3.1 Hardware-Voraussetzungen für den Host

Grundsätzliches zu den Hardware-Voraussetzungen finden Sie in *Teil 1 des Buches*. Achten Sie vor allem darauf, dass bereits alle Controller und Netzwerkkarten im Server vor der Linux-Installation eingebaut sind. So kann das Setup diese gleich automatisch erkennen und einbinden, und Sie müssen das nicht nachträglich tun.

### 4.3.2 Benötigte Software für die komplette Installation von Debian und VMware

Alle Links zu den Downloads finden Sie am Ende des Workshops unter *Abschnitt 4.11, „Links zur benötigten Software“*. Da sich die aktuellen Versionen ändern, ersetzen Sie die Namen der Pakete im Text mit Ihren aktuellen Downloads.

#### Die Debian-Distribution herunterladen

Der Server wird mit dem Stable-Release (Sarge) in der Version 3.1 mit Kernel 2.6.8 installiert. Es genügt das Herunterladen einer minimalen Netzeinstellung, *netinst-Images* genannt. Das bootfähige ISO-Image ist kaum größer als 100 MB. Es enthält die notwendigsten Pakete zur Installation. Einige Dinge werden Sie später direkt aus dem Internet nachinstallieren. Wenn Sie keinen schnellen Internet-Zugang besitzen, sollten Sie sich die kompletten Debian-DVDs besorgen oder etwas Geduld mitbringen.

#### 64-Bit-Hardware als Host

VMware unterstützt zwar 64-Bit-Hosts, ist aber keine native 64-Bit-Anwendung. Wählen Sie deshalb *i386* als Architektur der Debian-Distribution, auch wenn Sie über 64-Bit-Hardware verfügen. Eine 64-Bit-Installation mit Debian ist für Einsteiger als VMware-Basis nicht zu empfehlen, da einige 32-Bit-Bibliotheken und Anpassungen am System notwendig sind.

Die *i386*-Distribution von Debian läuft auch auf 64-Bit-Hardware problemlos. Wenn Sie einen 64-Bit-Kernel verwenden wollen, sollten Sie zu SUSE greifen, um Problemen aus dem Weg zu gehen (siehe auch *Abschnitt 4.10, „Installation des VMware Servers unter SUSE Linux“*). Wer sich dennoch an 64-Bit-Debian versuchen will, findet hier eine Anleitung:

<http://blog.robinz.info/archives/2006/03/17/install-vmware-server-on-debian-amd64em64t/>

## VMware Server herunterladen

Die Installationspakete von VMware benötigen Sie für Debian als TAR-Archive. Unter Linux gibt es getrennte Installationen für den eigentlichen Server und für das VMware Management Interface (Web-Interface).

- ▶ Server: *VMware-server-XXX.tar.gz*
- ▶ Web-Interface: *VMware-mui-XXX.tar.gz*

## Any-Any-Patches zur Anpassung an verschiedene Distributionen

Linux ist leider mittlerweile alles andere als ein einheitliches System. Eine Vielzahl von Distributionen läuft langsam, aber sicher immer weiter auseinander. So gibt es auch bei der VMware-Installation immer wieder Probleme mit kleineren Unverträglichkeiten.

**Unverträglichkeiten beheben**

Der so genannte *Any-Any-Patch* des VMware-Kenners Petr Vandrovec behebt Probleme verschiedener nicht unterstützter Distributionen mit VMware. In manchen Versionen laufen z.B. Linux-Gäste mit Kernel 2.6 auf Hosts mit Kernel 2.6 ohne den Patch teilweise zu langsam. Manchmal funktioniert schon die Installation von VMware ohne den Patch nicht richtig. Mit der aktuellen Version des VMware Servers wird der Patch zwar nicht mehr benötigt. Sollten aber irgendwann mit folgenden Versionen wieder Probleme hinzukommen, dann kann der Patch Ihnen vielleicht helfen, und es ist gut zu wissen, wo es ihn gibt.

- ▶ Any-Any-Patch: *vmware-any-any-updateXXX.tar.gz*

Installieren Sie VMware immer ohne den Patch. Sollten Probleme auftreten, können Sie die Updates jederzeit nachträglich mit einer Neuinstallation einspielen.



## 4.4 Installation von Debian Linux als Basis auf der Hardware

Nach dem Herunterladen und Brennen des Debian ISO-Images erfolgt die einfache Linux-Installation in weniger als 15 Minuten.

### 4.4.1 Grundinstallation von Debian auf dem Host

Nach dem Booten von der gebrannten CD bleibt der Installer in einer Eingabeaufforderung stehen. Starten Sie die Installation bitte nicht gleich mit `←`, sondern mit dem Befehl `linux26`. Dadurch wird die modernere Kernel-Version 2.6 installiert und nicht die Version 2.4 (Abbildung 4.1).

Abbildung 4.1:  
Mit dem Kommando  
linux26 wird die  
Kernel-Version 2.6  
installiert



Die Debian-Installation erklärt sich von selbst. Neben den Spracheinstellungen werden zu Beginn Rechnername und Domäne abgefragt. Als Domäne genügt z.B. *local*.

**Partitionierung der Festplatten im Host**

Einzig und allein bei der Partitionierung sollten Sie eingreifen. Für eine Pilotumgebung muss man es nicht unnötig kompliziert machen, folgende Aufteilung ist ausreichend (Tabelle 4.1):

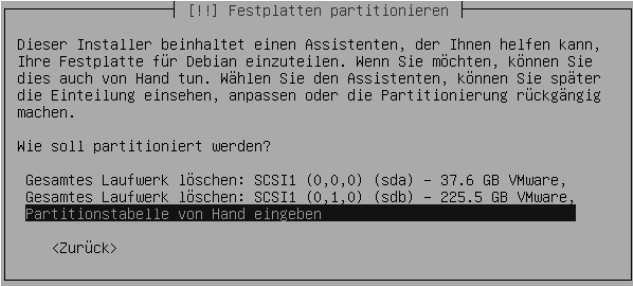
Tabelle 4.1:  
Eine einfache Parti-  
tionierung für ein  
Pilotsystem

| Mountpoint    | Dateisystem | Größe                           |
|---------------|-------------|---------------------------------|
| /             | ext3        | 10 GB                           |
| Swap          | Swap        | mindestens das doppelte des RAM |
| /vmaschinen01 | ext3        | gesamter Rest für die VMs       |



Die Partition */vmaschinen01* für die virtuellen Maschinen bringen Sie aus Performancegründen wenn möglich auf einem gesonderten Plattensystem unter.

Abbildung 4.2:  
Wählen Sie eine  
manuelle Partitio-  
nierung



Folgende Schritte sind für eine manuelle Partitionierung notwendig:

1. Wählen Sie im ersten Bildschirm PARTITIONSTABELLE VON HAND EINGEBEN, und drücken Sie  (Abbildung 4.2).
2. Wählen Sie im nächsten Bildschirm die erste Festplatte aus, auf der das System liegen soll, und drücken Sie .
3. Lassen Sie eine neue leere Partitionstabelle schreiben.
4. Wählen Sie den entstandenen freien Speicher mit .
5. Wählen Sie EINE NEUE PARTITION ERSTELLEN. Als Platz genügen 2–10 GB. Verwenden Sie nicht den gesamten Platz, sondern lassen Sie noch Raum für die Swap-Partition!
6. Als Typ ist *Primär* richtig, und die Partition gehört an den Anfang des freien Speichers.

**Systempartition erstellen**

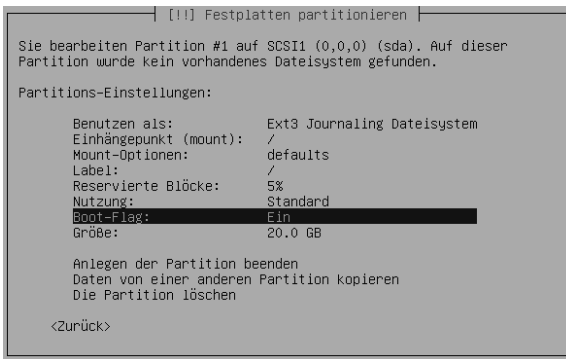


Abbildung 4.3:  
Die erste Partition  
für das Betriebs-  
system

7. Der EINHÄNGEPUNKT (MOUNT) ist / für die Wurzel (Abbildung 4.3).
8. Setzen Sie das Bootflag (Abbildung 4.3), und als Filesystem lassen Sie Sie *ext3*.
9. Schließen Sie ab mit ANLEGEN DER PARTITION BEENDEN.

Jetzt ist noch eine Partition für die Auslagerungsdatei anzulegen:

**Swap-Partition erstellen**

1. Wiederholen Sie die Schritte auf dem restlichen freien Speicher, und legen Sie eine Partition vom Doppelten Ihrer RAM-Größe an.
2. Unter BENUTZEN ALS machen Sie diesen Plattenbereich zur Swap-Partition (Abbildung 4.4).

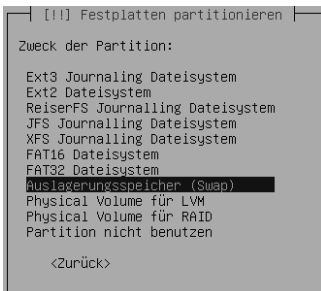


Abbildung 4.4:  
Die zweite Partition  
ist für die Auslage-  
rungsdatei reser-  
viert

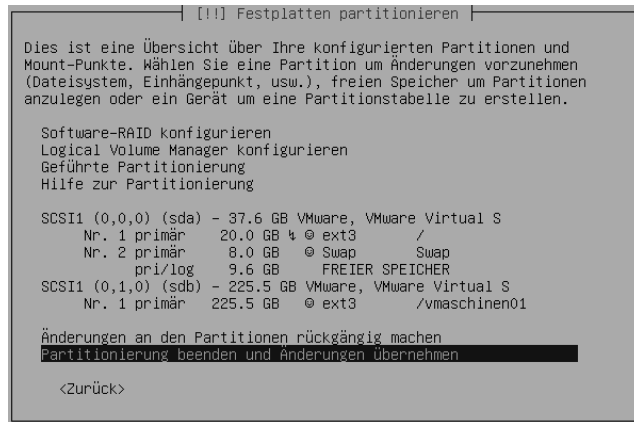
3. Schließen Sie auch hier ab mit ANLEGEN DER PARTITION BEENDEN.

## Partition für die VMs anlegen

Jetzt können Sie auf einer zusätzlichen Platte oder auf dem restlichen freien Platz eine weitere große Partition erstellen für die zukünftigen virtuellen Maschinen.

1. Wiederholen Sie die Schritte auf dem restlichen freien Speicher, und legen Sie eine Partition in voller Größe an.
2. Drücken Sie auf EINHÄNGEPUNKT (MOUNT) , und vergeben Sie einen Namen von Hand, im Beispiel `/vmaschinen01`.
3. Als Filesystem lassen Sie `ext3`.
4. Zum Schluss sollte sich folgende Übersicht ergeben (Abbildung 4.5). Schließen Sie nun mit ÄNDERUNGEN ÜBERNEHMEN die Partitionierung ab.

Abbildung 4.5:  
So könnte die fertige  
Partitionierung bei  
zwei Plattensys-  
temen im Server  
aussehen



5. Bestätigen Sie das Schreiben der Änderungen mit JA.



In einer Produktivumgebung sollten mindestens auch die Verzeichnisse `/var`, `/temp` und `/home` auf getrennten Partitionen liegen, um eine Gefährdung des Systems wegen einer volle Systemplatte, etwa durch überlaufende Log-Dateien, zu verhindern.

## Restliche Installation von Debian

### Bootloader GRUB

Jetzt erfolgt die restliche geführte Installation wieder selbsterklärend und automatisch. Folgen Sie bei der Installation des Bootloaders GRUB zur Einfachheit den Vorgaben. In unserem Beispiel eines neuen Rechners können Sie GRUB wie vorgeschlagen in den Boot Record installieren lassen (Abbildung 4.6).

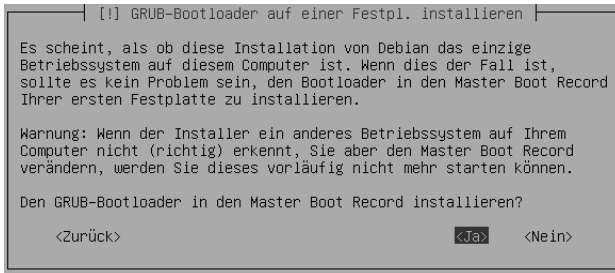


Abbildung 4.6:  
GRUB ist der Boot-  
loader von Linux

## Neustart und Basiskonfiguration des Host-Systems

Damit ist der erste Teil abgeschlossen, Debian bootet jetzt neu und startet dann automatisch die Basiskonfiguration, in der Sie den Vorgaben folgen und ein Passwort für *root* sowie einen neuen Nutzer angeben. Hier könnten Sie bei der APT KONFIGURATION auch gleich die Quellen für weitere Pakete angeben, das geht aber auch später. Drücken Sie **[↩]** auf den Eintrag CDRROM. Sorgen Sie dafür, dass Ihre CD im Laufwerk liegt, damit diese gleich als Installationsquelle indiziert werden kann. Weitere CDs und apt-Quellen fügen Sie vorerst nicht hinzu.

Am Ende der geführten Konfiguration, bei der abschließenden Debian-Software-Auswahl, setzen Sie mit der **[Leertaste]** den Punkt bei MANUELLE PAKETWAHL (Abbildung 4.7) und brechen das automatisch startende Aptitude sofort mit **[q]** ab (Abbildung 4.8). Das erspart eine größere Anzahl heruntergeladener oder installierter Pakete. Wenn Sie einen schnellen Internet-Zugang haben bzw. die komplette Distribution auf DVD, sollten Sie Aptitude die vorgeschlagenen Pakete installieren lassen.

## Manuelle Paket- auswahl

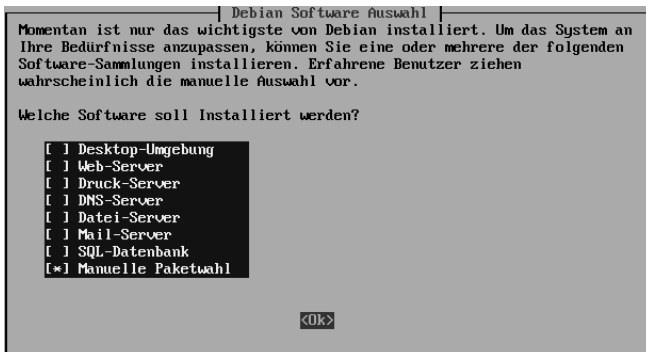


Abbildung 4.7:  
Je nach Installations-CD haben Sie hier mehr Auswahlpunkte zur Verfügung. Installieren Sie nichts automatisch

Bei der letzten Abfrage zur Mailkonfiguration genügt KEINE KONFIGURATION ZUM JETZIGEN ZEITPUNKT. Damit sind Sie mit der Grundinstallation schon fertig und können sich als Benutzer *root* anmelden.

Abbildung 4.8:  
Aptitude können Sie  
abbrechen, um nichts  
Unnötiges zu  
installieren

```

Aktionen Rückgängig Paket Suchen Optionen Ansichten Hilfe
f10: Menü ? : Hilfe q: Beenden u: Update g: Download/Installieren/Entf. von P
aptitude 0.2.15.9 Werde 176MB mehr belegen DL Größe: 62,3M
--\ Pakete, die automatisch installiert werden, um Abhängigkeiten zu erfüllen
pi# libx11-6 +1425kB <keine> 4.3.0.dfsg
pi# tc18.4 +3207kB <keine> 8.4.9-1
pi# tk8.4 +2634kB <keine> 8.4.9-1
pi# xfree86-common +1315kB <keine> 4.3.0.dfsg
pi# xlibs-data +7664kB <keine> 4.3.0.dfsg
--\ Pakete, die zurückgehalten werden
i kernel-image-2.6.8-2-686 2.6.8-16 2.6.8-16sa
--\ Pakete, die installiert werden
pi bc +188kB <keine> 1.06-15
pi bin86 8kB <keine> 0.16.14-1.
pi bind9-host 8kB <keine> 1:9.2.4-1
pi binutils 19kB <keine> 2.15-6

```

Diese Pakete werden installiert, weil sie für ein anderes Paket notwendig sind,  
das Sie zur Installation ausgewählt haben.

#### 4.4.2 Weitere Pakete auf dem Host installieren

**Nutzer root** Die Bedienung des Hosts erfolgt vorerst mit dem Benutzer *root*. Andere Nutzer legen Sie später an. Sie können sich nach der Installation bereits an der Kommandozeile anmelden.

#### Paketquellen für die nachträgliche Installation mit apt konfigurieren

**Pakete bequem  
installieren mit  
apt-get**

Die wenigen zusätzlich benötigten Software-Pakete richten Sie einfach mit dem Befehl `apt-get` ein. Ist nicht die gesamte Distribution auf CD oder DVD verfügbar, dann muss dem Debian Installer noch eine Internet-Quelle genannt werden. Das erledigt der Befehl `base-config` mit der Menüauswahl APT KONFIGURIEREN (Abbildung 4.9). Haben Sie mehrere Datenträger, können Sie diese hier ebenfalls als Quelle aufnehmen und automatisch indizieren. Die gewünschten Quellen werden automatisch in die Datei `/etc/apt/sources.list` aufgenommen, die auch manuell editiert werden kann. Ein `apt-get update` an der Kommandozeile aktualisiert die Paketlisten.

Abbildung 4.9:  
Mit base-config  
können bequem die  
Paketquellen für apt  
konfiguriert werden

```

| Apt Konfiguration |
Bitte wählen Sie die Zugriffsmethode auf das Debian Archiv für apt (das
Debian Paket Management Tool):

Wenn Sie beispielsweise eine Debian CD besitzen, wählen Sie »cdrom«,
wenn Sie von einem Spiegel-Server aus dem Internet installieren wollen,
wählen Sie »ftp« oder »http«.

Zugriffsmethode für apt auf das Archiv:

cdrom
http
ftp
Dateisystem
Liste der Paketquellen von Hand editieren

<Ok> <Abbrechen>

```

#### Nützliche Pakete nachträglich mit apt-get installieren

Als erste Pakete sollten Sie den Midnight-Commander für ein übersichtliches Arbeiten im Dateisystem und SSH für die spätere Fernbedienung per Kommandozeile installieren. Die Installation führen

Sie mit folgendem Befehl durch, wobei apt-get automatisch die richtige Quelle wählt:

```
apt-get install mc ssh
```

Die Netzwerkkarten wurden vom Debian Installer mit DHCP konfiguriert, dadurch sollte der Internet-Zugang für apt-get schon funktionieren. Ansonsten führen Sie erst die Schritte zur Konfiguration einer festen IP-Adresse aus (siehe Abschnitt 4.4.3, „Netzwerk auf dem Host konfigurieren und vorbereiten“).



#### 4.4.3 Netzwerk auf dem Host konfigurieren und vorbereiten

Sie sollten für einen Server immer eine IP-Adresse festlegen, weil sonst der Host wechselnde Adressen über DHCP im LAN erhalten würde. Dazu können Sie entweder den gerade installierten Midnight-Commander mit dem Befehl `mc` starten, zur Konfigurationsdatei navigieren und diese mit `[F4]` editieren. Sie können natürlich auch den nicht gerade intuitiven Linux-Editor `vi` verwenden. Folgende Dateien müssen Sie anpassen:

**Feste IP-Adresse für den Host vergeben**

► Datei `/etc/network/interfaces`:

```
DHCP-Benutzung auskommentieren:
iface eth0 inet dhcp
auto eth0
iface eth0 inet static
address 192.168.1.10
netmask 255.255.255.0
gateway 192.168.1.1
```

Weiterhin sollte dem Host ein DNS-Server bekannt sein, schon alleine damit apt-get weiterhin Pakete installieren kann:

**DNS-Server konfigurieren**

► Datei `/etc/resolv.conf`

```
nameserver 192.168.1.1
```

Mit folgenden Befehlen können Sie die Netzwerkkonfiguration anzeigen oder Adapter starten und beenden:

```
ifconfig
ifdown eth0
ifup eth0
```

Mit einigen Ping-Befehlen in Ihr LAN und ins Internet sollten Sie die Konfiguration abschließend testen:

**Netzwerk testen**

```
ping www.vmaschinen.de
```



## 4.5 Installation von VMware auf dem vorbereiteten Host

**Auch SUSE und andere Distributionen**

Auf unserem fertig eingerichteten Debian-Grundsystem können Sie den VMware Server installieren. Hinweise zur Installation unter SUSE Linux finden Sie am Ende des Kapitels. Weitere Informationen zu anderen Distributionen finden Sie im Handbuch zum VMware Server und in den diversen Foren.

### 4.5.1 Vorbereitung zur VMware-Installation

Neben den eigentlichen Programmen von VMware sind für die Installation einige Linux-Pakete, wie die Kernel-Header und der Compiler, nötig. Zuerst richten Sie die benötigten Linux-Pakete ein:

```
apt-get install kernel-headers-$(uname -r) build-essential xlibs-dev
```

Anschließend packen Sie die Archive der VMware-Programme aus, die im Beispiel auf einer gebrannten CD vorliegen:

```
mount /dev/cdrom /mnt
mkdir /install
cd /install
tar zxvf /mnt/VMware-server-XXX.tar.gz
tar zxvf /mnt/VMware-mui-XXX.tar.gz
tar zxvf /mnt/vmware-any-any-updateXXX.tar.gz
```

Alle Pakete liegen jetzt ausgepackt im Verzeichnis */install* und können auch für spätere Neuinstallationen immer wieder verwendet werden.

### 4.5.2 Installation des VMware Servers

Das Installationsskript von VMware übernimmt das Kopieren aller Dateien in die richtigen Verzeichnisse:

```
cd /install/vmware-server-distrib
./vmware-install.pl
```

**Der Any-Any-Patch wird nicht mehr benötigt**

Normalerweise wird nach dem Kopieren automatisch das Konfigurationsskript *vmware-config.pl* gestartet, wenn Sie auf die entsprechende Frage mit *Ja* antworten. Im Normalfall lassen Sie das zu. Wenn Sie dagegen aus irgendwelchen Gründen den schon genannten Any-Any-Patch installieren müssen, dann brechen Sie an dieser Stelle ab, indem Sie mit *Nein* antworten. Jetzt können Sie den Patch einspielen, der u.a. Änderungen an den kopierten Sources der VMware-Module vornimmt:

```
cd /install/vmware-any-any-updateXXX
./runme.pl
```

Das Skript *runme.pl* des Patches startet das vorher abgebrochene *vmware-config.pl* dann automatisch neu. Wenn Sie den Patch nicht verwenden, wurde *vmware-config.pl* bereits vom VMware Installationskript gestartet, und Sie machen an dieser Stelle einfach weiter ohne den Patch.

Installieren Sie immer ohne den Any-Any-Patch, er wird aktuell nicht mehr benötigt. Sollten in Folgeversionen Probleme auftreten, können Sie die Installation jederzeit wiederholen, an dieser Stelle den Patch einspielen und erst dann *vmware-config.pl* ausführen.



Jetzt erfolgt die Konfiguration des VMware Servers inklusive notwendiger Übersetzung der VMware-Module. Alle Fragen können Sie mit den Standardvorgaben beantworten. Die EULA müssen Sie erst mit der Leertaste nach unten durchblättern, bevor Sie diese bestätigen können. Das Skript konfiguriert auch Ihr Netzwerk. Schauen Sie zur genaueren Vorgehensweise bitte in *Teil 3, Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“*. Durch einen erneuten Aufruf von */usr/bin/vmware-config.pl* lässt sich später die Konfiguration jederzeit wiederholen, vorerst genügen auch hier die Standardantworten.

**vmware-config.pl installiert den Server**

### 4.5.3 Installation des Web-Interface vom VMware Server

Das *VMware Management Interface*, bzw. das so genannte Web-Interface, müssen Sie im Gegensatz zur Windows-Version des VMware Servers separat installieren. Unter Debian benötigen Sie zusätzliche Dateien und zwei Links, damit der Webserver für das Management Interface startet:

```
apt-get install libdb2
ln -s /usr/lib/libcrypto.so.0.9.7 /usr/lib/
libcrypto.so.4
ln -s /usr/lib/libssl.so.0.9.7 /usr/lib/libssl.so.4
```

Die eigentliche Installation erfolgt wieder mit einem Skript von VMware. Auch hier können alle Fragen mit den Vorgaben beantwortet werden:

```
cd /install/vmware-mui-distrib
./vmware-install.pl
```

### 4.5.4 Steuerung von VMware direkt am Host

Der VMware-Host ist bereits fertig! Sie finden hier noch schnell ein paar Hinweise zur Bedienung, im Normalfall müssen Sie am Host aber kaum eingreifen. **Fertig!**

- ▶ Folgender Befehl beendet und startet die Dienste des VMware Servers (beim Hochfahren des Hosts erfolgt der Start der Dienste automatisch):  

```
/etc/init.d/vmware stop | start
```
- ▶ Damit steuern Sie das Web-Interface:  

```
/etc/init.d/httpd.vmware stop | start
```
- Überprüfung der laufenden Dienste** ▶ Mit folgendem Befehl können Sie überprüfen, ob alle Dienste auf den entsprechenden Ports lauschen:  

```
netstat -an|grep LIST |grep -E -e 8222 -e 8333 -e 902
```

Port 902 ist die Remote-Konsole und 8222/8333 ist das Web-Interface.
- ▶ Und mit diesem Befehl haben Sie einen Überblick über die laufenden VMware-Prozesse:  

```
ps -ef|grep vmware
```

In der Liste sollten *vmware-serverd* und *vmware-mui/apache* auftauchen. Wenn Sie ein NAT-Netzwerk konfiguriert haben, finden sich zusätzlich *vmnet-natd* und *vmnet-dhcpd*.
- Konfiguration ändern** ▶ Damit konfigurieren Sie nachträglich den Server und das Web-Interface:  

```
/usr/bin/vmware-config-mui.pl
/usr/bin/vmware-config.pl
```
- VMware Server deinstallieren** ▶ VMware kann mit folgendem Kommando wieder deinstalliert werden:  

```
/usr/bin/vmware-uninstall.pl
```

## 4.6 Bedienung und Konfiguration des VMware Servers von einem Windows-Client

Die gesamte weitere Administration und Bedienung können Sie ab jetzt ganz bequem von einem beliebigen Client im LAN ausführen.

### 4.6.1 Das Web-Interface und die Remote-Konsole des VMware Servers

- Web-Interface und Remote-Konsole** Laden Sie am Client zuerst das *VMware Management Interface* im Browser, wobei Sie die eventuell erscheinende Zertifikatsmeldung bestätigen können, Sie wissen ja, mit welchem Server Sie es zu tun

haben. Gleich von der Startseite können Sie ohne Anmeldung die *VMware Server Console for Windows* herunterladen und installieren (Abbildung 4.10).

`https://ihr_host:8333`

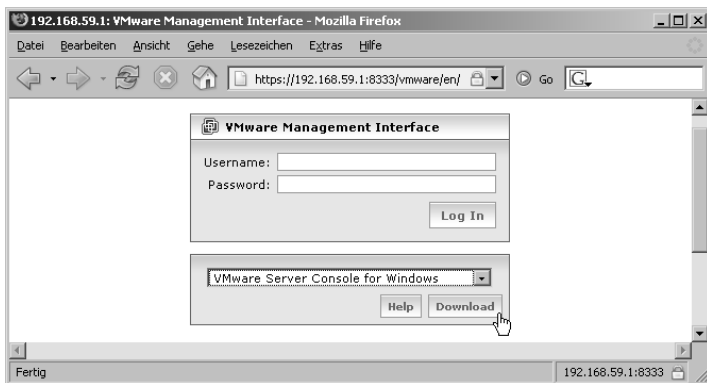


Abbildung 4.10:  
Das Web-Interface  
verwenden Sie zum  
einfachen Down-  
load der VMware  
Server Console

Als Nutzer *root* lassen sich dann in der frisch installierten Remote-Konsole bereits die VMs erstellen, starten und bedienen. Als erste Amtshandlung sollten Sie hier unter *HOST/SETTINGS/GENERAL* den Pfad anpassen, in dem Ihre neuen VMs automatisch angelegt werden, in unserem Workshop wäre das */vmaschinen01* (siehe auch Teil 1, Kapitel 3, „Installation und Konfiguration der einzelnen Produkte“).

**Standardpfad  
anpassen**

Später können Sie weitere Nutzer auf dem Linux-System anlegen, um den Zugriff auf die virtuellen Maschinen mit Dateirechten besser zu kontrollieren. Zur Rechteverwaltung finden Sie Informationen in Teil 3, Kapitel 5, „Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs“.



## 4.6.2 Besonderheiten unter Linux bei der Arbeit mit VMware

Um Ärger mit Dateien zu umgehen, die größer als 2 GB sind, sollten Sie virtuelle Platten unter Linux grundsätzlich in 2-GB-Segmenten erstellen. Das erspart Ärger bei bestimmten FTP-Clients, bei älteren Dateisystemen, die keine größeren Dateien unterstützen, und ermöglicht gleich ein einfaches Brennen und Weitergeben fertiger VMs auf DVD (siehe Teil 2, Kapitel 5, „Virtuelle Umgebungen mit dem VMware-Player weitergeben“).

**Dateien > 2 GB**

Im Gegensatz zum Windows-Host fehlt in der Remote-Konsole eines Linux-Hosts der Menüpunkt *HOST/VIRTUAL NETWORK SETTINGS*. Die Netzwerkkonfiguration übernimmt unter Linux das schon bekannte Skript *vmware-config.pl*. Die Einrichtung des internen DHCP-Servers oder des NAT-Dienstes erfolgt über die Dateien in */etc/vmware/*

**Netzwerk-  
verwaltung**

*vmnetX/nat* und */etc/vmware/vmnetX/dhcpd*. Detaillierte Informationen zum Netzwerk finden Sie in Teil 3, Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“.

##### Konto für die VMs

Weiterhin vermisst der Windows-Admin im Menü VM/SETTINGS OPTIONS/STARTUP/SHUTDOWN den Eintrag für den VIRTUAL MACHINE ACCOUNT, unter dem die Gäste laufen. VMs werden auf dem Linux-Host immer als der Besitzer der zugehörigen Konfigurationsdatei (\*.vmx) ausgeführt, bei unserem ersten Kennenlernen also als Nutzer *root*.

### 4.6.3 Weitere nützliche Programme für die Bedienung vom Client – *putty* und *winscp*

##### Kommandozeile und Dateisystem

Mit einem Terminalprogramm wie *putty* können Sie vom Client auf die Kommandozeile des Servers zugreifen. *Winscp* ermöglicht den komfortablen Zugriff auf das Dateisystem von einem Windows-Client, ohne erst die Emulation von Windows-Freigaben mittels Samba am Linux Host zu installieren.



Wenn die Anmeldung an diesen beiden Programmen sehr lange dauert, kann das an einer fehlenden Namensauflösung liegen. Haben Sie keinen DNS-Server am Host eingetragen, löst er Ihren Clientnamen nicht auf. Abhilfe schafft ein Eintrag des Clients, von dem aus Sie zugreifen wollen, mit der zugehörigen IP-Adresse in die Datei */etc/hosts* am Server.

## 4.7 Die weitere Konfiguration des Hosts zur Windows-Anbindung

Vor allem die Anbindung der Dateisysteme des Hosts an die Windows-Welt kann noch stark verbessert werden. Schließlich wollen Sie VMs ja auch hin und her kopieren oder sichern.

### 4.7.1 Host-Verzeichnisse im Windows-Netzwerk mit Samba freigeben

##### Von Windows auf unseren Host zugreifen

Um VMs komfortabel auf den Windows-Laptop zu kopieren oder Dateien der virtuellen Maschinen zu editieren, kann der Linux-Host Verzeichnisse wie ein Windows-Server freigeben. Dazu ist der Samba-Server zu installieren:

```
apt-get install samba
```

Um das Verzeichnis */vmaschinen01* freizugeben, in dem Ihre VMs liegen, müssen noch folgende Dinge eingestellt werden. Machen Sie zuerst von der Datei *smb.conf* eine Sicherungskopie:

```
cp /etc/samba/smb.conf /etc/samba/smb_sich.conf
```

Ersetzen Sie das Original durch folgenden Inhalt (mittels *mc*, *vi* oder der Editierfunktion von *WinSCSP*):

```
[global]
workgroup = vmaschinen
netbios name = vmhost01
security = user

[vmaschinen01]
path = /vmaschinen01
public = yes
writeable = yes
```

Jetzt muss noch ein Nutzer mit Samba-Passwort für den Zugriff angelegt werden:

```
adduser nutzer01
smbpasswd -a nutzer01
```

Wir geben wenigstens Leserechte für alle auf das Verzeichnis */vmaschinen01*:

```
chmod o+rx /vmaschinen01
```

Sie können für Testzwecke auch Ihrem Nutzer *root* ein Samba-Passwort geben (das widerspricht allerdings den gängigen Sicherheitskonventionen):

```
smbpasswd -a root
```

Sie sollten Samba neu starten, um die Änderungen schneller zu übernehmen:

```
/etc/init.d/samba restart
```

Ab jetzt können Sie die Freigabe *\\mein\_vmhost\vmaschinen01* ganz normal mit dem Windows-Explorer oder mit `net use` verbinden.

#### **4.7.2 Vom Host auf Windows-Freigaben anderer Server zugreifen**

Wenn sich die ISO-Image-Sammlung auf einem Windows-Server im LAN befindet, können Sie auf dem Linux-Host eine Windows-Freigabe mittels SMB-Mount verbinden. Die Unterstützung müssen Sie noch mit *apt* einrichten:

```
apt-get install smbfs
```

**Komfortabel  
auf Windows-  
Verzeichnisse  
zugreifen**

Jetzt können Freigaben von Windows-Servern auf unserem Linux-Host verbunden werden. Da das alles eine ganz schöne Tipperei wird, legen Sie am besten folgenden Eintrag in der Datei */etc/fstab* an, dabei ersetzen Sie Rechnername, Name der Freigabe, IP-Adresse, Nutzer und Passwort mit Ihren Gegebenheiten:

```
//win_server01/iso-freigabe /iso-images01 smbfs
ip=192.168.1.5,username=nutzer,password=passwort 0 0
```

Der Eintrag */iso-images01* ist der Mountpoint auf dem Linux-Host. Dazu fehlt noch ein Verzeichnis:

```
mkdir /iso-images01
```

Jetzt können Sie die Verbindung bei Bedarf ganz einfach herstellen, im Verzeichnis */iso-images01* erscheint auf dem Host der Inhalt der Windows-Freigabe und kann verwendet werden wie ein lokales Verzeichnis:

```
mount /iso-images01
```

### 4.7.3 Eine NTFS-Partition am Linux-Host einbinden und lesen

Auch NTFS-Partition lassen sich mounten, z.B. die Festplatte mit virtuellen Maschinen. Da auf NTFS-Partitionen kein schreibender Zugriff möglich ist, funktionieren virtuelle Platten allerdings nur mit einem Snapshot, dessen Redo-Logs auf einer beschreibbaren Linux-Partition liegen, oder Sie kopieren die VMs auf eine Linux-Partition. Die Bezeichnungen der Platten und Partitionen in Ihrem Host finden Sie mit diesem Befehl:

```
fdisk -l
```

Zum einfachen Mounten fügen Sie wieder eine Zeile in der Datei */etc/fstab* hinzu, hier ist nur */dev/hdb1* mit Ihrer Partition anzupassen, */ntfs01* ist der Mountpoint:

```
/dev/hdb1 /ntfs01 ntfs rw,user 0 0
```

Zusätzlich benötigen Sie noch ein Verzeichnis als Mountpoint, in dem dann nach dem Mounten der Inhalt der NTFS-Partition erscheint:

```
mkdir /ntfs01
mount /ntfs01
```

## 4.8 Die gesamte Installation und Konfiguration auf einen Blick

Sie haben jetzt ein lauffähiges System, das sich gut in eine Windows-Umgebung integriert. Damit können Sie Ihre ersten Schritte in der virtuellen Welt machen. Zur Bedienung, den virtuellen Platten, Netzwerken usw. schauen Sie bitte in den entsprechenden Kapiteln im Buch nach. Alle Schritte finden Sie als Zusammenfassung hier nochmals auf einen Blick:

### ► **Vorbereitung:**

Alle Hardware in den Host einbauen (Netzwerkkarten!).

Alle Pakete besorgen und auf CD brennen:

Debian: *Netinst-ISO (i386)*

Server: *VMware-server-XXX.tar.gz*

Web-Konsole: *VMware-mui-XXX.tar.gz*

Eventuell Any-Any-Patch: *vmware-any-any-updateXXX.tar.gz*

### ► **Host installieren:**

Installation mit dem Befehl `linux26`.

Separate Partition für die VMs anlegen!

Anmeldung vorerst mit `root`.

Apt-Quellen mit `base-config` auswählen.

Erste Pakete einrichten:

`Apt-get install ssh mc`

Feste IP-Adresse und DNS konfigurieren:

Dateien:

*/etc/network/interfaces*

*/etc/resolv.conf*

Befehle:

`ifconfig`

`ifdown eth0`

`ifup eth0`

### ► **Installation von VMware:**

Benötigte Pakete installieren:

`apt-get install kernel-headers-$(uname -r) build-essential xlibs-dev`

TAR-Archive von CD auspacken:

`mount /dev/cdrom /mnt`

`mkdir /install`

`cd /install`

`tar xzvf /mnt/VMware-server-XXX.tar.gz`

`tar xzvf /mnt/VMware-mui-XXX.tar.gz`

`tar xzvf /mnt/vmware-any-any-updateXXX.tar.gz`



Server installieren:

```
cd /install/vmware-server-distrib
./vmware-install.pl
```

Bei Problemen Installation mit dem Any-Any-Patch wiederholen:

```
(bei vmware-config.pl abbrechen!)
cd /install/vmware-any-any-updateXXX
./runme.pl
```

Web-Interface installieren.

Pakete und symbolische Links:

```
apt-get install libdb2
ln -s /usr/lib/libcrypto.so.0.9.7 /usr/lib/lib-
crypto.so.4
ln -s /usr/lib/libssl.so.0.9.7 /usr/lib/libssl.
so.4
```

Installation:

```
cd /install/vmware-mui-distrib
./vmware-install.pl
```

Konfiguration von Server und Web-Interface:

```
/usr/bin/vmware-config.pl
/usr/bin/vmware-config-mui.pl
```

Befehle zum Verwalten:

```
/etc/init.d/vmware stop / start
/etc/init.d/httpd.vmware stop / start
netstat -an|grep LIST |grep -E -e 8222 -e 8333 -e
902
ps -ef|grep vmware
```

#### ► Am Client

Web-Interface starten im Browser mit [https://ihr\\_host:8333](https://ihr_host:8333)

Remote-Konsole installieren übers Web-Interface.

Putty und WinSCP installieren.

#### ► Zusätzliche Optionen

Nutzer auf dem Host anlegen und Rechte vergeben.

Samba installieren und Verzeichnisse freigeben.

NTFS und Windows-Freigaben mounten.

## 4.9 Mehr als 4 GB RAM im Host mit PAE verwenden

Virtuelle Maschinen benötigen als Lebenselixier eines ganz besonders – Hauptspeicher! Wenn Sie bisher auf den meisten normalen Servern mit 4 GB RAM bereits üppig ausgestattet waren, wird auf einem Virtualisierungs-Host schnell der Wunsch nach mehr laut.

Haben Sie über 4 GB RAM in Ihrem Host stecken, so können Sie diesen allerdings oftmals gar nicht verwenden. Aufgrund der begrenzten Adressierungsbreite lässt er sich einem 32-Bit-System normalerweise nicht ansprechen. Um diese Einschränkung zu umgehen, wurde die so genannte *Physical Address Extension*, kurz *PAE*, entwickelt, die es ermöglicht, bis zu 64 GB Hauptspeicher zu benutzen. Wollen Sie diese Funktion unter Linux einschalten, muss der Kernel mit einer speziellen Option kompiliert werden.

**PAE – Physical Address Extension**

Auf 64-Bit-Systemen mit 64-Bit-OS kann der Speicher auch ohne zusätzliche Optionen voll genutzt werden. Allerdings ist die Installation des VMware Servers auf einem 64-Bit-Debian nicht zu empfehlen, da trotzdem eine 32-Bit-Umgebung benötigt wird, um VMware-Programme auszuführen, was das Vorhaben für Einsteiger etwas kompliziert macht. Verwenden Sie dazu eine unterstützte Distribution wie SUSE.



#### 4.9.1 Kernel mit PAE-Option neu übersetzen

Zum Glück ist es unter Debian recht einfach, einen neuen Kernel zu konfigurieren. Folgende Schritte sind notwendig:

Ersetzen Sie in den folgenden Befehlen die aktuelle Versionsnummer Ihres Kernels. Im Beispiel lautet diese 2.6.8. Sie erfahren die Version mit dem Befehl `uname -r`.



1. Zuerst installieren Sie die Kernel-Quellen (Internet-Zugang notwendig):  

```
apt-get install kernel-source-2.6.8
```
2. Weiterhin werden zusätzliche Pakete zum Kompilieren des Kernels benötigt:  

```
apt-get install build-essential binutils bin86
kernel-package libncurses5-dev shellutils alien
fakeroot
```
3. Jetzt sind die Kernel-Quellen auszupacken:  

```
cd /usr/src/
tar xjvf kernel-source-2.6.8.tar.bz2
```
4. Um nicht alle Parameter für einen neuen Kernel festlegen zu müssen, was eine ganz schöne Arbeit wäre, verwenden Sie einfach die vorhandene Konfiguration und ändern nur einen Wert. Die aktu-

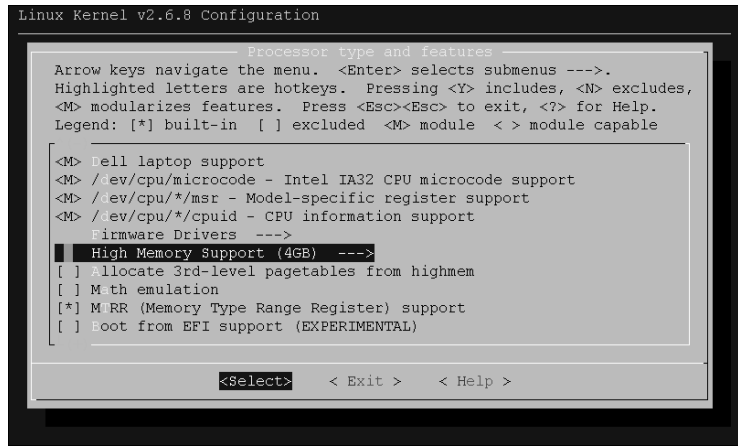
elle Konfiguration des installierten Standard-Kernels kopieren Sie dazu aus dem Bootverzeichnis:

```
cd /usr/src/kernel-source-2.6.8
cp /boot/config-$(uname -r) .config
make oldconfig
```

5. Jetzt können Sie ganz einfach den neuen Kernel menübasiert konfigurieren:

```
make menuconfig
```

Abbildung 4.11:  
Mit `make menuconfig` können menübasiert die Kernel-Parameter eingestellt werden



**Parameter für PAE und SMP konfigurieren**

Suchen Sie den Eintrag `PROCESSOR TYPE AND FEATURES/HIGH MEMORY SUPPORT (4 GB)`, und ändern Sie ihn in `64 GB` (Abbildung 4.11). Zusätzlich können Sie bei einem Multiprozessor-Host gleich noch `SMP` einschalten über den Menüpunkt `SYMMETRIC MULTI-PROCESSING SUPPORT`.

6. Vor der Übersetzung noch etwas aufräumen:

```
make-kpkg clean
```

7. Und so wird der Kernel übersetzt:

```
fakeroor make-kpkg --append_to_version -pae-smp --
initrd --revision=01 kernel_image
```

Den Wert `-pae-smp` können Sie mit einer Zeichenkette ersetzen, die Ihren neuen Kernel knapp beschreibt, die Nummer hinter `revision=` können Sie hochzählen, wenn Sie verschiedene Versionen erstellen.

Die Warnung zu `initrd` und dem notwendigen `cramfs patch` ignorieren Sie, und Sie antworten auf die Frage `Should I abort[Ny]?` mit `N`!

**Kaffeepause!**

Jetzt ist es an der Zeit, eine Tasse Kaffee zu holen. Das Übersetzen dauert je nach System 30 Minuten (3 GHz CPU) bis zu mehreren Stunden (alte Hardware).

8. Der fertige Kernel muss anschließend noch installiert werden:

```
cd /usr/src
dpkg -i kernel-image-2.6.8-pae-smp_01_i386.deb
```

Dabei wird unter anderem auch das Bootmenü des Bootloaders GRUB angepasst. In der Datei `/boot/grub/menu.lst` können Sie zur Vorsicht kontrollieren, ob das neue Kernel-Image als Booteintrag vorhanden ist.

**Bootloader GRUB**

9. Beim nächsten Neustart steht Ihr neuer Kernel im Bootmenü zur Auswahl.

Nach der Installation von VMware sollte das Web-Interface des VMware Servers Ihnen die wirkliche RAM-Größe anzeigen – auch auf 32-Bit-Hardware.

## 4.10 Installation des VMware Servers unter SUSE Linux

Die gleiche Installation, wie oben beschrieben, können Sie auch unter jeder anderen Distribution vornehmen. Die folgende Anleitung beschreibt das Vorgehen für das verbreitete SUSE Linux. Diese Distribution wird von VMware offiziell unterstützt. Vor allem auf einem 64-Bit-System ist die Distribution sehr gut geeignet, weil sie eine funktionierende 32-Bit-Umgebung für die Kompatibilität mitbringt. Dadurch kann VMware Server ohne Probleme auf 64-Bit-Hardware installiert werden und ohne PAE-Option die volle RAM-Ausstattung nutzen. Auch für 32-Bit-Hardware ist SUSE Linux genau wie Debian geeignet.

**Ideal für 64-Bit-Systeme**

### 4.10.1 Installation von SUSE Linux 10

Wenn Sie nicht die kommerzielle Distribution gekauft haben, können Sie die OpenSource Software Edition von SUSE Linux bei OpenSUSE herunterladen. Für die minimale Installation benötigen Sie mindestens ein Bootabbild für eine Internet-Installation passend zu Ihrer Rechnerarchitektur, z.B. *x86-64* für ein 64-Bit-System. Unter YaST konfigurieren Sie später eine Installationsquelle für zusätzlich benötigte Pakete, die Sie dann aus dem Internet nachinstallieren. Oder Sie laden sich die vollständigen CDs herunter. Den Link für die Internet-Quellen finden Sie unter *Installation Repository* (bzw. *Installationsdaten*) in der Tabelle auf der SUSE Download-Webseite.

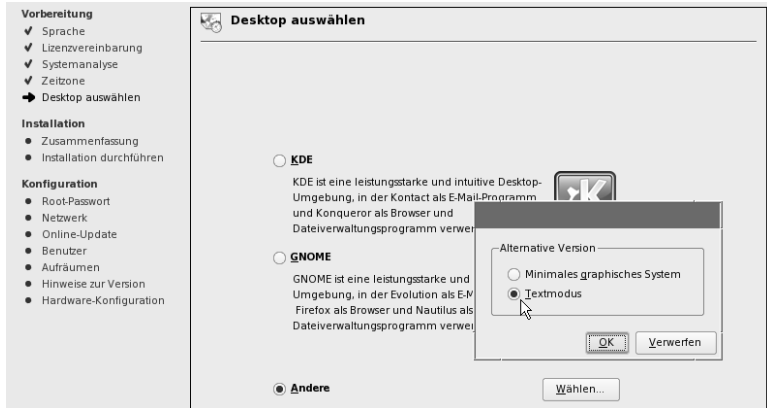
**Kostenloses OpenSUSE**

#### Installation von SUSE Linux

Bei der Installation wählen Sie gleich zu Beginn keine grafische Oberfläche, sondern NUR TEXTMODUS (Abbildung 4.12). Das genügt für einen schlanken Host völlig und bläht ihn nicht unnötig auf.

**Nur Textmodus genügt**

Abbildung 4.12:  
Die Bedienung des  
schlanken Hosts  
erfolgt vom LAN-  
Client. Deshalb  
genügt der Text-  
modus



## Partitionierung der Host-Platte

Während der Installation sollten Sie bei der Partitionierung eingreifen und nur eine kleine 10-GB-Systempartition erstellen. Den Rest der Platte (wenn möglich ein gesondertes Plattensystem) reservieren Sie für die virtuellen Maschinen (siehe Tabelle 4.1). Den übrigen Teil der Installation erledigt der komfortable Installationsassistent selbsterklärend.

## Nacharbeit nach der Installation von SUSE

Nach dem ersten Neustart ist noch etwas Nacharbeit notwendig. Mit dem Konfigurationswerkzeug *YaST*, das Sie mit dem gleichnamigen Befehl `yast` starten können, erfolgt die gesamte Einrichtung und Wartung des Systems auch für den Neuling sehr einfach. Hier lassen sich zusätzliche Pakete installieren oder die Netzwerkkarten konfigurieren (Abbildung 4.13).

Folgende Dinge müssen Sie noch mit YaST erledigen:

- ▶ Feste IP-Adresse samt DNS-Server und Default-Gateway vergeben über NETZWERKGERÄTE/NETZWERKKARTE.
- ▶ SSH installieren, damit Sie später vom Client aus mit Putty die Kommandozeile bedienen können: NETZWERKDIENTE/ADMINISTRATION VON EINEM ENTFERNTEN RECHNER. Vergessen Sie nicht, dabei auch gleich den Firewall-Port zu öffnen!
- ▶ In der Firewall müssen noch die Ports für die VMware Remote Console und für das Web-Interface geöffnet werden über SICHERHEIT UND BENUTZER/FIREWALL/ERLAUBTE DIENSTE/ERWEITERT. Folgende Ports werden benötigt:  
Port 904 für die Remote-Konsole (902 ist schon belegt!).  
Ports 8222 und 8333 für das Web-Interface.



Sie können auch über SICHERHEIT UND BENUTZER/FIREWALL/SCHNITTSTELLEN/ÄNDERN Ihre Netzwerkkarte zur *internen Zone* erklären, oder Sie schalten für den Anfang zum Testen die Firewall gleich ganz ab.

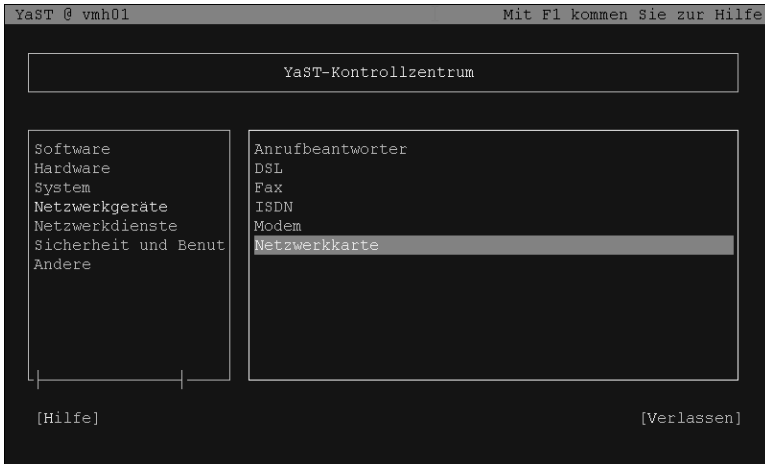


Abbildung 4.13:  
YaST ermöglicht unter SUSE eine menübasierte Konfiguration des Systems

- Folgende Pakete müssen Sie vor dem Setup von VMware installieren über SOFTWARE/SOFTWARE INSTALLIEREN ODER LÖSCHEN/SUCHEN (Abbildung 4.14):
  - *compat* (auf 64-Bit-Systemen *compat-32*)
  - *gcc, gcc-c++* (nur für die Perl-API des VMware Servers notwendig)
  - *kernel-source* (nur wenn die Übersetzung der VMware Module nicht funktioniert)

Compiler und Kernel-Header benötigen Sie je nach Distribution nur im Bedarfsfall, wenn VMware keine passenden kompilierten Binärmodule mitliefert. Wenn Sie alle CDs oder die DVD zur Hand haben, installieren Sie einfach alles prophylaktisch.

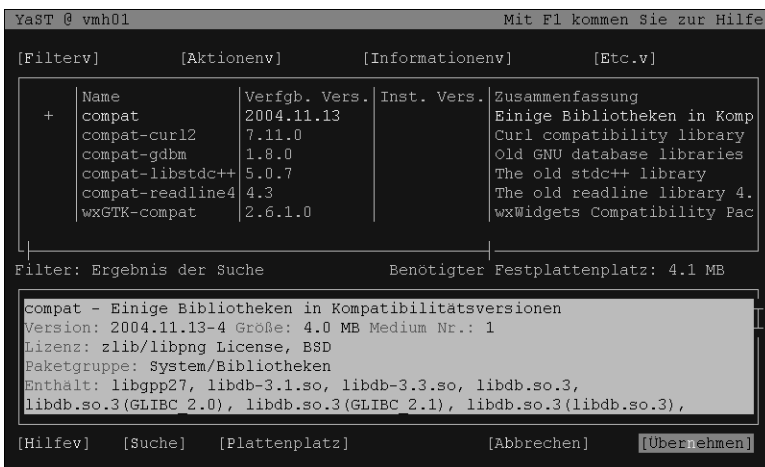


Abbildung 4.14:  
Benötigte Module lassen sich sehr einfach mit YaST installieren

## Besonderheiten bei der Installation des VMware Servers unter SUSE

### Port für die Remote-Konsole

Unter SUSE ist Port 902 (Remote-Konsole) schon reserviert. Deshalb schlägt *vmware-config.pl* Port 904 vor, den Sie verwenden können. Denken Sie später daran, bei der Anmeldung an der Remote-Konsole diesen Port mit anzugeben, z.B. *vmh01:904*. Der Grund dafür sind Einträge zum Port 902 in der Datei */etc/services*, die Sie vor der Installation des VMware Servers auch einfach mit *#* auskommentieren und durch folgende Zeile ersetzen können – danach lässt sich nach einem Neustart auch der Standardport 902 wieder verwenden:

```
vmware-authd 902/tcp #VMware-authd
```

### RPM oder TAR

Die Installation der Pakete des VMware Servers kann als RPM oder auch als TAR-Archiv erfolgen. Bei VMware gibt es entsprechende Dateien zum Herunterladen. Mit dem TAR-Archiv können Sie die oben bei Debian beschriebene Methode gleich wieder genauso nachvollziehen (bis auf *apt-get*!). Sollten Sie das RPM-Paket installieren, müssen Sie danach das Skript *vmware-config.pl* manuell starten:

```
/usr/bin/vmware-config.pl
```



Sollten Sie nach dem Anzeigen der Lizenzbedingungen und auch bei den Netzwerkeinstellungen in den VMware-Skripten keine Frage *Yes/No* sehen und die Installation geht nicht weiter, dann geben Sie an diesen Stellen blind ein *q* ein. Jetzt erscheinen die fehlenden Bildschirmausgaben.

### Der Compiler ist nicht immer notwendig

Für unterstützte Distributionen, wie SUSE, liefert VMware fertig kompilierte Binärmodule mit. Damit entfällt eine Übersetzung der Quellen beim Ausführen von *vmware-config.pl*. Sie brauchen also nicht unbedingt Kernel-Header und Compiler. Das gilt nur, wenn Sie vorerst auf die Perl-API von VMware verzichten können, denn diese benötigt *gcc*! Die während des Installationskriptes auftauchende Frage zum Compiler können Sie mit *No* beantworten:

```
Setup is unable to find the "gcc" program on your
machine. Please make sure it is installed. Do you
want to specify the location of this program by hand?
[yes] no
```

### Kernel-Header und Compiler, wenn es doch nicht geht

Da aber meist die Entwicklung der Distributionen schneller voranschreitet als die der VMware-Pakete, kann es sein, dass Sie früher oder später doch wieder Kernel-Header und Compiler bereitstellen müssen. Am umfassendsten gelingt das über *YaST* und die Software-Selektion *KERNEL-ENTWICKLUNG*, dort ist wirklich alles dabei.

Wenn es dann immer noch bei der Installation Probleme geben sollte, müssen vorher folgende Befehle ausgeführt werden:

```
cd /usr/src/linux
make clean
make cloneconfig
make prepare
```

Der Rest der Installation erfolgt wie oben unter Debian beschrieben. Die optionalen Komponenten, wie Samba usw., können Sie komfortabel mit YaST einrichten.

**Abschluss der  
Einrichtung**

## 4.11 Links zur benötigten Software

- ▶ Debian-CD-Images:  
*<http://www.debian.de/CD/netinst/>*
- ▶ Debian-Handbuch und ausführliche Installationsbeschreibung:  
*<http://debiananwenderhandbuch.de/instsarge.html>*
- ▶ VMware Server Download und Handbücher:  
*<http://www.vmware.com/products/server/>*
- ▶ VMware Any-Any-Update:  
*<http://platan.vc.cvut.cz/ftp/pub/vmware/>*
- ▶ OpenSUSE-Download:  
*[http://de.opensuse.org/Stabile\\_Version](http://de.opensuse.org/Stabile_Version)*





# 5 Virtuelle Umgebungen mit dem VMware Player weitergeben

Mit dem kostenlosen VMware Player geben Sie fertig installierte und perfekt konfigurierte Umgebungen aus virtuellen Maschinen per DVD, Internet oder auf dem Laptop kinderleicht an Kunden, Mitarbeiter und Freunde weiter.

**Kostenlose  
VMware Runtime**

Sogar neue VMs können Sie mit etwas Hintergrundwissen erstellen und dadurch für einfache Anwendungen auf die kostenpflichtige VMware Workstation oder auf den gewichtigen VMware Server verzichten.

## Workshop im Überblick

### Hauptprodukt

- ▶ VMware Player
- ▶ Auch Gäste von Virtual PC laufen sofort im Player.

### Praktische Verwendung

- ▶ In Schulungsumgebungen können Sie jedem Teilnehmer unzerstörbare Testsysteme beliebiger Konfiguration schnell zur Verfügung stellen.
- ▶ Komplette Produktinstallationen versenden Sie als Instant-Demo an Kunden.
- ▶ Fertig konfigurierte Systeme lassen sich als Appliance verteilen.

### Schwerpunkte

- ▶ Unterschiede zur Vollversion
- ▶ Erweitern des Players durch Editieren der *vmx*-Datei
- ▶ Versteckte Funktionen des Players
- ▶ Erstellen einer optimal transportablen, platzsparenden VM

### Zielgruppe

- ▶ Software-Firmen, Entwickler, Vertriebsmitarbeiter
- ▶ Schulen, Ausbilder, Trainer
- ▶ Privatpersonen mit geringem Budget

## 5.1 Praktische Verwendung von VMware Player

### Auch VMs von Microsoft

Der VMware Player ist eine kostenlose Runtime-Umgebung für virtuelle Maschinen und ermöglicht das Ausführen fertig installierter Gäste auf jedem beliebigen PC ohne zusätzliche Lizenzkosten. Sogar VMs von Microsoft Virtual PC laufen unter dem Player. VMware liefert damit die Kernkomponenten seiner Virtualisierungssoftware zum Nulltarif, denn unter der Haube ist der Player eine vollwertige VMware Workstation 5.5. Trotz massiver Einschränkungen der Oberfläche ist der Player sehr nützlich, um VMs weiterzugeben oder mit virtuellen Maschinen zu experimentieren. Jeder Anwender kann den Player kostenlos und ohne Registrierung aus dem Internet herunterladen. Selbst als kostenlose Alternative zu den Vollprodukten lässt sich mit ihm leben, etwa um eine Live-CD auszuprobieren oder um eine Linux-Distribution zu testen.



Einen Schnelleinstieg zum VMware Player mit einer Mustervolage von der Buch CD liefert der Workshop in Teil 2, Kapitel 6, „Schulungs- oder Demo-Umgebung schnell aufgebaut“.

### 5.1.1 Unterschiede und Gemeinsamkeiten zu den Vollprodukten

Virtuelle Maschinen, die mit den Vollprodukten VMware Workstation oder Server erstellt wurden, arbeiten unter dem Player ohne Probleme. Es genügt, wenn Sie das komplette Verzeichnis einer VM kopieren und die Konfigurationsdatei auf dem Zielrechner im Player öffnen. Maschinen vom ESX Server müssen erst exportiert werden. Selbst komplette virtuelle Netzwerke lassen sich weitergeben und im Player betreiben. Mehrere VMs laufen im Player problemlos parallel (Abbildung 5.1). Die einzelnen Gäste öffnet der Player im Gegensatz zu den Vollprodukten immer in eigenen Fenstern.



Mit Tricks lassen sich auch völlig ohne Vollprodukte neue VMs erstellen (siehe Abschnitt 5.8, „Neue VMs für den Player ohne Vollprodukt erstellen“).

### Kein Virtual SMP

Nur Virtual SMP (*Symmetrisches Multiprozessor-System*), die Unterstützung von zwei virtuellen CPUs in den Gästen, bietet der Player nicht. VMs, die als Dualprozessor-Maschinen erstellt wurde, müssen angepasst werden (siehe Abschnitt 5.3.5, „Dualprozessor-VMs im Player betreiben“), sonst laufen sie im Player nicht.



Abbildung 5.1:  
Mehrere VMs  
können im Player  
auch parallel laufen

Die augenscheinlichsten Einschränkungen betreffen die spartanische Bedienoberfläche des Players. Bis auf das Ändern der RAM-Größe, das An- und Abhängen von CD, Floppy und USB und die Auswahl des Netzwerkmodus fehlen alle Funktionen der VMware Workstation bzw. des Servers. Der Player kann weder neue virtuelle Maschinen erstellen noch die vorhandene Hardware ändern. Es gibt keine Snapshot-, Klon- oder Teamfunktionen. Weiterhin unterstützt der Player keine Shared Folders zum einfachen Datenaustausch mit dem Host. Drag&Drop und die Arbeit mit der Zwischenablage funktionieren allerdings.

## Oberfläche

Die Menüs zur Netzwerkkonfiguration fehlen ebenfalls fast komplett. Sie können keine virtuellen Netzwerkkarten hinzufügen oder entfernen. Für vorhandene Netzwerkkarten, die in der Vollversion konfiguriert wurden, stehen als Verbindungstypen nur Bridged, NAT und Host-only zur Verfügung. Das flexible Custom-Netz fehlt völlig, wodurch Sie interne abgeschottete Netzwerke zwischen den Gästen nur mit Tricks erstellen können.

## Netzwerk

Für viele der fehlenden Funktionen im Player gilt aber: „Wo ein Wille ist, ist auch ein Weg“! Mehr dazu unter *Abschnitt 5.6*, „Versteckte Funktionen zutage fördern“.



### 5.1.2 Versionen des VMware Players

VMware stellt den Player in zwei Varianten zur Verfügung, die sich nur in der Art der Installation, aber nicht in den Funktionen unterscheiden.

#### Der Player als freie Version für Endanwender

Endanwender können sich die Software als einzelnes Paket herunterladen und völlig frei verwenden. Diese Version lässt sich nicht parallel zu vorhandenen Vollprodukten, wie älteren Versionen der VMware Workstation oder dem VMware Server, installieren. Zur Remote-Konsole von VMware Server läuft der Player aber problemlos parallel auf demselben Client.

#### Der Player für Entwickler im Bundle mit VMware Workstation

**Auch in der Evaluierungsversion**

Für Entwickler ist die VMware Workstation ab Version 5.5 ideal, da der Player bereits integriert ist. Dadurch können Sie VMs in der Vollversion mit allem Komfort installieren und vorbereiten und vor der Weitergabe gleich im Player testen. Selbst nach Ablauf der Evaluierungsphase der VMware Workstation ist es rein technisch weiterhin möglich, VMs in der Workstation zu erstellen und dann im integrierten Player laufen zu lassen. Das erfordert allerdings ein ständiges Hin- und Herschalten, da VMs nicht gleichzeitig in beiden Versionen geladen sein dürfen, und es entspricht auch nicht den Lizenzbedingungen für die Evaluierungsversion.

### 5.1.3 Anwendungsbeispiele des Players für verschiedene Einsatzzwecke

Auch wenn der Player auf den ersten Blick recht simpel daherkommt, belegen einige Beispiele schnell den Nutzen der unscheinbaren Software.

#### Schulungsumgebung aufbauen und verwalten

Allen Teilnehmern einer Schulung können Sie auf Ihren PCs jederzeit unzerstörbare Testmaschinen in beliebiger Konfiguration und mit beliebigen vorinstallierten Systemen bereitstellen. In wenigen Minuten ist durch einfaches Kopieren ein komplettes Schulungskabinett mit neuer Software ausgestattet. Siehe dazu auch *Teil 2, Kapitel 6, „Schulungs- oder Demo-Umgebung schnell aufgebaut“*.

#### Eine Linux-Distribution im VMware Player ausprobieren

Ohne Dualboot-Konfigurationen und ohne das vorhandene Betriebssystem zu gefährden, können Sie im VMware Player eine Linux-Version parallel zu Ihrem gewohnten Windows in einer abgeschotteten

Umgebung betreiben und testen. Mit der Muster-VM auf der Buch-CD können Sie eine virtuelle Maschine in dem Player laufen lassen und darin Linux installieren.

Sie können auch bereits fertig installierte Linux-Distributionen von der VMware-Seite laden und sofort im Player benutzen (siehe „Fertig installierte Beispiele von der VMware-Webseite“). Damit sparen Sie sich die Installation und können sofort loslegen. Wenn Sie Linux selbst installieren wollen, dann beachten Sie bitte die Hinweise zur Installation der VMware Tools unter Linux in *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*.

### **Fertige Software-Pakete verteilen**

Komplett installierte und perfekt konfigurierte Software-Pakete, wie Intranetserver, Groupware-Lösungen oder Firewalls, können Sie als sofort lauffähige Appliances im Internet oder auf DVD verteilen. Die virtuelle DMZ aus *Teil 2, Kapitel 3, „Virtuelle DMZ mit Firewall und Webserver im Internet“* wäre bereits eine Anwendung, die Sie direkt im Player weitergeben können.

### **Virtuelle DMZ**

### **Entwicklungsumgebung auf dem Laptop mitnehmen**

Ihren fertig konfigurierten Webserver samt Perl, PHP und MySQL haben Sie als Entwicklungs- und Demo-Umgebung auf dem Laptop immer mit dabei, ohne zusätzliche Lizenz einer VMware Workstation.

### **Instant-Demo für Kunden versenden**

Als Software-Entwickler können Sie sogar eine komplette Testumgebung samt Datenbank- und Webserver sowie passend konfigurierter Client-PCs vorbereiten und dann auf DVD an Interessenten schicken. Die Kunden haben keinerlei Installationsarbeit, benötigen keine zusätzliche Hardware und können sich sofort das Produkt als fertige Instant-Demo auf jedem beliebigen PC anschauen.

### **Fertig installierte Beispiele von der VMware-Webseite**

Ein simples Beispiel liefert VMware auf seiner Webseite bereits selbst. Eine Browser Appliance, bestehend aus Ubuntu Linux mit Mozilla Firefox, steht zum Download bereit. Sie startet ruck, zuck im Player, um ein abgeschottetes Surfen im Internet zu ermöglichen, ohne den eigenen PC zu gefährden. Viele andere Produkt-Demos von Drittanbietern und fertig installierte freie Betriebssysteme finden Sie auf der Webseite von VMware im *Virtual Machine Center* zum kostenlosen Download: <http://www.vmware.com/vmtm/appliances/>.

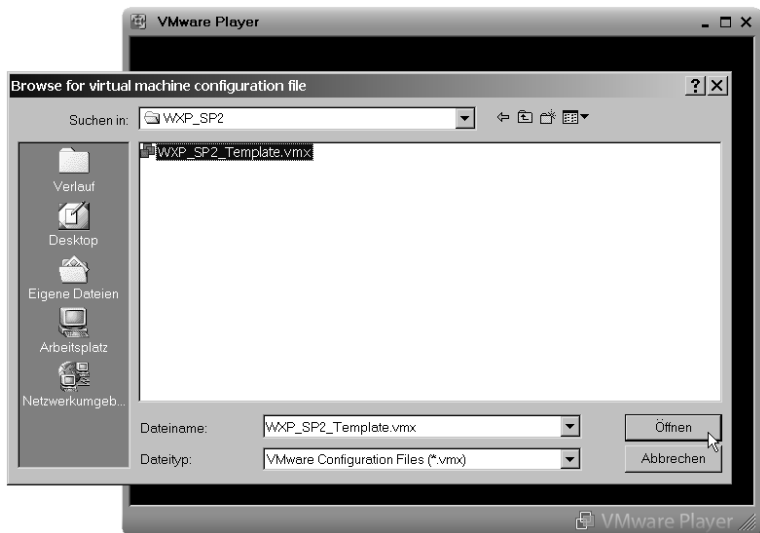
## 5.2 Umgang mit dem VMware Player

Der Player ist dank seiner abgespeckten Oberfläche sehr einfach zu bedienen.

### 5.2.1 Einschalten einer virtuellen Maschine und Abschalten mit PowerOff oder Suspend

Die verzweifelte Suche nach den Buttons für START, STOPP bzw. SUSPEND können Sie sich sparen – es gibt sie nicht. Beim Starten öffnet der Player automatisch einen Dialog, in dem Sie die Konfigurationsdatei einer vorhandenen virtuellen Maschine auswählen können (Abbildung 5.2). Diese VM startet dann sofort.

Abbildung 5.2:  
Durch direkte Auswahl der Konfigurationsdatei startet eine VM im Player



Startbare VMware-Konfigurationsdateien haben immer die Dateiendung \*.vmx. Konfigurationen von Virtual PC enden mit \*.vmc. Sie können diese Dateien auch direkt im Explorer mit einem Doppelklick starten.

#### Abschalten oder herunterfahren

Schließen Sie das Player-Fenster wieder, dann wird auch die VM automatisch beendet. Im Menü PLAYER/PREFERENCES können Sie festlegen, was beim Beenden mit dem laufenden System in der VM passiert (Abbildung 5.3). Ist *Power off the virtual machine* eingestellt, dann schaltet der Player die VM beim Schließen des Fensters einfach ab. Sind die VMware Tools in der Maschine installiert, dann fahren diese das Betriebssystem vorher automatisch herunter, andernfalls wirkt das Ausschalten wie ein virtueller Stromausfall.

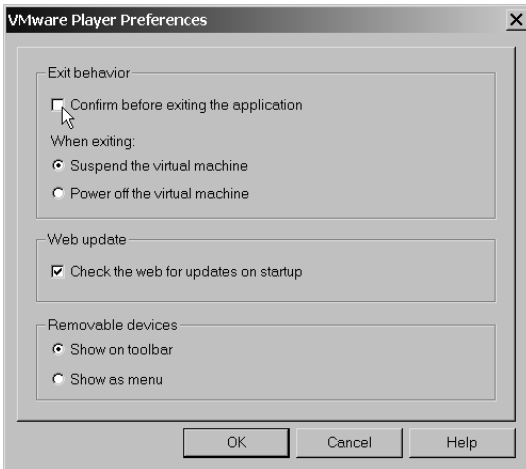


Abbildung 5.3:  
Das Menü **PLAYER/PREFERENCES** bestimmt, was beim Beenden mit dem laufenden System passiert

Bei der Einstellung *Suspend the virtual machine* werden dagegen der aktuelle Zustand und der RAM-Inhalt der Maschine vor dem Ausschalten abgespeichert. Wenn Sie die VM erneut starten, steht das System sofort wieder genau an der gleichen Stelle, ohne erst neu booten zu müssen. Ganze Demo-Umgebungen können Sie auf diese Weise vor der Produktvorstellung blitzschnell zum Leben erwecken.

### Suspend und Blitzstart

Für den Fall, dass der Gast einmal festhängt und sich partout nicht mehr beenden lässt, können Sie über den Menüpunkt **PLAYER/TROUBLESHOOT/POWER OFF** bzw. **RESET** buchstäblich den virtuellen Stecker ziehen (Abbildung 5.4).

### Hartes PowerOff

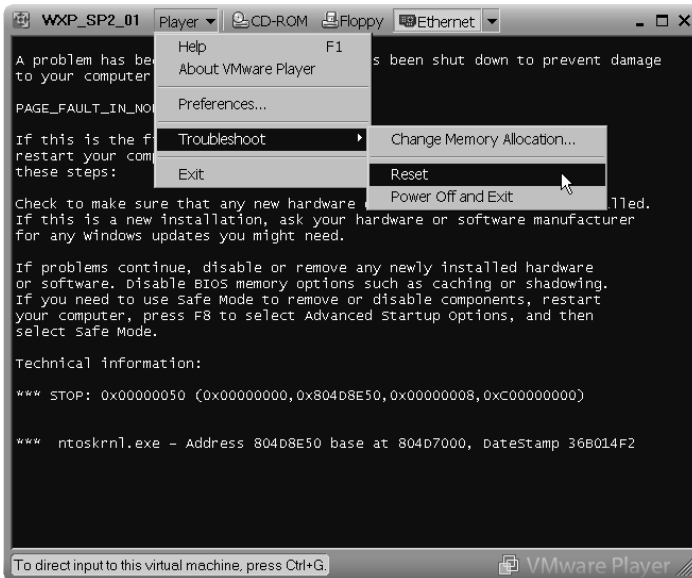


Abbildung 5.4:  
Hartes Abschalten ist möglich, wenn beim Testen in der VM einmal alles zu spät ist



### 5.2.2 Geräte und RAM einer VM zuweisen

CD, Floppy und die Netzwerkkarten hängen Sie im Menü an oder ab. Die VM „denkt“ dabei, Sie haben das Netzkabel entfernt oder die CD ausgeworfen. Im Menü PLAYER/TROUBLESHOOT können Sie die RAM-Größe der VM an Ihre Gegebenheiten auf dem Host anpassen. Lassen Sie immer genug Hauptspeicher für Ihr Wirtssystem übrig. Das war es dann auch schon, Geräte hinzufügen oder entfernen können Sie im Player nicht.

### 5.2.3 Der virtuelle Bildschirm der Gäste

**Auflösung des Gastes skalieren**

Ändern Sie durch Ziehen mit der Maus die Größe des Fensters einer laufenden VM, dann skaliert der Player die Auflösung des Gastsystems stufenlos und passt sie der neuen Größe und dem Seitenverhältnis an. Dazu müssen in der VM die VMware Tools installiert sein. Auf diese Weise können Sie in einem Gast auch Widescreen-Auflösungen für Programmtests nachbilden.

**Den Gast in den Vollbildmodus schalten**

Zur besseren Bedienung können Sie den Gast auch in den Vollbildmodus umschalten. Das erledigen Sie mit dem üblichen Windows-Symbol zum Maximieren oben rechts im Fenster. Der Gast scheint dann direkt auf dem Host-Rechner zu laufen. Mit der Tastenkombination **[Strg] + [Alt]** oder über die kleine eingblendete Leiste am oberen Rand des Vollbildes verbannen Sie die VM wieder zurück ins Fenster.

## 5.3 VMs für den Einsatz im Player vorbereiten und optimieren

Um eine virtuelle Maschine mit dem Player weiterzugeben, kopieren Sie einfach den gesamte Ordner einer VM. So können Sie VMs auf andere Rechner über das LAN oder auf einer USB-Platte übertragen. Wenn das Transportmedium allerdings platzbeschränkt oder langsam ist, etwa eine DVD bzw. das Internet, sollten Sie die VM vor der Weitergabe optimieren.

### 5.3.1 Die virtuellen Platten optimieren

**Platten in 2-GB-Streifen verwenden**

Zur Vorbereitung für die Weitergabe über eine DVD können Sie bei der Erstellung der virtuellen Platten den Haken an *Split disk into 2 GB files* setzen. Dadurch teilt VMware die Plattendateien in 2-GB-Happen auf (Abbildung 5.5), die sich später auch bei größeren VMs problemlos auf mehrere DVDs verteilen lassen.

Schon vorhandene monolithische virtuelle Platten, die bereits nicht mehr auf eine DVD passen, können nachträglich mit dem Kommandozeilentool *VMware Disk-Manager* in 2-GB-Streifen aufgeteilt werden (siehe dazu auch *Abschnitt 5.4, „Platz in den Gästen sparen“*).

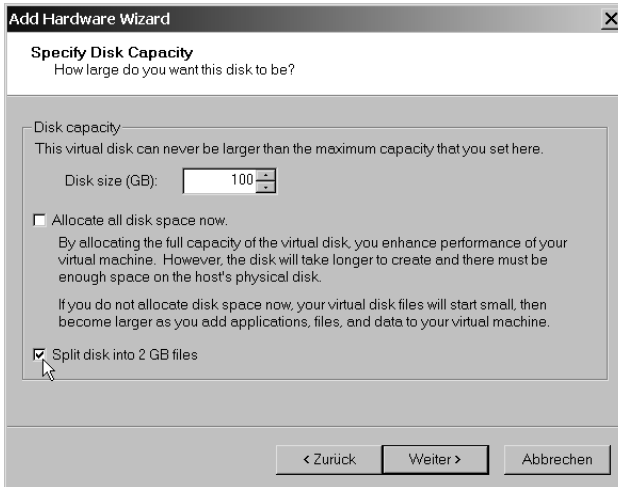


Abbildung 5.5:  
Bei der Erstellung der virtuellen Platten im Server oder in der Workstation sollten 2-GB-Segmente verwendet werden

Standardmäßig verwendet VMware Workstation Zuwachsplatten. Das bedeutet, eine 100-GB-Platte belegt nur so viel Platz, wie das System in der VM wirklich verwendet. Das verhindert Platzverschwendung und Verschnitt durch zu groß angelegte virtuelle Platten. Beim VMware Server sollten Sie beim Erstellen einer Platte den automatisch gesetzten Haken *Allocate all disk space now* entfernen, sonst entsteht keine Zuwachsplatte, sondern der Wizard reserviert den gesamten Plattenplatz schon vor (Abbildung 5.5). Weitere Informationen zu den virtuellen Platten finden Sie in *Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“*.

**Zuwachsplatten verwenden**

### 5.3.2 Snapshots mit dem VMware Player benutzen

Der Player bietet zwar keinen Snapshot-Manager, um Wiederanlaufpunkte zu setzen und Änderungen zu verwerfen, trotzdem können Sie einige Funktionen nutzen. Der Gast startet im Player immer mit dem Snapshot, der zuletzt im Vollprodukt aktiv war. Ein Wechsel zu einem anderen Snapshot ist im Menü des Players nicht möglich.

**Wiederanlaufpunkte**



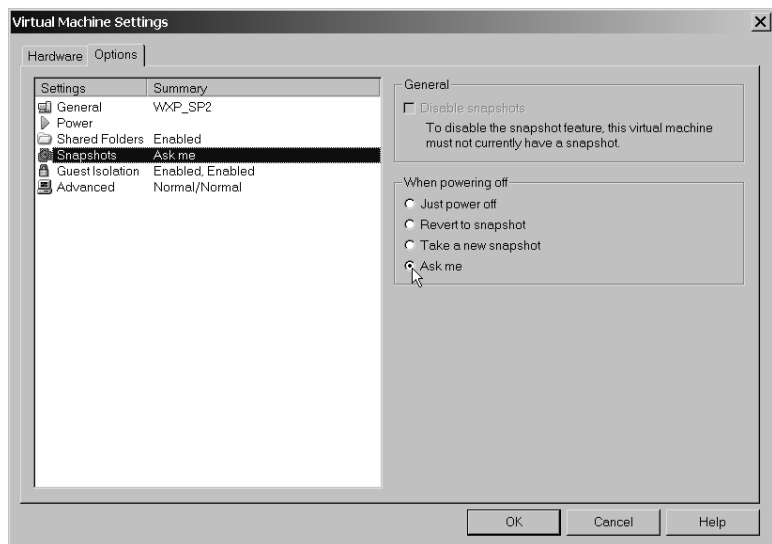
Bei aktivem Snapshot werden Änderungen nicht direkt auf die virtuelle Platte geschrieben, sondern in Redo-Logs zwischengepuffert. Diese Logs können Sie verworfen und damit auch alle Änderungen und verunglückten Tests im Gastsystem rückgängig machen. War kein Snapshot aktiv, werden Änderungen immer unwiderruflich auf die virtuellen Platten geschrieben. Details zu den Snapshots erfahren Sie in Teil 3, Kapitel 4, „Die Snapshot- und Clone-Funktion der VMware-Produkte“.

## Änderungen an virtuellen Platten verworfen

### Sauberer Grundzustand

Im Schulungsbetrieb oder für Kunden-Demos ist es nützlich, die virtuellen Maschinen jederzeit wieder in einen sauberen Grundzustand bringen zu können. Setzen Sie dazu in der Vollversion nach abgeschlossener Konfiguration der VM einen Snapshot. Im Menü der VMware Workstation oder des Servers können Sie unter SETTINGS/OPTIONS/ SNAPSHOTS einstellen, wie der Player später mit den Redo-Logs der virtuellen Platten umgeht (Abbildung 5.6).

Abbildung 5.6:  
Was mit den Redo-Logs der Snapshots im Player passiert, kann in der Workstation oder im Server voreingestellt werden



- ▶ *Just power off* – Die Redo-Logs der virtuellen Platten werden immer weiter fortgeschrieben. Der Anwender kann sie gegebenenfalls irgendwann manuell zurücksetzen.
- ▶ *Revert to snapshot* – Sämtliche Änderungen in den Redo-Logs werden beim Abschalten der VM immer ungefragt verworfen.
- ▶ *Take a new snapshot* – Diese Option unterstützt der Player nicht, sie wirkt wie *Just power off*.

- *Ask me* – Der Player fragt beim Abschalten der VM, was mit den Redo-Logs passieren soll. Sie entscheiden selbst, ob Sie zum Grundzustand zurückkehren oder nicht (Abbildung 5.7). Der Player fragt nur beim Abschalten, nicht im Suspend-Modus (siehe Abschnitt 5.2.1, „Einschalten einer virtuellen Maschine und Abschalten mit PowerOff oder Suspend“).

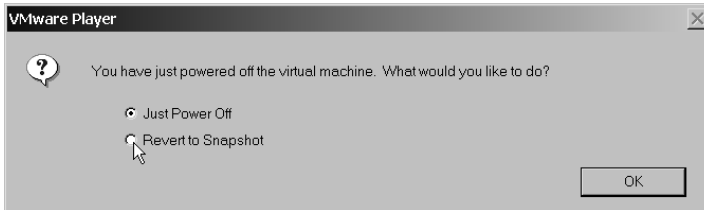


Abbildung 5.7:  
Ist die richtige  
Option gesetzt, fragt  
der Player beim  
Abschalten, was  
mit den Änderungen  
passieren soll

## Separate Datenplatten im Gast verwenden

Manchmal ist es bei der Verwendung von Snapshots sinnvoll, eine separate Datenplatte im Modus *Independent persistent* zu betreiben. Auf diese Weise bleiben Daten erhalten, die während der Demo oder Schulung eingepflegt wurden, auch wenn die Änderungen am Gastsystem verworfen werden. Dieser Modus lässt sich in den Vollprodukten vor dem ersten Snapshot über den Button **ADVANCED** bei den Einstellungen einer Platte festlegen (Abbildung 5.8). Eine virtuelle Platte in diesem Modus wird immer unwiderruflich beschrieben, auch wenn die VM einen Snapshot hat.



Abbildung 5.8:  
In der Vollversion  
kann zu jeder Platte  
unter **ADVANCED**  
der Modus einge-  
stellt werden

### 5.3.3 Linked Clones mit dem VMware Player benutzen

#### Eine Basisplatte für mehrere VMs

Grundsätzlich können Sie VMs einfach komplett kopieren und so beliebig viele Klone herstellen. Das verschwendet aber bei größeren Umgebungen unnötig viel Platz, wenn Sie sowieso immer das gleiche OS verwenden. VMware Workstation verfügt über eine Funktion, um so genannte *linked Clones* zu erstellen (siehe dazu auch *Teil 3, Kapitel 4, „Die Snapshot- und Clone-Funktion der VMware-Produkte“*). Die platzsparenden *linked Clones* funktionieren auch unter dem Player. Bei dieser Art von Klon setzen verschiedene Maschinen bei einer Grundinstallation auf ein und derselben virtuellen Platte auf. Die Maschinen könne trotzdem völlig unabhängig betrieben werden, da VMware Änderungen in separate Redo-Logs schreibt. Damit wird z.B. die 2 Gigabyte große Grundinstallation einer Maschine nur ein einziges Mal benötigt. Weitere Gäste mit dem gleichen Betriebssystem verwenden dieselbe Basisplatte und schreiben nur ihre individuellen Änderungen in eigene Redo-Logs. Das kann sehr praktisch beim Weitergeben größerer Testumgebungen sein.

#### Absolute Pfade in relative Pfade ändern

Allerdings verwenden *linked Clones* in der *vmx*-Datei absolute Pfade als Verweis auf die Mutter-VM, was vor allem beim Weitergeben zum Problem wird. Nach dem Kopieren auf einen anderen PC liegen die VMs in völlig anderen Verzeichnisstrukturen, die Klone können so nicht starten, weil sie die zugrunde liegende Mutter-VM nicht finden. Die absoluten Pfadangaben müssen in der *vmx*-Datei manuell in relative Pfade geändert werden.

Die *linked Clones* sollten Sie grundsätzlich in eigenen Unterverzeichnissen direkt im Ordner der Mutter-VM anlegen. Das sorgt für kurze Pfadangaben und gewährleistet nach dem Kopieren, dass der Pfad relativ zur Mutter-VM gleich bleibt. Nach dem Erstellen des *linked Clones* in der VMware Workstation über VM/CLONE passen Sie folgende Einträge in den *vmx*-Dateien der Klone manuell mit einem Texteditor an, ersetzen Sie dabei den Namen der Konfigurationsdatei der Mutter-VM:

```
fileSearchPath = ".;..\\"
cloneOf0 = "..\name_der_mutter_vm.vmx"
```



Existieren vor dem Klonen schon *Independent*-Platten, lassen sich über den Wizard nur noch *full Clones*, also komplette Kopien, erstellen. Legen Sie diese Platten gegebenenfalls erst nach dem Erstellen der *linked Clones* in jedem Gast separat an.

### 5.3.4 Der Player kennt keine Teamfunktion der VMware Workstation

Die Teamfunktion der VMware Workstation kennt der Player nicht. Als Alternative bietet sich an, Verknüpfung zu allen *vmx*-Dateien der einzelnen virtuellen Maschinen an einer zentralen Stelle abzulegen. Das ermöglicht dem Anwender, sofort mit einem Doppelklick die benötigten VMs im Player zu starten. Ein Hochfahren zusammenhängender Teams ist mittels Batch-Datei und Startbefehl auf diese Weise ebenfalls möglich.

VMs, die unter VMware Workstation in ein Team eingebunden wurden, lassen sich unter dem Player nicht starten (Abbildung 5.9). Lösen Sie VMs aus dem Team, bevor Sie diese weitergeben. Nachträglich können Sie auch folgenden Eintrag manuell aus der *vmx*-Datei entfernen:

```
inVMTeam = "TRUE"
```

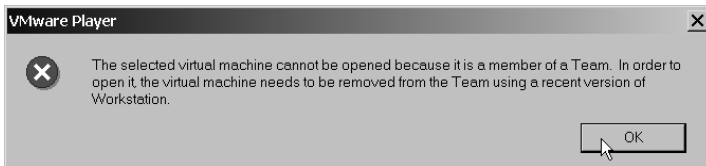


Abbildung 5.9:  
Teams werden vom  
Player nicht unter-  
stützt

### 5.3.5 Dualprozessor-VMs im Player betreiben

Wenn Sie die Quellmaschine unter dem Server oder der Workstation mit zwei virtuellen Prozessoren eingerichtet haben, wird es damit Probleme geben. Der Player reicht immer nur eine CPU an die Gäste durch, VMs mit Dual-CPU müssen für den Betrieb im Player auf eine CPU umgestellt werden. Im Gastbetriebssystem muss die Dualprozessor-Unterstützung abgeschaltet werden. Ein Gast mit Windows NT 4 läuft sonst in einen Blue Screen, bei anderen Windows-Versionen steht die CPU des Host-Systems auf 100% Last. Hintergründe und Vorgehensweise dazu finden Sie in *Teil 3, Kapitel 6, „P2V – physische Server in virtuelle Maschinen übernehmen“*.

**Blue Screen**

### 5.3.6 VMs von einem Linux-Host im Player benutzen

Wollen Sie VMs von einem Linux-Host im Player auf einem Windows-System laufen lassen, dann müssen Sie in der *vmx*-Datei teilweise die Pfade für Floppy und CD-ROM anpassen. Sonst können diese Geräte im Player unter Umständen nicht verwendet werden (Abbildung 5.10). Suchen Sie folgende Einträge in der *vmx*-Datei:

**Floppy und  
CD-ROM**

```
floppy0.fileName = "/dev/fd0"
ide1:0.fileName = "/dev/cdrom"
```

Und ersetzen Sie diese durch folgende:

```
floppy0.fileName = "A:"
ide1:0.fileName = "auto detect"
```

Abbildung 5.10:  
Vor allem bei älteren  
Konfigurations-  
dateien kann es beim  
Wechsel von Linux  
zu Windows Prob-  
leme geben



### 5.3.7 Lauffähige VMs verteilen und weitergeben

Die vorbereiteten und getesteten VMs können Sie per DVD, USB-Platte oder Internet verteilen. Die Betriebssysteme in den Maschinen benötigen dabei natürlich entsprechende Lizenzen, wenn keine freie Software verwendet wird.



Beachten Sie beim Verteilen mittels DVD, dass nach dem Kopieren von DVD auf Festplatte die Zielf Dateien oft schreibgeschützt sind. Vor dem Start der VMs müssen Sie deshalb das Attribut *Nur Lesen* aller Dateien in den Verzeichnissen der VMs zurücksetzen.

## 5.4 Platz in den Gästen sparen

Um beim Transportieren der virtuellen Maschinen möglichst viel Platz zu sparen, sollten Sie vor der Weitergabe in der Vollversion einige Vorkehrungen treffen:

- ▶ *Snapshots ausdünnen* – Jeder Snapshot belegt zusätzlichen Platz, da Sektoren der Platte in jedem Redo-Log mehrfach enthalten sein können. Löschen Sie im Snapshot-Manager alle unnötigen Snapshots. Einer genügt normalerweise für den Einsatz im Player, da zwischen ihnen sowieso nicht gewechselt werden kann.
- ▶ *Snapshots im laufenden Betrieb* – Ein Snapshot im laufenden Betrieb sichert auch den RAM-Inhalt einer VM. Haben Sie der Maschine 256 MB RAM zugewiesen, dann entsteht bei jedem Snapshot eine Datei in dieser Größe. Erstellen Sie den abschließenden Snapshot vor der Weitergabe also im abgeschalteten Zustand der VM.
- ▶ *Kein Suspend* – Auch bei einem Suspend wird der RAM-Inhalt in einer Datei gespeichert. Also fahren Sie die VM richtig herunter vor der Weitergabe.
- ▶ *Platten in Segmente teilen* – Platten, die zu groß für eine DVD sind, können mit folgendem Kommando nachträglich in 2-GB-Segmente aufgeteilt werden, wenn das bei der Erstellung verpasst wurde:

```
C:\Programme\VMware\VMware Workstation\
vmware-vdiskmanager.exe" -r quellplatte.vmdk -t 1
zielplatte.vmdk
```

- ▶ *Platten mit Shrink verkleinern* – Zuwachsplatten belegen zwar nur den Platz, der in der VM wirklich belegt ist. Wurden Inhalte im Gast wieder gelöscht, werden Zuwachsplatten aber nicht automatisch kleiner. Die Shrink-Funktion der VMware Tools gibt nicht benötigten Platz von Zuwachsplatten wieder frei, siehe Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“.
- ▶ *Linked Clones* – Für mehrere VMs mit dem gleichen Betriebssystem können Sie *linked Clones* anlegen, damit die Grundinstallation nur ein einziges Mal auf eine DVD muss (siehe auch Abschnitt 5.3.3, „Linked Clones mit dem VMware Player benutzen“).
- ▶ *Separate virtuelle Platte für das Swapfile* – Auch das Swapfile im Gastsystem einer VM benötigt Platz. Liegt es auf einer extra Platte, können Sie diese vor dem Brennen mit einer Version ersetzen, in der das File noch leer war.
- ▶ *Komprimierung* – Die VMs zu komprimieren spart zwar Platz, benötigt aber sehr viel Zeit zum Auspacken. Sinnvoller kann eine Verwendung von komprimierten Dateisystemen in den VMs selbst sein.

## 5.5 Netzwerkunterstützung des VMware Players

Die Netzwerkfunktionalität steht im Player fast uneingeschränkt zur Verfügung (Abbildung 5.11). Etwas problematisch ist der Aufbau eines abgeschotteten Testnetzwerks, da sich der Modus *Custom* im Player nicht über das Menü einstellen lässt. Lesen Sie zum besseren Verständnis des Netzwerks bitte Teil 3, Kapitel 1, „Virtuelle Netzwerke Teil 1 – Schnellstart“, und Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“.



Abbildung 5.11:  
Der Custom-Modus  
fehlt im Menü vom  
Player



## Custom-Netz für abgeschottete Testnetzwerke

### Abgeschottete Testnetze

Im Custom-Modus kommunizieren mehrere VMs, etwa in einem Demo-Netzwerk, intern an einem virtuellen Switch, ohne das echte LAN zu stören. Um VMs auf diese Weise virtuell zu verkabeln, benötigt der Host nicht einmal eine physische Netzwerkkarte. Wenn Sie die VM unter der VMware Workstation, bzw. dem Server, vorbereitend mit Netzwerkkarten im Modus Custom ausstatten, dann funktionieren sie im Player ohne Probleme. Wenn aber ein Anwender im Player einmal den Modus NAT, Host-only oder Bridged auswählt, kann er nicht wieder auf Custom zurückschalten. Das Menü bietet diesen Modus nicht an. Hier hilft eine zusätzliche Kopie der *vmx*-Datei mit den originalen Einstellungen, die im Notfall zurückkopiert werden kann, oder ein Snapshot, der ebenfalls die Originalkonfiguration wieder herstellt.



Durch manuelles Editieren der *vmx*-Datei ist unter dem Player eine freie Konfiguration des Netzwerks möglich (siehe auch unter Abschnitt 5.6, „Versteckte Funktionen zutage fördern“).

## Netzwerkverwaltung unter VMware Player mit *vmnetcfg.exe*

Mit dem Programm *vmnetcfg.exe* können Sie auch unter dem Player die virtuellen Netzwerke genauso verwalten, wie es in den Netzwerkworkshops im Teil 3 des Buches beschrieben ist. Sie finden das Tool auf Ihrer Festplatte im Programmverzeichnis des Players.

## 5.6 Versteckte Funktionen zutage fördern

### vmx-Datei editieren

Viele der Einschränkungen des Players können Sie durch direktes Editieren der Konfigurationsdatei umgehen. So kann der Endanwender nachträglich einige Änderungen an der Konfiguration vornehmen, ohne erst die VMware Workstation oder den VMware Server zu installieren.

### 5.6.1 Netzwerkkarten hinzufügen oder im Custom-Modus betreiben

Folgende Einträge in der *vmx*-Datei fügen eine zweite virtuelle Netzwerkkarte im Custom-Modus am virtuellen Switch VMNet3 hinzu. Genauso bringen Sie auch die vorhandene virtuelle Netzwerkkarte in den Custom-Modus. Mit diesen Einträgen kommunizieren mehrere VMs intern miteinander, auch völlig ohne physische Netzwerkkarte (Ersetzen Sie die Nummer bei *ethernetX* mit der Nummer der jeweiligen virtuellen Netzwerkkarte):

```
ethernet1.present = "TRUE"
ethernet1.startConnected = "TRUE"
ethernet1.connectionType = "custom"
ethernet1.vnet = "Vmnet3"
```

### 5.6.2 Virtuelles CD-Laufwerk mit ISO-Image betreiben

Der Player verwendet standardmäßig das physische CD-Laufwerk Ihres Computers. Wenn Sie ein ISO-Image als CD in einem Gast einlegen wollen, dann suchen Sie folgende Zeilen:

```
ide1:0.fileName = "auto detect"
ide1:0.deviceType = "cdrom-raw"
```

Und ändern Sie diese in:

```
ide1:0.fileName = "e:\iso_images\meine_cd.iso"
ide1:0.deviceType = "cdrom-image"
```

### 5.6.3 Virtuelle Platten hinzufügen

Auch eine zusätzliche Platte können Sie einbinden. Dazu müssen Sie die Behälterdatei einer vorhandenen Disk kopieren und der *vmx*-Datei zuweisen. Achten Sie auf den Typ der Platte, SCSI oder IDE:

```
ide0:1.present = "TRUE"
ide0:1.fileName = "Kopie_einer_Platte.vmdk"
ide0:1.deviceType = "disk"
```

### 5.6.4 UUID-Abfrage nach dem Kopieren unterdrücken

Auch die lästige Frage zum Erstellen eines neuen *Unique Identifiers (UUID)*, die nach dem Kopieren der VMs immer erscheint, lässt sich unterdrücken. So erstellt VMware einfach immer eine neue UUID in den kopierten Maschinen:

```
uuid.action = "create"
```

### 5.6.5 Arbeit mit Snapshots, die in den Vollprodukten gesetzt wurden

Mit folgenden Zeilen stellen Sie den Modus zum Verwerfen oder Aufheben der Änderungen am Snapshot ein (siehe auch *Abschnitt 5.3.2, „Snapshots mit dem VMware Player benutzen“*):

- ▶ Immer nachfragen:  
undopoint.action = "prompt"
- ▶ Immer verwerfen:  
undopoint.action = "autoRevert"
- ▶ Weiter fortführen:  
undopoint.action = "keep"

Eine Musterdatei mit weiteren wichtigen kommentierten *vmx*-Einträgen der VMware Workstation finden Sie auf der Buch-CD.



## 5.7 Gäste von Microsoft Virtual PC im VMware Player betreiben

Auch Maschinen von der Konkurrenz laufen im VMware Player. Eine \*.vmc-Datei eines Gastes von Virtual PC oder Virtual Server können Sie ganz einfach im Player auswählen. Damit geben Sie auch als Virtual PC-Nutzer Gäste mit dem kostenlosen Player weiter. Zusätzlich unterstützt der Player Images von *Symantec LiveState Recovery*.

### Keine Differenzplatten

Leider kommt der Player nicht mit den Differenzplatten der Microsoft-Produkte zurecht und produziert nur eine Fehlermeldung über eine defekte Datei (Abbildung 5.12). Wollen Sie also Maschinen von Microsoft mit dem Player weitergeben, müssen Sie vorher alle Differenzplatten zu einer einzigen Basisplatte verdichten.

Abbildung 5.12:  
Differenzplatten  
werden vom Player  
nicht erkannt



## 5.8 Neue VMs für den Player ohne Vollprodukt erstellen

### Mustervorlagen

Um neue VMs für den Player zu erstellen, benötigen Sie eigentlich nur eine Musterkonfigurationsdatei und eine leere virtuelle Platte. Diese Vorlage können Sie beliebig vervielfältigen und im Player starten. Wenn Sie eine Installations-CD ins Laufwerk Ihres PC einlegen oder ein ISO-Image in der *vmx*-Datei einbinden, dann können Sie auf der leeren virtuellen Platte ein neues Betriebssystem installieren und im VMware Player laufen lassen.



Auf der Buch-CD befindet sich ein Muster für eine leere virtuelle Maschine, die Sie sofort für den Player als Vorlage verwenden können.

### Konfigurationstools

Mittlerweile gibt es einige Webseiten, die *vmx*-Generatoren anbieten, mit denen sich gültige Konfigurationsdateien erstellen lassen, z.B.:

<http://petruska.stardock.net/Software/VMware.html>

<http://www.consolevision.com/members/dcgrendel/vmxform.html>

Nicht zuletzt erhalten Sie auf den VMware-Webseiten fertig installierte virtuelle Maschinen mit den unterschiedlichsten Gastsystemen:

<http://www.vmware.com/vmtn/appliances/>

Wenn Ihnen das alles zu umständlich ist, dann erstellen Sie sich mit dem kostenlosen VMware Server oder der 30 Tage lauffähigen Evaluierungsversion der VMware Workstation komfortabel einen Satz Mustergäste für den späteren Einsatz im Player.

Einziges Problem bei selbst erstellten virtuellen Maschinen sind die VMware Tools, die zum Player nicht mitgeliefert werden. Die ISO-Images, auf denen die Tools untergebracht sind, erhalten Sie aus einer Evaluierungsversion der VMware Workstation oder vom kostenlosen VMware Server. Diese ISO-Images binden Sie als CDs in die VM ein und installieren die Tools im Gast über die Datei *setup.exe*. Weitere Infos zu den Tools erhalten Sie in *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*.

#### VMware Tools

Wenn Sie die Vollprodukte nicht erst installieren wollen, dann können Sie die ISO-Images der Tools mit jedem ZIP-Programm direkt aus den Installationspaketen der Linux-Version des kostenlosen VMware Servers (Endung *\*.tar.gz*) entpacken. Die Datei *windows.iso* enthält beispielsweise die Tools für Windows-Gäste.





# 6 Schulung und Demo mit VMware Player und Workstation

Sie bauen eine Schulungs- oder Demo-Umgebung mit dem kostenlosen VMware Player oder der komfortablen VMware Workstation in nicht mehr als einer Stunde auf. Der Workshop zeigt auch das Zusammenspiel der Produkte. Nebenbei erlernen Sie die Verwendung des VMware Players mit einer Vorlage-VM von der Buch-CD.

**Geld und Zeit sparen**

Mit dem VMware Player sparen Trainer, Lehrkräfte und experimentierfreudige Laien jede Menge Geld, Zeit und Nerven. Das Konzept ist genauso mit den Microsoft-Produkten zu realisieren, etwa mit Virtual PC 2004.

## Workshop im Überblick

### Hauptprodukt

- ▶ VMware Player oder Workstation (das Konzept kann auch mit Microsoft Virtual PC realisiert werden)

### Praktische Verwendung

- ▶ Sie bauen eine Schulungsumgebung auf und stellen jedem Teilnehmer unzerstörbare Testsysteme beliebiger Betriebssystemkonfigurationen schnell zur Verfügung.

### Schwerpunkte

- ▶ Schnelleinstieg zum VMware Player in Stichpunkten.
- ▶ VMs als Mustervorlagen installieren und verteilen.
- ▶ Sauberen Grundzustand einer VM sichern und wiederherstellen.
- ▶ Klonen auf Basis einer und derselben virtuellen Platte erstellen.

### Zielgruppe

- ▶ Schulen, Ausbilder, Trainer
- ▶ Software-Firmen, Entwickler, Vertriebsmitarbeiter
- ▶ Ambitionierte Laien

## 6.1 Virtuelle Maschinen in Schulungen einsetzen

### Flexibel und preiswert

Ausbilder mit EDV-Themen haben es schwer. Vor allem die große Anzahl unterschiedlicher Betriebssysteme sowie unüberschaubare Konfigurationen verschiedenster Anwendungen bringen die Administratoren der Klassenräume, in den meisten Fällen also die Lehrkräfte selbst, zunehmend ins Schwitzen. Den geplagten Trainern und Lehrern können virtuelle Maschinen das Leben wieder erleichtern. Sie sind wesentlich flexibler als Dual-Boot-Installationen, Platten-Images oder PC-Wächterkarten. Und mit dem kostenlosen VMware Player ist diese Lösung auch äußerst preiswert.



Auf der Buch-CD befindet sich eine lauffähige Vorlage-VM, die Sie beliebig vervielfältigen können und in der sich verschiedene Betriebssysteme installieren können.

### 6.1.1 Vorteile und Nachteile einer virtuellen Schulungs- oder Demo-Umgebung

Hier ein paar Vorteile, die sich durch die Verwendung virtueller Maschinen auf den Schulungs-PCs ergeben:

- Viele Vorteile**
- ▶ *Unterschiedliche Konfigurationen blitzschnell bereitstellen* – Beim Wechsel der Klasse oder des Ausbildungsthemas können innerhalb von Minuten vorbereitete spezifische Konfigurationen bereitgestellt werden; mit beliebigen Betriebssystemen und beliebigen Anwendungen. Jeder Ausbilder kann sicher sein, zum Stundenbeginn eine saubere, zum Thema passende Umgebung vorzufinden.
  - ▶ *Mehrere Betriebssysteme gleichzeitig auf einem PC* – Problemlos kann jeder Teilnehmer sein eigenes Testnetz auf einem PC betreiben, z.B. um die Anbindung eines Clients an einen Server durchzuspielen. Sogar Linux läuft parallel zu Windows oder Netware.
  - ▶ *Personalisierte Installationen* – Teilnehmer können Ihre eigene Umgebung auf Datenträgern, dem Laptop oder sogar auf dem USB-Stick mitnehmen, um zu Hause weiterzuüben. Später kann diese persönliche Umgebung jederzeit wieder auf dem Schulungs-PC weiterverwendet werden.
  - ▶ *Keine Image-Sicherung, Wächterkarte oder Dual-Boot nötig* – Die umständliche Verwaltung mehrerer Partitionen oder Platten-Images entfällt. Auf dem Schulungs-PC wird nur noch ein einziges sauberes Host-System benötigt, an dem nicht direkt gearbeitet wird.
  - ▶ *Immer wieder sofort zur sauberen Grundinstallation* – Jede Testumgebung kann in Sekunden in ihren ursprünglichen sauberen Grundzustand zurückgesetzt werden.

Zwei Nachteile will ich Ihnen nicht verheimlichen:

**Wenige Nachteile**

- *Performance* – Virtualisierung kostet ein wenig Leistung. Vor allem im Grafikbereich gibt es Einschränkungen, etwa wenn Multimedia- oder CAD-Anwendungen zum Einsatz kommen.
- *Eingeschränkte Hardware* – Spezielle Hardware, wie Audio-Installationen, Messplätze o.Ä., können in einer VM nicht immer verwendet werden.

In diesen Fällen bietet es sich an, problematischen Anwendungen parallel zu den virtuellen Testumgebungen direkt auf den Schüler-PC zu installieren, z.B. um auf bestimmte Labor-Hardware zuzugreifen. Am realen PC werden dann nur diese Anwendungen benutzt, getestet wird dagegen in den VMs.



## 6.2 Konzept der Schulungsumgebung mit dem VMware Player

Der Workshop verfolgt ein einfaches Konzept: Auf einem Master-PC erstellen Sie verschiedene Gäste mit unterschiedlichen Betriebssystemen und Konfigurationen. Die erstellten Vorlagen werden dann auf die Schulungsplätze verteilt. Dort laufen diese VMs im kostenlosen VMware Player. Ein paar Zusätze verfeinern das Ganze, z.B. das platzsparende Klonen durch Verwendung einer einzigen Basisinstallation oder das Abspeichern individueller Änderungen der Schüler auf einem USB-Stick.

### 6.2.1 Der Master-PC zum Erstellen und Verwalten der Vorlagen

Auf dem Master-PC erstellen Sie die Vorlagen für die virtuellen Schulungsmaschinen. Hier können Sie schon den VMware Player verwenden. Der Nachteil des Players ist die extrem eingeschränkte Oberfläche, mit der keine Konfiguration der Maschinen möglich ist. Auf der Buch-CD finden Sie deshalb ein ausreichend vorbereitetes Muster, aus dem Sie sehr einfach durch Kopieren weitere Gäste erstellen können (siehe Abschnitt 6.2.3, „Die Vorlage-VM auf der Buch-CD“).

**VMware Player**

### Alternativen für den Master-PC

Der Einsatz des ebenfalls kostenlosen VMware Servers auf dem Master-PC hätte den Vorteil, bei der Erstellung der Mustermaschinen wesentlich flexibler zu sein und mehr Komfort zu besitzen. Wir konzentrieren uns trotzdem auf den Player. Schon allein, damit Sie die notwendigen Interna beim Einsatz auf den Schüler-PCs kennen ler-

**VMware Server**



nen. Außerdem müssten Sie sich in den Server erst einarbeiten, was zwar kein Problem ist, aber mit dem Player und der Mustervorlage von der CD ist die Anwendung geradezu simpel.

**VMware  
Workstation**

Die ausgereifteste Lösung für den Master-PC ist die kostenpflichtige VMware Workstation, die es auch in einer 30 Tage lauffähigen Evaluierungsversion gibt. Sie bietet vor allem mehrere Snapshots, was in der Entwicklungsphase der Vorlagen von großem Nutzen sein kann. Damit lassen sich mehrere Wiederanlaufpunkte verwalten, z.B. zum Verwerfen fehlgeschlagener Installationsversuche. Weiterhin können Sie Versionen einer einzigen VM mit und ohne Service-Pack oder mit unterschiedlichen Browserversionen erstellen und je nach Bedarf verteilen. Das geht mit dem Server und dem Player nur eingeschränkt. Wichtige Hinweise zur Verwendung des Players in Verbindung mit VMware Workstation finden Sie in *Teil 2, Kapitel 5, „Virtuelle Umgebungen mit dem VMware-Player weitergeben“*.

## **6.2.2 Die Schüler-PCs als Wirtsrechner für die Schulungs-VMs**

Auf jedem Schüler-PC installieren Sie auf einer möglichst sauberen Grundinstallation von Windows oder Linux den VMware Player. Das ist völlig unkompliziert (siehe auch *Teil 1, Kapitel 3, „Installation und Konfiguration der einzelnen Produkte“*). Ein Image oder eine Wächterkarte kann diese Basis vor versehentlichen Änderungen schützen, das ist aber nicht unbedingt notwendig, da die Schüler nicht direkt am Wirtssystem arbeiten sollen.

Idealerweise haben die PCs eine Netzwerkkarte zum einfachen Verteilen und Kopieren der VMs über das LAN sowie ausreichend Plattenplatz für alle benötigten virtuellen Maschinen. Die Arbeit mit ein bis zwei virtuellen Maschinen ist ab 1 GB RAM und einer CPU ab 1,5 GHz möglich, bei genügsamen Gästen reichen bereits 512 MB physischer Hauptspeicher.

## **6.2.3 Die Vorlage-VM auf der Buch-CD**

Sie finden auf der Buch-CD eine Vorlage, die Sie für die Einrichtung Ihrer Muster-VMs verwenden können. Sie besteht eigentlich nur aus einer Konfigurationsdatei *vm.vmx* und einer leeren virtuellen Platte im Unterordner *sys*. In einem weiteren Unterordner *redologs* liegen später automatisch die aktuellen Änderungen der Teilnehmer. VMware kann alle Schreibzugriffe auf eine virtuelle Platte in so genannte Redo-Logs umleiten. Dadurch wird die originale Platte nicht angetastet, und später können die Änderungen in diesen Redo-Logs verworfen oder übernommen werden (siehe *Abschnitt 6.5, „Erweiterte Konzepte für die Verwendung der virtuellen Maschinen“*).

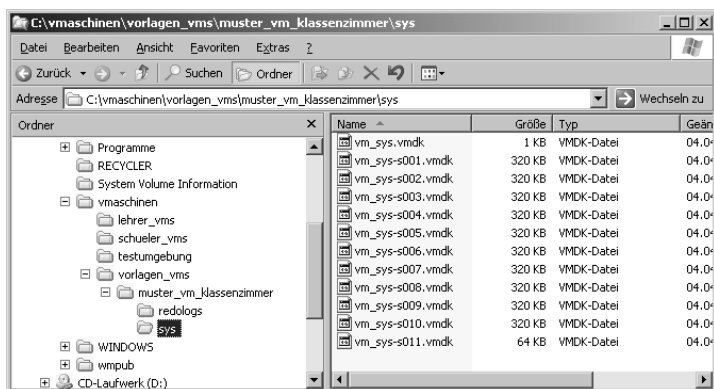


Abbildung 6.1:  
Die Muster-VM  
verfügt über eine  
20-GB-IDE-Platte,  
aufgeteilt in 2-GB-  
Segmente

Die virtuelle Platte *vm\_sys.vmdk* der Vorlage wurde als 20-GB-IDE-Platte erstellt, das bietet ausreichend Platz für die Anwendungen im Gast. Bei der Erstellung wurde die Platte in 2-GB-Segmente aufgeteilt, Sie sehen das an der Anzahl Dateien mit dem Namen *vm\_sys-sXXX.vmdk* mit laufender Nummer (Abbildung 6.1).

Die Aufteilung in Segmente ermöglicht ein Brennen auf DVD und eine einfachere Wiederholung von Kopiervorgängen bei Abbrüchen. Zur besseren Übersicht wurde ein eigenes Verzeichnis *sys* für die Platte angelegt, damit die vielen Plattendateien übersichtlich an einem separaten Ort liegen. Es handelt sich um eine Zuwachsplatte, was bedeutet, dass die Dateien nur so viel Platz belegen, wie das Gastsystem verwendet. Aus diesem Grunde sind die Dateien der leeren 20-GB-Platte auch noch sehr klein.

Durch Kopieren des gesamten Verzeichnisses mit der virtuellen Platte und zusätzliches Kopieren der Einträge in der *vmx*-Datei einer virtuellen Maschine könnten Sie der VM auch mehrere Datenträger zuweisen, das ist für unser Beispiel nicht notwendig. Mehr Informationen zu den virtuellen Platten finden Sie in *Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“*.

## 6.2.4 Andere Lösungsansätze mit einem zentralen VMware Server anstelle des Players

Sie können den kostenlosen VMware Server ebenfalls auf jedem Arbeitsplatz installieren, aber der Player ist schlanker. Vor allem verhindert seine eingeschränkte Oberfläche Spielereien der Lehrgangsteilnehmer und konzentriert sich auf das Notwendigste.

**VMware Server  
lokal oder als  
zentraler Host**

Eine weitere Möglichkeit sind die zentrale Bereitstellung eines leistungsfähigen Rechners mit VMware Server und die Installation der *VMware Server Console* zur Fernbedienung auf den Schülerplätzen. Hier setzt vor allem die Anzahl der Teilnehmer Grenzen, da zehn

gleichzeitig startende Windows-VMs selbst flotte Hardware in die Knie zwingen können. Dazu kommt ein wesentlich größerer Verwaltungsaufwand bei den Zugriffsrechten.

Die Vorteile wären eine zentrale Verwaltung der Gäste und ein zentral einsehbarer Bildschirm der Lehrgangsteilnehmer vom Lehrer aus über die VMware Server Console. Und selbst mit sehr alten und schwachen Schüler-PCs könnten die Teilnehmer problemlos mit modernen Betriebssystemen arbeiten, weil die Verarbeitung zentral auf einem leistungsstarken Host erfolgt. Vorausgesetzt die Teilnehmerzahl überfordert nicht den Host.

## 6.3 Erstellen der Muster-VMs als Vorlage für die Schulungssysteme unter dem Player

Der wichtigste Punkt des Konzeptes ist die Erstellung der Mustermaschinen, die dann später an die Schüler-PCs verteilt werden. Das Weitergeben ist unkompliziert und wurde bereits vollständig in *Teil 2, Kapitel 5, „Virtuelle Umgebungen mit dem VMware-Player weitergeben“*, beschrieben. Sollten Sie noch Fragen zum VMware Player haben, dann lesen Sie bitte das genannte Kapitel.

### 6.3.1 Schritt für Schritt: Anleitung zur Installation der Muster-VM

Hier finden Sie die Vorgehensweise zur Erstellung einer Schulungs- oder Demo-Umgebung mit dem Muster von der Buch-CD:

1. *Ordnerstruktur vorbereiten* – Zur besseren Übersicht sollten Sie eine Ordnerstruktur auf dem Master-PC anlegen. Einen Basisordner *vmaschinen* mit Unterordnern wie *testumgebung* und *vorlagen* bzw. *lehrer* und *schueler*. In diesen Ordnern liegen später die fertig konfigurierten VMs und die erstellten Vorlagen.
2. *Vorlage kopieren* – Kopieren Sie die Vorlage-VM von der Buch-CD in ein eigenes Verzeichnis auf dem Master-PC. Sie können die Vorlage immer wieder für neue VMs verwenden. Benennen Sie die Verzeichnisse der kopierten VMs nach einem sinnvollen System; entweder nach der Art der Betriebssysteminstallation in diesem Gast, nach Lehrthemen oder auch nach Klassen.

**System bei  
den Namen**



Von CD kopierte Dateien sind meistens schreibgeschützt. Entfernen Sie zuerst den Schreibschutz, bevor Sie mit der Installation in der VM beginnen, sonst kann der Gast nicht auf seine virtuelle Platte schreiben.

3. *Dokumentieren* – Legen Sie in jedem Verzeichnis eines Gastes eine Textdatei an, in der Sie genau dokumentieren, was Sie zu welchem Zeitpunkt an diesem Muster geändert haben. So wissen Sie später immer, was in diesem Muster installiert ist und welche Einstellungen, Patches oder Anwendungen bereits enthalten sind.
4. *Setup-CD des Gastbetriebssystems einlegen* – Legen Sie eine Installations-CD ins reale Laufwerk Ihres Master-PC ein. Die VM-Mustervorlage von der CD arbeitet standardmäßig damit. Oder verwenden Sie ein ISO-Image, suchen Sie dazu folgende Zeilen in der *vmx*-Datei der Mustervorlage:

```
idel:0.fileName = "auto detect"
idel:0.deviceType = "cdrom-raw"
```

und ersetzen Sie diese hiermit:

```
idel:0.fileName = "e:\iso_images\meine_cd.iso"
idel:0.deviceType = "cdrom-image"
```

5. *Typ des Betriebssystems festlegen* – Passen Sie in der *vmx*-Datei den Typ Ihres zu installierenden Betriebssystems an, indem Sie den richtigen Eintrag aus dem Ende der Datei kopieren. Das optimiert VMware für den Gast und führt unter anderem zu einer besseren Performance.
6. *VM starten* – Sie können mit einem Doppelklick auf die *vmx*-Datei die VM bereits im Player starten. Der VMware Player startet dadurch automatisch mit der virtuellen Maschine und versucht, von einer CD bzw. einem ISO-Image zu booten. Sie können auch den Player starten und dann im Startdialog zu Ihrer VM navigieren (Abbildung 6.2).

**CD oder  
ISO-Image  
verwenden**

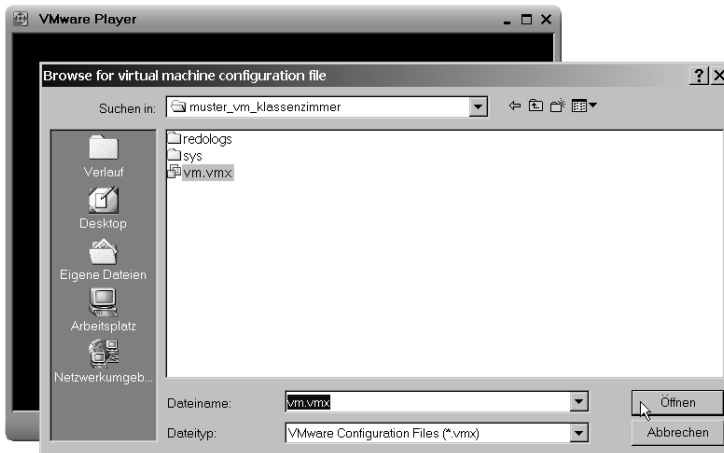


Abbildung 6.2:  
Gleich nach dem  
Start des Players  
muss in einem Dia-  
log die Konfigura-  
tionsdatei einer VM  
ausgewählt werden

7. *Betriebssystem installieren* – Der Gast erkennt die CD, und die Setup-Routine des Betriebssystems startet. Sie können eine ganz normale Systeminstallation auf der leeren virtuellen Platte durchführen (Abbildung 6.3). Da die Platte vom Typ IDE ist, gibt es keine Treiberprobleme im Gastsystem.



Um innerhalb der VM die Tastatur benutzen zu können, müssen Sie einmal in das Fenster des Gastes klicken, mit **[Strg] + [Alt]** kommen Sie wieder heraus.

Sollten Sie eine Installation wiederholen und die virtuelle Platte ist nicht mehr leer, dann kann es sein, dass der Gast nicht mehr von CD, sondern immer von der Platte bootet. Indem Sie beim Start im Gast die Taste **[F2]** festhalten, gelangen Sie ins virtuelle CMOS-Setup und können dort die Bootreihenfolge ändern.

Abbildung 6.3:  
Der Gast greift auf  
die CD im realen  
Laufwerk oder auf  
ein ISO-Image zu  
und installiert das  
Betriebssystem auf  
der virtuellen Platte



8. *VMware Tools installieren* – Gleich im Anschluss an die Betriebssysteminstallation sollten Sie im Gast die VMware Tools installieren. In reinen Text-VMs, z.B. einem Linux-Server, benötigen Sie die Tools nicht unbedingt. Unter Windows bringen die Tools vor allem eine frei skalierbare Bildschirmauflösung in der VM und fliegenden Wechsel der Maus zwischen Gast und Host (siehe Abschnitt 6.4, „Installation der VMware Tools in einem Gast unter dem VMware Player“).
9. *Netzwerk einrichten* – Die Vorlage von der Buch-CD arbeitet standardmäßig mit einer Netzwerkkarte im Modus *Bridged*, was bedeutet, das Gastsystem ist ein vollwertiger LAN-Client und verwendet die Netzwerkkarte in den Schulungs-PCs parallel zum Host-System mit. Wollen Sie dagegen zwei VMs nur intern kommunizieren lassen (z.B. Client und Server) ohne Kontakt zum Host oder zum LAN, dann suchen Sie in der *vmx*-Datei die Einträge *ethernet0.connectionType* und *ethernet0.vnet*, und ersetzen Sie die Zeilen durch folgende:

```
ethernet0.connectionType = "custom"
ethernet0.vnet = "Vmnet3"
```

Die Gäste bemerken nicht, dass sie nur an einem virtuellen Netzwerk angeschlossen sind, und können wie in einem richtigen LAN kommunizieren. Die Gastsysteme bleiben aber von Ihrem

LAN im Schulungsraum isoliert und können keinen Schaden anrichten. Detaillierte Infos zum Netzwerk finden Sie in *Teil 3, Kapitel 1* und *Kapitel 2*.

10. *Wiederanlaufpunkt (Snapshot) setzen* – Während der Betriebssysteminstallation schreibt die Vorlage-VM noch direkt auf die virtuelle Platte. Um den Teilnehmern jederzeit die Möglichkeit zu geben, zum sauberen Stand der Grundinstallation zurückzukehren, können Sie vor der Verteilung an die Arbeitsplätze in der VM ein *Redo-Log* einschalten. Alle weiteren Änderungen schreibt VMware in dieses Log und nicht mehr auf die virtuelle Platte. Das Gastsystem merkt davon aber nichts. Sie können alle Änderungen später wieder verwerfen, indem Sie die Redo-Logs einfach löschen (Abbildung 6.4). Um das Redo-Log einzuschalten, suchen Sie folgende Zeile in der vmx-Datei:

```
ide0:0.mode = "persistent"
```

Und ändern diese in:

```
ide0:0.mode = "undoable"
```

**Redo-Log  
einschalten**

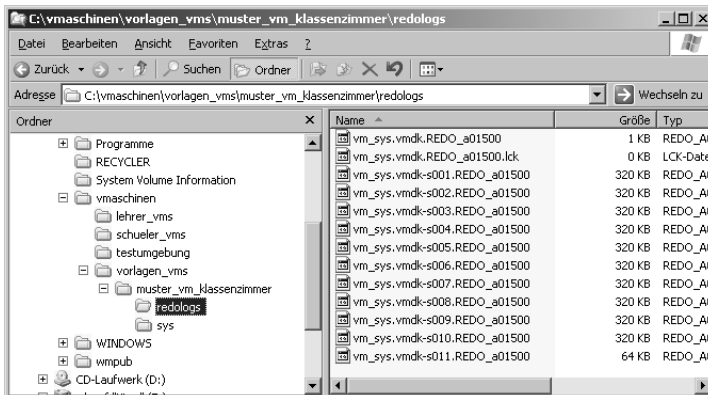


Abbildung 6.4:  
Das Redo-Log der  
virtuellen Platte puffert  
alle Änderungen.  
Durch Löschen des  
Logs werden Änderungen  
verworfen

11. *Gast in den Grundzustand zurücksetzen* – Im Verzeichnis *redologs* jeder VM entstehen beim Start Dateien mit der Erweiterung *REDO* und einer laufenden Nummer, z.B. *meine\_platte.vmdk.REDO\_a02360*. Das sind die Redo-Logs (Abbildung 6.4). Da wir eine Platte in 2-GB-Segmenten verwenden, entstehen mehrere solcher Dateien. In diesen Dateien stehen alle Änderungen, die ein Teilnehmer während der Sitzung gemacht hat. Durch einfaches Löschen dieser Dateien (nicht des Ordners!) versetzen Sie den Gast wieder in den Grundzustand. Das funktioniert nur bei ausgeschalteter VM.
12. *VMs verteilen* – Läuft Ihr Betriebssystem in der VM und sind alle Tools installiert, können Sie das komplette Verzeichnis als Vorlage sichern und auf jedem PC im Schulungsraum verteilen. Erstellen Sie eine Verknüpfung mit der *vmx*-Datei auf dem Desktop der Schüler-PCs, dann hat jeder Teilnehmer per Mausklick den ersten virtuellen Testrechner zur Verfügung.

## 6.4 Installation der VMware Tools in einem Gast unter dem VMware Player

Die VMware Tools sind vor allem für die komfortable Bedienbarkeit der Gäste wichtig. Sie bieten optimierte Bildschirmauflösungen und verbessern das Maushandling. Weiter Informationen zu den Tools finden in *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*.

### ISO-Images der VMware Tools

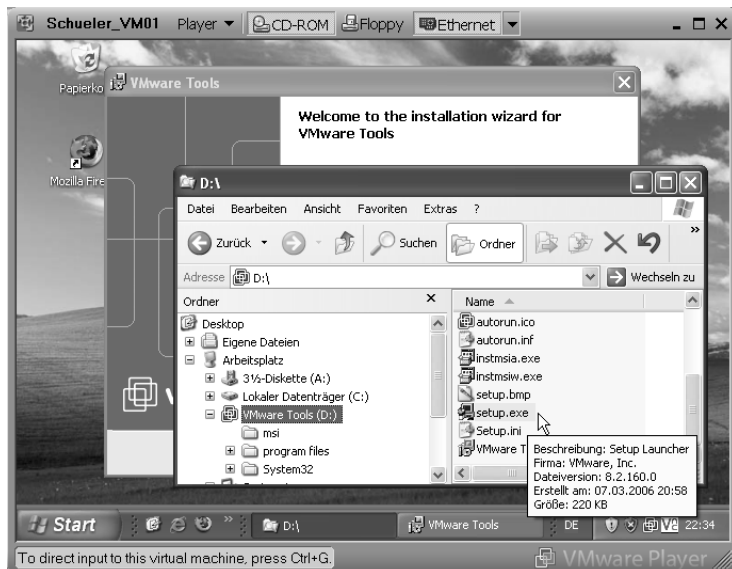
Zum Installieren der VMware Tools benötigen Sie die zugehörigen ISO-Images, auf denen sich die Dateien und das Setup befinden. In den Vollversionen von VMware werden diese ISO-Images mitgeliefert und über einen Menüpunkt automatisch in einem Gast als CD eingebunden, sobald ein Anwender die Tools installieren will. Mit dem Player werden die Tools nicht mitgeliefert.

Am einfachsten erhalten Sie die ISOs aus dem *tar.gz*-Paket für die Linux-Version des kostenlosen VMware Servers. Dieses Paket können Sie mit jedem ZIP-Programm dekomprimieren. Die Dateien sind nach dem Betriebssystem benannt und haben die Endung *\*.iso*, z.B. *windows.iso* oder *linux.iso*.

Nach dem Auspacken der Image-Datei ändern Sie wieder die Zeilen für die virtuelle CD-ROM in der Konfigurationsdatei *\*.vmx* in Ihrer VM (im ausgeschalteten Zustand) und weisen dort das ISO-Image der VMware Tools zu:

```
idel:0.fileName = "e:\ausgepackt\windows.iso"
idel:0.deviceType = "cdrom-image"
```

Abbildung 6.5:  
Das Setup der  
VMware Tools kann  
direkt von der virtu-  
ellen CD im Gast-  
system gestartet  
werden



Nach dem erneuten Start der virtuellen Maschine können Sie im Gast die CD mit dem Button CD-ROM verbinden. Eventuell startet dann das Setup der Tools im Gast bereits automatisch. Wenn nicht, starten Sie auf der im Gast erscheinenden CD die *Setup.exe* der VMware Tools mit einem Doppelklick (Abbildung 6.5).

## 6.5      **Erweiterte Konzepte für die Verwendung der virtuellen Maschinen**

Das Konzept kann noch um einige interessante Funktionen erweitert werden, z.B. platzsparendes Vervielfältigen der VMs.

### 6.5.1    **Zentrale Ablage der virtuellen Basisplatte mit linked Clones für die Schüler**

Um nicht Dutzende Male immer wieder die gleiche VM mit dem gleichen Betriebssystem für verschiedene Testszenarien und für verschiedene Teilnehmer oder Klassen auf den Schüler-PC vorzuhalten, können mehrere VMs eine virtuelle Platte gleichzeitig verwenden. Das funktioniert, da in den Gästen jeweils eigene Redo-Logs eingeschaltet sind., wodurch Änderungen nicht direkt auf die virtuelle Platte geschrieben werden, sondern in die Redo-Logs.

Damit ist es möglich, die virtuelle Platte einer Grundinstallation als Basisplatte an einer zentralen Stelle für mehrere VMs abzulegen. Alle weiteren VMs der Schüler verwenden dann diese zentrale Platte lesend, schreiben aber in eigene Redo-Logs, z.B. in einem Verzeichnis mit dem Namen des Schülers (Abbildung 6.6). Das Gastsystem bemerkt dabei keinen Unterschied (zu den Redo-Logs siehe auch Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“).

**Platz und Zeit  
zum Kopieren  
sparen**

Gehen Sie folgendermaßen vor, um wechselnden Schülern auf einem PC VMs mit der gleichen Basisplatte zur Verfügung zu stellen:

1. Kopieren Sie die vorbereitete Muster-VM mit installiertem Betriebssystem auf den Schüler-PC in ein zentrales Verzeichnis. Es genügt bereits die virtuelle Platte der VM.
2. Schützen Sie die kopierte Muster-VM vor Änderungen, entweder durch Dateirechte oder durch das Attribut *Schreibgeschützt*.
3. Kopieren Sie die Muster-VM ohne die virtuelle Platte in ein Vorlagenverzeichnis für die Schüler. Es genügen die Datei *\*.vmx* und das leere Verzeichnis *redologs* für die Redo-Log-Dateien, die beim ersten Start automatisch entstehen. Sie müssen nicht für jede VM eine eigene virtuelle Platte kopieren.

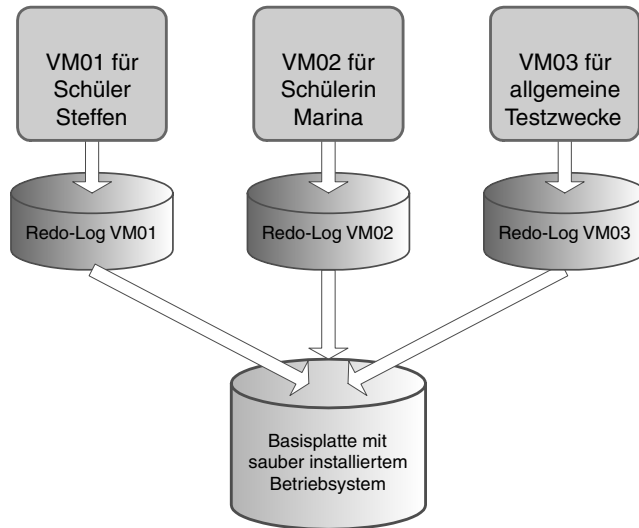


4. Passen Sie in der *vmx*-Datei der virtuellen Maschine den Pfad zur zentralen Basisplatte an, und schalten Sie die Redo-Logs ein:

```
ide0:0.fileName = "e:\pfad_zur_basis\
basisplatte.vmdk"
ide0:0.mode = "undoable"
```

5. Kopieren Sie diese vorbereitete VM in die jeweiligen Nutzerverzeichnisse. Bei Start der VM entstehen automatisch neue Redo-Logs, jeweils im Nutzerverzeichnis. Alle VMs lesen zwar von der gleichen Platte, schreiben aber in ihre eigenen Redo-Logs.

Abbildung 6.6:  
Verschiedene Redo-  
Logs entkoppeln die  
VMs von der virtuel-  
len Platte und ermög-  
lichen eine gemein-  
same Verwendung



Ein installiertes Muster von jedem Betriebssystem müssen Sie also nur ein einziges Mal schreibgeschützt auf jedem Arbeitsplatz-PC hinterlegen. Jede VM, die irgendwann einmal benötigt wird, verweist dann auf diese eine virtuelle Platte. Lange Kopiervorgänge am Beginn jeder Unterrichtseinheit fallen weg, für jeden Schüler müssen Sie nur noch eine vorbereitete Konfigurationsdatei kopieren.

Wichtig ist dabei, die zentrale Basisplatte vor Änderungen bzw. vor versehentlichem Löschen zu schützen, entweder über Dateirechte oder mit einem Schreibschutzattribut. Sollte doch einmal etwas passieren, können Sie diese Vorlage aber auch schnell wieder vom Master-PC kopieren.



Je nach Anzahl der Teilnehmer und Aktivität in den VMs funktioniert das in einem Gigabit-LAN sogar, wenn die Basisplatte zentral auf dem Fileserver oder auf einem NAS liegt.

## 6.5.2 Personalisierte Verwendung der Schüler-VMs

Wenn die Lehrgangsteilnehmer ihre eigenen Änderungen sichern wollen, dann könnten sie die komplette VM kopieren. Das nimmt allerdings Zeit und Platz in Anspruch, da eine Grundinstallation meist schon ein Gigabyte Platz belegt. Spätestens wenn die Änderungen auf einem USB-Stick gesichert werden sollen, reicht der Platz nicht mehr aus. Auch hier bietet sich eine Lösung über die Redo-Logs an. Auf den Schüler-PCs muss wieder nur eine zentrale Basisplatte zur Verfügung stehen.

Am Ende einer Sitzung sichert der Teilnehmer nur die Redo-Logs (Abbildung 6.4), die meist recht klein sind, und die *vmx*-Datei mit der Konfiguration der VM auf einen USB-Stick oder auf eine CD. Bei der nächsten Sitzung kann er diese Dateien wieder in sein Verzeichnis einspielen, auch auf einem anderen Arbeitsplatz, und mit der gleichen Konfiguration weiterarbeiten, mit der die letzte Stunde endete. Dazu muss nur die gleiche Basisplatte wieder zur Verfügung stehen. Wenn Sie dem Teilnehmer eine DVD mit der Basisplatte zur eigenen Verwendung mitgeben (Betriebssystemlizenzen beachten!), kann er seine Konfiguration sogar zu Hause oder in der eigenen Firma zum Nachvollziehen des Stoffes verwenden. Er muss nach jeder Unterrichtseinheit seine Redo-Logs auf einem USB-Stick mitnehmen und hat zusammen mit der Basis-VM auf DVD immer den aktuellen Stand.

**Kopieren der Redo-Logs mitnehmen**

Es genügen nicht nur die Redo-Logs, sondern der Teilnehmer muss auch die Konfigurationsdatei (\*.vmx) mitsichern, weil sie die richtige Versionsnummer der Redo-Logs enthält. Nach jedem Löschen der Redo-Logs generiert VMware immer wieder eine andere neue Nummer. Wenn nicht die originale Konfigurationsdatei wiederhergestellt wird, werden die alten gesicherten Logs dann einfach ignoriert.

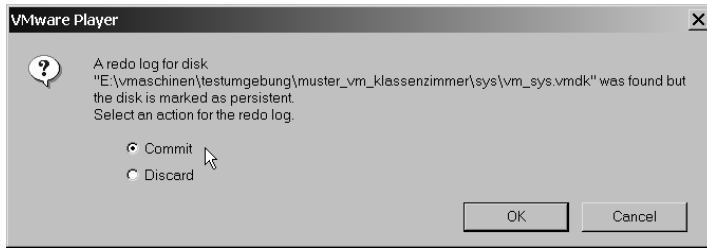


## 6.5.3 Wichtiger Hinweis zum Redo-Log der Vorlage-VM

Die als Vorlage verwendete VM verhält sich wie eine kompatible Maschine aus den älteren VMware-Produkten Workstation 4 oder GSX Server 3. In den neueren Versionen entstehen normalerweise keine Redo-Logs in der ursprünglichen Form mehr. Diese Funktion wird in den multiplen Snapshots ersetzt, die sich aber manuell schwieriger verwalten lassen.

Die Redo-Logs der Vorlage-VM entstehen beim Starten der VM automatisch, sobald Sie einer Platte den Status *undoable* gegeben haben. Löschen Sie die Logs, dann entstehen sie beim nächsten Start automatisch leer wieder neu. Das ist einfach und praktisch im Player, der keine eigene Snapshot-Verwaltung mitbringt.

Abbildung 6.7:  
Der VMware Player  
kann auch fragen,  
was mit den Ände-  
rungen in den Redo-  
Logs geschehen soll



Wollen Sie ein Redo-Log nachträglich nicht verwerfen, sondern die Änderungen direkt auf die Basisplatte übertragen, um diese Änderungen für immer zu erhalten, dann ändern Sie den Modus der Platte in der *vmx*-Datei von *undoable* wieder auf *persistent*:

```
ide0:0.mode = "persistent"
```

**Änderungen  
unwiderruflich  
übernehmen**

VMware fragt jetzt beim Starten der VM, was mit den Redo-Logs geschehen soll (Abbildung 6.7). Antworten Sie mit *Commit*, werden die Änderungen aus den Logs unwiderruflich auf die zugrunde liegende virtuelle Platte übertragen. Danach schreibt VMware nur noch auf die virtuelle Platte, bis Sie wieder den Status auf *undoable* setzen. Damit können Sie erfolgreiche Änderungen, z.B. eine Programminstallation, übernehmen, obwohl Sie die VM mit Redo-Logs betrieben haben. Bei einer zentralen Basisplatte funktioniert das allerdings nur für eine VM. Nach einer Änderung an der Basisplatte passen alle darauf aufsetzenden Redo-Logs nicht mehr dazu, sie sind inkonsistent und müssen verworfen werden..

#### 6.5.4 Basis-PC durch Vollbild vor dem Teilnehmer verbergen

Sie können im begrenzten Maße den realen PC vor den Teilnehmern verbergen, wenn Sie die VM im Vollbildmodus starten. Fügen Sie folgende Zeilen in Ihrer der *vmx*-Datei hinzu:

```
gui.powerOnAtStartup = "TRUE"
gui.fullScreenAtPowerOn = "TRUE"
gui.exitAtPowerOff = "TRUE"
```

Jetzt startet die VM sofort im Vollbild, und der Teilnehmer denkt, das Gastsystem läuft direkt auf dem PC. Nur mit dem Hotkey **[Strg] + [Alt]** oder durch Herunterfahren des Gastsystems gelangt er wieder zum realen PC. Wenn Sie z.B. den Aufruf der *vmx*-Datei in die Autostartgruppe einbinden, kann eine bestimmte VM automatisch die Kontrolle übernehmen.

### 6.5.5 Zusammenarbeit mit der Workstation oder dem Server als Master-PC

Wenn Sie die kostenpflichtige Workstation oder den Server auf dem Master-PC verwenden, können Sie Ihre Muster-VMs komplett selbst erstellen und müssen nicht die Vorlage von der CD verwenden. Allerdings funktioniert dann die Verwaltung der Redo-Logs (Änderungen der Teilnehmer) etwas anders als beschrieben (für eine ausführlichere Beschreibung des Zusammenspiels mit der VMware Workstation siehe Teil 2, Kapitel 5, „*Virtuelle Umgebungen mit dem VMware Player weitergeben*“).

Sie können zum Abschluss Ihrer Vorbereitungen (Installation des Betriebssystems usw.) unter VMware Workstation vor dem Verteilen der VM einen Snapshot setzen und im Menü VM/SETTINGS/OPTIONS/SNAPSHOTS unter der Option WHEN POWERING OFF den Punkt *Ask me* wählen. Damit lassen Sie die Teilnehmer selbst entscheiden, was mit den Änderungen geschieht. Bei Abschalten der VM im Player erscheint eine entsprechende Abfrage.

#### Snapshots der VMware Workstation

Im Player wird immer nur der Snapshot verwendet, der zuletzt in der Workstation aktiv war. Sie können dadurch mit verschiedenen Snapshots in der Workstation vor dem Verteilen entscheiden, welchen Stand Ihrer VM die Teilnehmer erhalten, z.B. mit Service Pack 1 oder 2 bzw. mit verschiedenen installierten Applikationen. Mehr zur Snapshot-Verwaltung der Workstation 5.5 erfahren Sie in Teil 3, Kapitel 4, „*Die Snapshot- und Clone-Funktion der VMware-Produkte*“.





# 7 Eine virtuelle Pilotumgebung als Testfeld für produktive Einsätze

Schritt für Schritt bauen Sie unter Microsoft Virtual Server 2005 R2 eine Testumgebung aus virtuellen Servern und Clients auf. Damit können Sie beispielsweise Ihre komplette Produktionsumgebung oder Teile davon abbilden. In dieser virtuellen Pilotumgebung stehen vernetzte Server inklusive Directories (ADS oder NDS) sowie Kopien echter Benutzerkonten und Datenbestände für umfangreiche Testszenarien bereit. Testen können Sie mit originalgetreuen virtuellen Client-PCs. Beim Aufbau dieser Umgebung lernen Sie das Produkt Microsoft Virtual Server 2005 R2 kennen.

## Workshop im Überblick

### Hauptprodukt

- ▶ Microsoft Virtual Server 2005 R2

### Praktische Verwendung

- ▶ Patches und Service-Packs vor dem produktiven Einsatz ohne Risiko an sauberen Betriebssysteminstallationen testen.
- ▶ 1:1-Kopie der heißen Produktionsserver als Pilotumgebung vorhalten.
- ▶ Einzelne Systemeinstellungen oder umfangreiche Migrationen an Kopien echter Daten testen.
- ▶ Eine Virtualisierung vorbereiten und Probleme frühzeitig erkennen.

### Schwerpunkte

- ▶ Umgang mit virtuellen Maschinen in einer Pilotumgebung
- ▶ Vorbereitung für den Produktivbetrieb

### Zielgruppe

- ▶ Administratoren, Techniker, Consultants.

## 7.1 Einstieg mit einer Pilotumgebung

Immer mehr IT-Abteilungen machen sich darüber Gedanken, ob sich eine Virtualisierung bestimmter Server oder sogar der gesamten Infrastruktur lohnen könnten. Das Thema ist in aller Munde, und eine Konsolidierung des Inhaltes der überquellenden 19“-Schränke auf wenige leistungsfähige Hosts klingt durchaus verführerisch. Aber was kann Virtualisierung wirklich leisten, bringt es am Ende die versprochenen Vorteile oder nur neue Fehlerquellen?

Wenn Sie Bedenken haben, sofort Ihre wichtigen produktiven Server einer unbekannten Technologie anzuvertrauen, indem Sie die Systeme in virtuelle Maschinen packen, dann bietet sich der Einstieg über eine Pilotumgebung an. Mit einer virtuellen Kopie der Produktionsserver können Sie als Admin oder Consultant gefahrlos neue Patches bzw. komplette Migrationen an echten Daten und Benutzerkonten testen, ohne Angst um die produktive Umgebung zu haben. Dabei erlernen Sie gefahrlos den Umgang mit virtuellen Maschinen, bevor Sie ihnen heiße Dienste anvertrauen.

### 7.1.1 Vorstellung der Vorgehensweise an einem exemplarischen Beispiel

Exemplarisch soll in folgendem Beispiel die überfällige Migration einer Active Directory-Domäne mit Windows 2000 Servern auf Windows 2003 Servern in einer virtuellen Testumgebung vorbereitet werden. Genauso lässt sich der Umstieg auf Linux-Server oder von Netware auf Windows und umgekehrt in der Pilotumgebung ausgiebig testen. Auch der Umstieg von einer alten NT4-Domäne oder der Wechsel einer Exchange-Version kann damit endlich in Angriff genommen werden. Die eigentliche Migration der Betriebssysteme möchte ich hier allerdings nicht thematisieren. Mir geht es vielmehr darum, Ihnen an einem praktischen Beispiel das Grundkonzept und den Nutzen der Verwendung virtueller Maschinen zu zeigen. Der Workshop liefert Ihnen die virtuelle Infrastruktur, die Sie dann als Pilotumgebung für beliebige Projekte nutzen können.

#### **Beispiel einer Migration**

Zum Auftakt erfolgt die Installation eines sauberen Windows 2000-Domänencontrollers als erste virtuelle Testmaschine, an der sich die Migration mit beliebigen Wiederanläufen in Ruhe durchspielen lässt. Damit können Sie sich beispielsweise auf die lehrbuchmäßige Durchführung eines Upgrades vorbereiten und verschiedene Tools und Konzepte testen. Ich zeige Ihnen hier, wie Sie Ihre erste virtuelle Maschine erstellen und effektiv benutzen.

Nach und nach gesellen sich dann zur ersten Maschine weitere VMs, z.B. ein virtueller Testclient oder ein weiterer Server als zusätzlicher Domänencontroller. Sie lernen Grundlagen virtueller Netzwerke kennen und werden VMs klonen. Am Ende übernehmen Sie Kopien von Ihren echten Produktionsservern in virtuelle Maschinen, um an dieser originalgetreuen Umgebung die heiße Migration ausgiebig zu testen. Das Beispiel dient als Gerüst, um Ihnen den Umgang mit virtuellen Maschinen praxisnah zu vermitteln.

## 7.2 Vorbereitung der Verwendung von Microsoft Virtual Server 2005 R2

Die Installation von Microsoft Virtual Server 2005 R2 und die Voraussetzungen an den Host habe ich detailliert in *Teil 1, Kapitel 3, „Installation und Konfiguration der einzelnen Produkte“*, beschrieben. Ich gehe im Workshop davon aus, dass Sie bereits über einen funktionsfähigen Host mit genügend RAM und Plattenplatz verfügen. Sie sollten auf dem Host oder auf Ihrem Arbeitsplatz-PC im LAN mit der URL [http://mein\\_host:1024](http://mein_host:1024) die *Virtual Server-Verwaltungswebseite* im Internet Explorer erreichen (Abbildung 7.1). Wenn das nicht gelingt, dann überprüfen Sie bitte, ob der Port 1024 der Windows-Firewall auf dem Host geöffnet ist.

**Verwaltungswebseite testen**

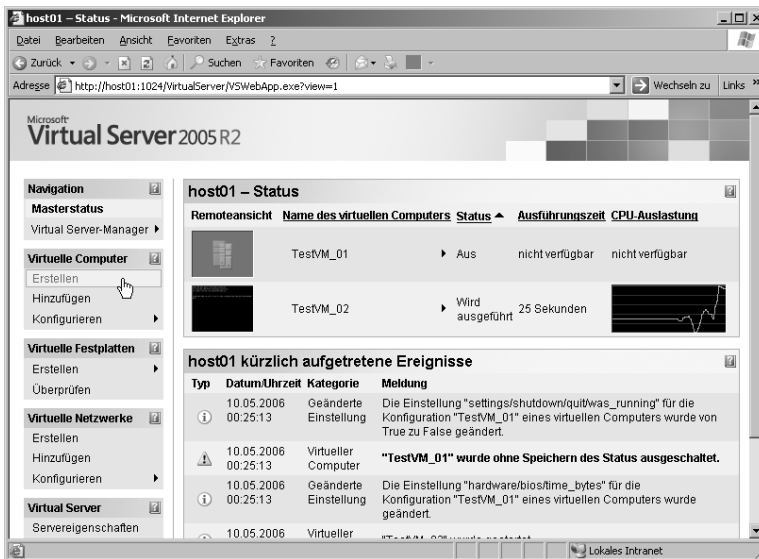


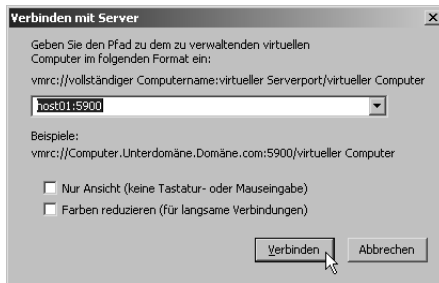
Abbildung 7.1:  
Die Virtual Server-Verwaltungswebseite sollte bereits funktionieren. Sie ist die Zentrale zur Bedienung des Hosts und aller Gäste



## Remotesteuerung mit vmrc.exe

Zusätzlich sollten Sie mit dem *Virtual Machine-Remotesteuerungsclient* (VMRC) eine Verbindung zum Host mit dem Link *mein\_host:5900* herstellen können (Abbildung 7.2). Den Client finden Sie als Datei *vmrc.exe* im Verzeichnis *C:\Programme\Microsoft Virtual Server\VMRC Client* auf dem Host-Rechner. Sie können die Datei an einer zentrale Stelle im LAN hinterlegen. Sollte eine Verbindung nicht gelingen, dann ist der Port 5900 am Host freizuschalten, gegebenenfalls ein laufender VNC-Dienst zu beenden und in der Verwaltungswebseite die *Virtual Machine-Remotesteuerung* zu aktivieren (siehe *Teil 1, Kapitel 3*). Sie benötigen den Remotesteuerungsclient nicht unbedingt, eine Fernsteuerung der Gäste ist auch im Browser möglich. Der separate Client macht aber die Bedienung von vielen parallel laufenden Gästen etwas komfortabler (siehe *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*).

Abbildung 7.2:  
Die Virtual  
Machine-Remote-  
steuerung bietet  
etwas mehr Komfort  
bei der Bedienung  
der Gastssysteme



## Übersichtliche Ordnerstruktur

Weiterhin sollten Sie auf Ihrem Host einen Ordner *\vmaschinen* mit den Unterordnern *testumgebung*, *mustervorlagen* und *produktion* angelegt haben, um die virtuelle Umgebung von Beginn an übersichtlich zu gestalten. Diese Ablageordner für Ihre zukünftigen VMs sollten aus Performancegründen möglichst auf einer separaten Festplatte liegen. Den Ordner *\vmaschinen\testumgebung* können Sie gleich noch in der Verwaltungswebseite unter *VIRTUAL SERVER/SERVEREIGENSCHAFTEN/SUCHPFADE* als den *Standardordner für Konfiguration virtueller Computer* hinterlegen, dort landen dann alle neu erstellten VMs, ohne dass Sie immer den vollständigen Pfad eintippen müssen (siehe *Teil 1, Kapitel 4*).

## 7.3 Die erste VM mit Virtual Server erstellen und installieren

Sobald Sie die Verwaltungswebseite in Ihrem Browser geladen haben, können Sie sofort die erste virtuelle Maschine der Pilotumgebung erstellen. In diesem Gast installieren Sie einen neuen Windows 2000-Domänencontroller als Testmaschine, um das Upgrade auf Windows Server 2003 an einer sauberen Umgebung erstmals durchzuspielen.

### 7.3.1 Erstellen der ersten virtuellen Maschine

Über VIRTUELLE COMPUTER/ERSTELLEN gelangen Sie zum Dialog, wo Sie eine neue VM erzeugen können (Abbildung 7.3).

**Virtuellen Computer erstellen**

**Name des virtuellen Computers**  
Geben Sie den Dateinamen für den virtuellen Computer ein, um den virtuellen Computer im Standardkonfigurationsordner zu speichern, der auf der Seite *Virtual Server-Suchpfade* angegeben ist. Geben Sie einen vollqualifizierten Pfad ein, um einen virtuellen Computer an einem anderen Speicherort zu erstellen.

Name des virtuellen Computers:

**Arbeitsspeicher**  
Die Größe des Arbeitsspeichers darf zwischen 4 MB und 818 MB liegen (736 MB werden als Maximalwert empfohlen).

Arbeitsspeicher des virtuellen Computers (in MB):

**Virtuelle Festplatte**  
Bevor Sie ein Betriebssystem auf diesem virtuellen Computer installieren können, müssen Sie ihm eine neue oder vorhandene virtuelle Festplatte zuordnen. Eine virtuelle Festplatte ist eine VHD-Datei, die auf der physikalischen Festplatte gespeichert ist und das Gastbetriebssystem, Anwendungen und Datendateien enthält.

☒ Neue virtuelle Festplatte erstellen  
Mit dieser Option wird eine unformatierte dynamisch erweiterbare virtuelle Festplatte im Verzeichnis der Konfigurationsdatei des virtuellen Computers erstellt. Die maximal zulässige Größe ist 127 GB für IDE-Festplatten und 2040 GB für SCSI-Festplatten.

Größe:  Einheiten:  Bus:

☐ Eine vorhandene virtuelle Festplatte verwenden

Pfad:

Dateiname (vhd):

Bus:

☒ Virtuelle Festplatte später zuordnen (Keine)

**Virtueller Netzwerkadapter**  
Ein virtueller Computer wird mit einem Ethernet-Netzwerkadapter vorkonfiguriert, der mit einem virtuellen Netzwerk verbunden werden kann.

Verbunden mit:

**Virtual Machine Additions**  
Wichtig: Die Installation von Virtual Machine Additions wird dringend empfohlen. Virtual Machine Additions stellt Leistungs- und Funktionserweiterungen für Windows-basierte Gastbetriebssysteme bereit. Diese Features umfassen: Zeitsynchronisation zwischen Gast- und Hostbetriebssystem, Mausintegration bei der Verwendung des ActiveX-Steuerelements in VMRC (Virtual Machine Remote Control) und ein Signal für das Gastbetriebssystem zum Überwachen des Status des virtuellen Computers.

Abbildung 7.3:  
Das Erstellen einer VM ist unkompliziert. Die virtuelle Platte lassen wir vorerst weg

Vergeben Sie der VM einen sinnvollen Namen, in unserem Beispiel nennen wir sie *TestVM\_01*. Die Arbeit mit diesem unspezifischen Namen macht den Workshop allgemein gültiger, sie könnte auch passend zu Ihrer konkreten Umgebung den Namen *W2K\_SP4* o.Ä. erhalten. Vielleicht wollen Sie ja auch von SUSE8 auf SUSE10 migrieren.

**Sinnvolle Namen für die VMs**

Sie sollten nicht unnötig viel RAM zuweisen, da sich alle Maschinen den vorhandenen Speicher mit dem Host-System teilen müssen. Eine virtuelle Platte erstellen Sie vorerst nicht, wählen Sie deshalb VIRTUELLE FESTPLATTE SPÄTER ZUORDNEN (KEINE). Zum einen erkläre ich Ihnen das Erstellen der Platte gleich im Anschluss etwas detaillierter, zum anderen sollten Sie nicht den automatisch vergebenen Namen verwenden.

Mit einem Klick auf ERSTELLEN befindet sich wenig später auf der Platte des Hosts ein Verzeichnis `\vmaschinen\testumgebung\TestVM_01` mit den Dateien der virtuellen Maschine. Vorerst finden Sie dort nur eine Datei `TestVM_01.vmc`, welche die Konfiguration der virtuellen Maschine enthält.

Abbildung 7.4:  
Die Konfigurations-  
seite einer VM zeigt  
im oberen Teil auch  
den aktuellen  
Status an



In der Verwaltungswebseite öffnen sich automatisch der Status und die Konfiguration zur eben erstellten VM. Über den kleinen schwarzen Pfeil am Namen der VM öffnet sich ein Menü, über das Sie die Maschine sofort starten könnten (Abbildung 7.4). Da die VM noch keine Platte hat, lassen Sie den Gast vorläufig aus. Sie können im unteren Teil der Konfigurationsseite Änderungen an der Hardware-Ausstattung des Gastes vornehmen. Zuerst erstellen Sie aber die fehlende virtuelle Platte.

### Die virtuellen Platten eines Gastes erstellen und zuweisen

Virtuelle Platten sind Dateien auf einem Host-Datenträger. In diese Dateien werden alle Schreib- und Lesezugriffe des Gastes umgeleitet, wobei das Betriebssystem in der VM „denkt“, mit echter Hardware zu arbeiten. Viele erweiterte Informationen zu den virtuellen Festplatten finden Sie in Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“.



Abbildung 7.5:  
Es stehen verschiedene Typen virtueller Platten zur Verfügung

Im Menüpunkt VIRTUELLE FESTPLATTEN/ERSTELLEN haben Sie die Wahl zwischen verschiedenen Plattentypen (Abbildung 7.5):

#### Typen virtueller Festplatten

- ▶ *Dynamisch erweiterbare virtuelle Festplatte* – Dieser Typ ist für unseren entstehenden Testserver ideal. Die Platte belegt auf dem Host nur so viel Platz, wie wirklich vom Gast verwendet wird, und wächst bei Bedarf mit.
- ▶ *Virtuelle Festplatte mit fester Größe* – Der gesamte Platz der virtuellen Platte wird bereits reserviert. Das kommt etwas der Performance zugute und verhindert das Defragmentieren der Datei auf der physischen Host-Platte. Solche virtuellen Platten belegen aber oftmals viel unnötigen Platz. In einer Testumgebung ist dieser Typ nicht zu empfehlen.
- ▶ *Differenzierende virtuelle Festplatte* – Auf diesen sehr interessanten Plattentyp werde ich weiter unten beim Thema Klonen noch eingehen. Damit können z.B. mehrere VMs die gleiche virtuelle Platte als Basisinstallation verwenden. Weiterhin können Sie mehrere aufeinander aufsetzende Versionsstände erstellen, um verschiedene Wiederanlaufpunkte bei Ihren Tests zu setzen, z.B. eine Version ohne einen bestimmten Service-Pack und eine Version mit diesen Patches.
- ▶ *Verknüpfte virtuelle Festplatte* – Eine solche virtuelle Platte ist mit einer physikalischen Platte des Hosts verknüpft. Sie können damit unter Virtual Server nicht direkt auf Partitionen physischer Festplatten zugreifen, sondern nur physische Partition in virtuelle Platten konvertieren. Das gelingt über VIRTUELLE FESTPLATTEN/ÜBERPRÜFEN/VIRTUELLE FESTPLATTE KONVERTIEREN.
- ▶ *Virtuelle Diskette* – Sie können eine virtuelle Diskette erstellen. Das ist manchmal ganz praktisch, wenn man ein älteres selbstentpackendes Treiberpaket unbedingt zum Auspacken eine Diskette benötigt. Haben Sie keine Diskette zur Hand, können Sie das Paket in einer VM auspacken und dort eine virtuelle Diskette verwenden.

Abbildung 7.6:  
Bei der Erstellung  
einer virtuellen  
Platte ist neben dem  
richtigen Typ auch  
ein aussagekräftiger  
Name wichtig

**Dynamisch erweiterbare virtuelle Festplatte**

Geben Sie den Speicherort an, an dem Sie eine dynamisch erweiterbare virtuelle Festplatte erstellen möchten. Sie können einen Speicherort aus einer Liste mit bekannten Speicherorten auswählen oder den vollqualifizierten Pfad eingeben. Die Liste der bekannten Speicherorte schließt alle unter den Suchpfaden oder im Konfigurationsordner gespeicherten Speicherorte ein. Beide Einstellungen werden auf der Seite [Suchpfade](#) angegeben.

Pfad:

Name der virtuellen Festplattendatei:

Größe:  Einheiten:

### Platten in System und Daten trennen

Wählen Sie eine DYNAMISCH ERWEITERBARE VIRTUELLE FESTPLATTE. Im folgenden Dialog habe Sie die Gelegenheit, einen sinnvollen Namen für den virtuellen Datenträger einzugeben (Abbildung 7.6). Ein aussagekräftiger Plattenname wie *TestVM\_01\_sys* macht die Zuordnung zur VM einfacher. Die Erweiterung *\_sys* sagt aus, dass es sich um die Systemplatte handelt. Die Möglichkeit, einen eigenen Namen zu vergeben und gegebenenfalls einen anderen Plattentyp auszuwählen, ist der Grund, warum wir die Platte nicht gleich beim Anlegen der VM automatisch erstellt haben.



Bei produktiven Maschinen sollten Sie die Platten eines Gastes immer in *System* und *Daten* trennen und entsprechend benennen. Eventuell ist sogar eine separate Platte für die Auslagerungsdatei (*Swap*) sinnvoll. Die Trennung hat später den Vorteil, dass Sie die virtuellen Platten für bessere Performance auf separaten physischen Datenträgern unterbringen können. Noch wichtiger ist die Aufteilung für ein vernünftiges Sicherungskonzept. Die meist recht kleine Platte mit dem System kann später einfach, je nach Bedarf wöchentlich oder in kürzeren Intervallen, wegekopiert werden und bietet damit für Disaster-Recovery eine 1:1-Kopie des enthaltenen Systems, ähnlich einem Image. Die umfangreichen Daten auf den Datenplatten können dagegen mit den üblichen Sicherungsagenten direkt über das Gastsystem weiterhin täglich gesichert werden (zur Datensicherung siehe auch Teil 3, Kapitel 5, „Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs“). Auch beim späteren Klonen der VM als Vorlage für weitere Maschinen muss nicht ständig der gesamte Datenballast mitkopiert werden, wenn System und Daten getrennt abgelegt sind.

### Ablageort der virtuellen Platte

Um die Platte zu erstellen, müssen Sie im Feld **PFAD** noch den Ort für die Datei der virtuellen Platte auswählen. Erstellen Sie die Platte im gleichen Verzeichnis wie Ihre VM. Da diese VM Virtual Server bereits bekannt ist, steht der vollständige Pfad in einer Liste zur Auswahl, die Sie neben dem Eingabefeld aufklappen können. Wenn Sie die virtuelle Platte in einem anderen Verzeichnis erstellen wollen, dann müssen Sie den vollständigen Pfad eintippen. Die virtuelle Platte ist nach dem Erstellen im Verzeichnis `\vmaschinen\testumgebung\TestVM_01` unter dem Namen `TestVM_01_sys.vhd` zu finden. Da es eine Zuwachsplatte ist, ist sie noch recht klein. Das wird sich ändern, sobald Sie das Betriebssystem installiert haben.

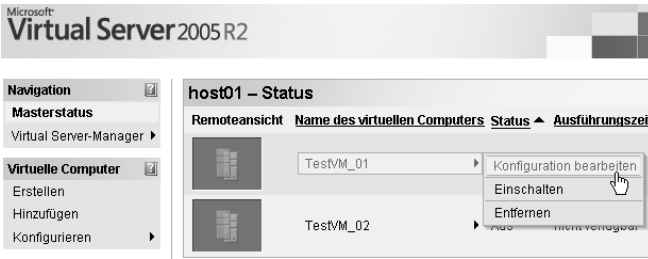


Abbildung 7.7:  
Zur Konfiguration  
eines Gastes gelangen  
Sie z.B. über  
das kleine Menü  
am Eintrag der VM  
im Masterstatus

In der Konfiguration der virtuellen Maschine, die wieder über das kleine Menü am Namen der VM erreichbar ist (Abbildung 7.7), können Sie nun über den Punkt **FESTPLATTEN** die eben erstellte Platte hinzufügen (Abbildung 7.8). Auf diese Weise können Sie später in Produktionsmaschinen mehrere virtuelle Platten erstellen und einbinden. Bestätigen Sie zum Übernehmen der neuen virtuellen Platte an dieser Stelle mit **OK**, auch wenn der große Button **DATENTRÄGER HINZUFÜGEN** mehr Aufmerksamkeit erregt – damit würden Sie allerdings nur eine weitere Platte hinzufügen.

**Virtuelle Platte  
dem Gast hinzu-  
fügen**

Für den Anfang können Sie generell mit virtuellen IDE-Platten arbeiten, vor allem wenn andere Gastbetriebssysteme als Windows zum Einsatz kommen, die manchmal Probleme mit der Erkennung des virtuellen SCSI-Controllers haben können. Im produktiven Einsatz sollten Sie für eine bessere Performance dagegen virtuelle SCSI-Platten verwenden. Dazu müssen Sie in der Konfiguration der VM unter **SCSI-ADAPTER** einen virtuellen SCSI-Controller hinzufügen und anschließend die virtuelle Platte einfach anstelle des *Primären Kanals 0* (Abbildung 7.8) an einen verfügbaren SCSI-Kanal binden. Dafür muss das Betriebssystem aber die passenden Treiber für den emulierten SCSI-Controller besitzen, Microsoft liefert zur Beschleunigung auch eigene optimierte Treiber für die Gäste (siehe *Teil 3, Kapitel 3*).

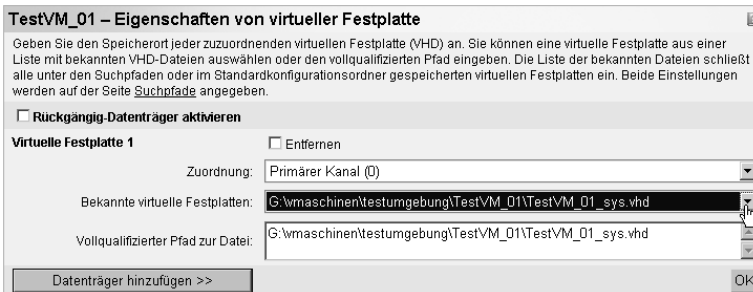


Abbildung 7.8:  
Die erstellte virtuelle  
Platte muss dem  
Gast in der Konfiguration  
noch zugewiesen werden

### 7.3.2 Installation des Betriebssystems in der virtuellen Maschine

Jetzt ist Ihre erste VM bereits startklar, ohne den kleinen Plattenexkurs wäre das Erstellen Sekundensache gewesen. Bevor Sie den Gast das erste Mal einschalten, müssen Sie sich entscheiden, von welchem Datenträger die Installation des Betriebssystems erfolgen soll.

#### Ein ISO-Image oder eine CD in der VM verwenden

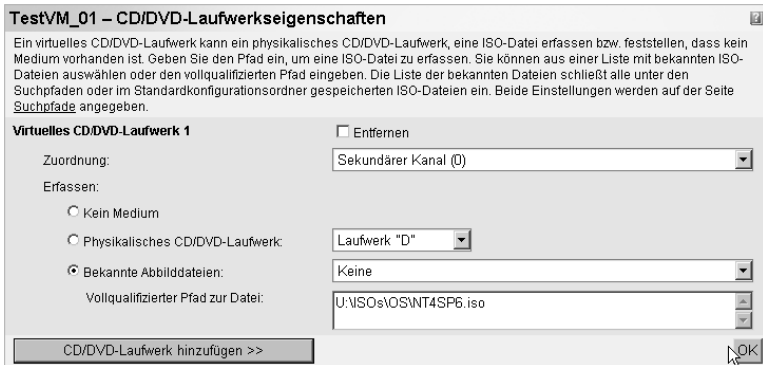
**Häufig verwendete CDs als ISO-Sammlung**

Sie können entweder ein CD ins physische Laufwerk des Hosts einlegen. Diese CD wird standardmäßig von der VM verwendet, Sie müssen nichts ändern. Oder Sie können auch ein ISO-Image als virtuelle CD in den Gast einbinden. Das ist sehr praktisch, wenn Sie sich von häufig verwendeten CDs bereits ein Image-Archiv erstellt haben. So entfällt der Weg zum Host, um CDs zu wechseln. Sie können dazu in der Konfiguration Ihrer neuen VM unter CD/DVD den Pfad zum ISO-Image angeben. Entweder müssen Sie ihn komplett eintippen, oder Sie hinterlegen den Pfad zu den ISO-Images in den *Virtual Server-Suchpfaden* (Abschnitt 7.2, „Vorbereitung der Verwendung von Microsoft Virtual Server 2005 R2“).



Eine Alternative zum Eintippen des langen Pfades ist es, im Windows-Explorer auf dem Host zum ISO-Image zu navigieren und den vollständigen Pfad aus der Adresszeile des Windows-Explorers zu kopieren.

Abbildung 7.9:  
Sehr praktisch ist die  
Verwendung eines  
ISO-Images als virtuelle  
CD im Gast



**Startreihenfolge im CMOS anpassen**

Sobald die Installations-CD Ihres Betriebssystems physisch oder als ISO-Image eingelegt ist, können Sie die VM über das kleine Menü am Namen der VM einschalten (Abbildung 7.7). Der Gast bootet von der CD und beginnt mit dem Setup. Wenn die VM nicht von der CD starten sollte, z.B. weil die virtuelle Platte nicht mehr leer ist, dann können Sie im Startbildschirm des Gastes gleich zu Beginn mittels **[Entf]** das virtuelle CMOS-Setup aufrufen, um die Reihenfolge der Startgeräte zu ändern (Abbildung 7.10).

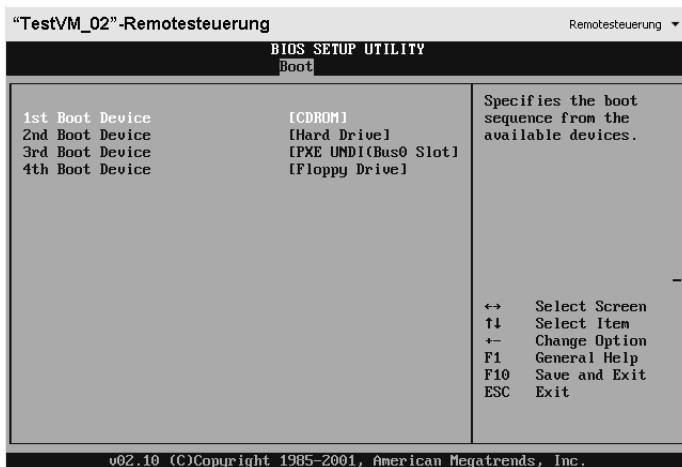


Abbildung 7.10:  
Eine VM verfügt  
sogar über ein virtu-  
elles CMOS-Setup,  
in dem sich z.B. die  
Bootreihenfolge  
anpassen lässt

## Tastatur, Maus und Bildschirm des Gastes bedienen

In unserem Beispiel der Testmigration würde jetzt der Windows 2000 Server in der VM installiert, aber ich sagte ja bereits, dass in der Pilotumgebung verschiedene Migrationsszenarien vorstellbar sind. Also habe ich in Abbildung 7.11 einmal ein alternatives Beispiel dargestellt. Den Bildschirm des Gastsystems sehen Sie, indem Sie einfach auf die Miniaturansicht der VM im Masterstatus klicken oder im Menü der VM den Punkt REMOTESTEUERUNG wählen. Dieser Menüpunkt existiert nur, wenn die VM läuft. Sie starten damit die Remotesteuerung, die als ActiveX-Plug-In im Browser läuft (Abbildung 7.11). Sie verlassen die Remotesteuerung wieder über den Menüpunkt MASTERSTATUS.

Um im Gastsystem die Tastatur oder die Maus zu benutzen, können Sie einfach ins Fenster der Maschine klicken oder die Tastatur verwenden, der Gast hat damit den Fokus. Mit der so genannten *Host-Taste* erhält Ihr lokaler Desktop den Fokus wieder zurück. Die *Host-Taste* ist standardmäßig **AltGr** und kann über das Menü REMOTESTEUERUNG/HOSTTASTE FESTLEGEN geändert werden. Zusätzlich muss als Ersatz für **Strg** + **Alt** + **Entf**, z.B. beim Anmeldebildschirm eines Gastes, eine Kombination aus Host-Taste + **Entf** verwendet werden.

## Tastatur und Maus im Gast

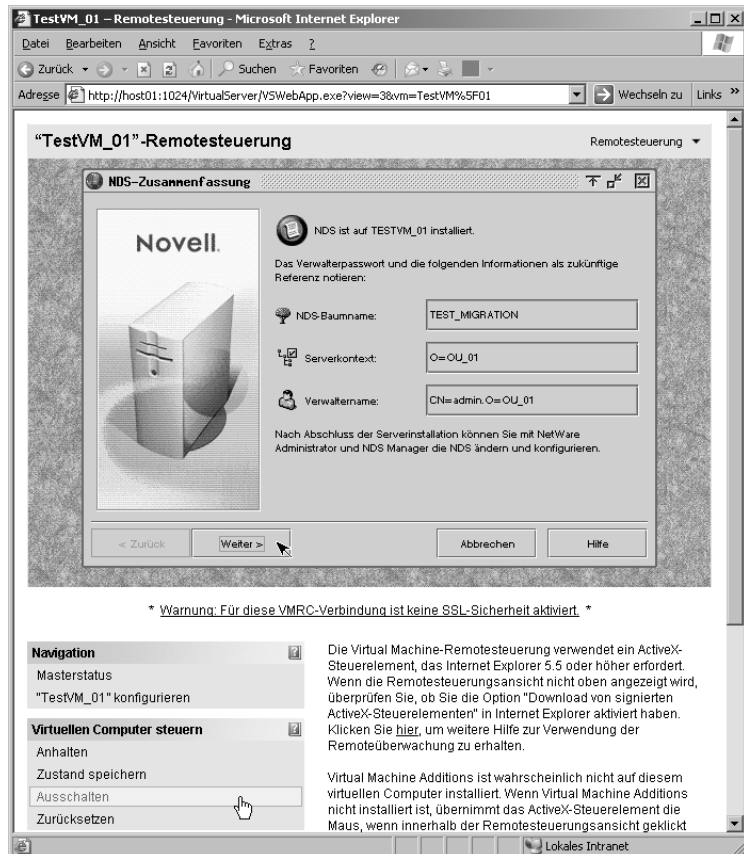
In der Remotesteuerung können Sie Ihre VM auch AUSSCHALTEN (PowerOff) oder ZURÜCKSETZEN (Reset). Die Funktion ANHALTEN entzieht der VM alle Ressourcen und friert sie damit ein, nach dem Fortsetzen macht der Gast sofort an der gleichen Stelle weiter. Mit ZUSTAND SPEICHERN wird der RAM-Inhalt der VM in einer Datei gesichert und die VM abgeschaltet. Später kann dieser gesicherte Status jederzeit wiederhergestellt werden, und das Gastsystem steht in Sekunden wieder an der Stelle, an welcher der Zustand gespeichert wurde. Im Gegensatz zum ANHALTEN funktioniert das auch, wenn der Host zwischenzeitlich aus war. Das entspricht dem Suspend-

## PowerOn, PowerOff, Suspend



Modus eines Laptops und kann viel Zeit sparen, um z.B. eine komplette Testumgebung neu zu starten.

Abbildung 7.11:  
In der Remotesteuerung können Sie im Gast arbeiten und die VM ein- oder ausschalten, ganz gleich welches Gastsystem läuft



### Jeder Gast im eigenen Fenster

Als Alternative können Sie für jeden Gast ein eigenes Fenster mit der Remotesteuerung öffnen, das jederzeit in der Taskleiste Ihres Desktops zur Verfügung steht. Dazu gehen Sie einfach mit der rechten Maustaste auf die Miniatur einer VM (z.B. im Masterstatus) und wählen im Kontextmenü des Browsers **IN NEUEM FENSTER ÖFFNEN**. Weiterhin können Sie auch die *vmrc.exe* zur Fernsteuerung verwenden. Weitere Hinweise zur Bedienung finden Sie in *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*.

### Die Virtual Machine Additions in den Gästen installieren

Das Gastsystem führt in der VM sein gewohntes Setup von der eingelegten CD aus durch, installiert alle Dateien auf der virtuellen Platte und erkennt mittels Plug&Play die virtuelle Hardware, die der Virtualisierungslayer im Gast bereitstellt. Der Vorgang unterscheidet sich nicht von einem realen Rechner, der Gast merkt nichts davon, dass er nur in einer virtuellen Welt sein Dasein fristet.

Nach erfolgter Betriebssysteminstallation sollten Sie die so genannten *Virtual Machine Additions* in der neuen Maschine einrichten, wenn als Gastsystem Windows läuft. Dieses Software-Paket bringt unter anderem eigene Treiber für Maus und VGA mit. Dadurch wird dann ein nahtloser Fokuswechsel vom Host in die VM und umgekehrt möglich, auch ohne die Maus erst mit dem Host-Key lösen zu müssen. Die Installation der Additions startet im Gast automatisch, sobald Sie in der Konfiguration zur VM unter VIRTUAL MACHINE ADDITIONS den Haken bei VIRTUAL MACHINE ADDITIONS INSTALLIEREN setzen. Weitere Informationen zu den Additions finden Sie in *Teil 1, Kapitel 4*.

## 7.4 Virtuelle Netzwerke unter Microsoft Virtual Server 2005 R2

In unserem zukünftigen Test-Domänencontroller fehlen nach dem Abschluss der Grundinstallation noch alle notwendigen Service-Packs, Patches und eventuell benötigte Programme. Wie können Sie diese Dateien mit der VM austauschen, oder wie kommt die VM ins Internet, um sich dort selbst Patches abzuholen?

**Vier virtuelle Netzwerkkarten**

### 7.4.1 Anschlusstypen virtueller Netzwerkadapter

In jede Maschine können dafür bis zu vier virtuelle Netzkarten eingebaut werden. Sie erscheinen innerhalb der VM als Adapter vom Typ *DEC 21140* oder *Intel Ethernet Adapter*, für den jedes Betriebssystem Treiber mitbringt. Eine neue VM verfügt bereits über eine virtuelle Netzwerkkarte. In der Konfiguration der VM können Sie über NETZWERKADAPTER weitere Adapter hinzufügen oder vorhandene bearbeiten (Abbildung 7.12).

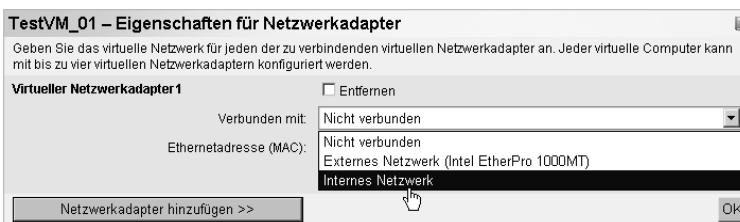


Abbildung 7.12:  
Eine virtuelle Netzwerkkarte kann mit verschiedenen Verbindungstypen konfiguriert werden

Es gibt verschiedene Möglichkeiten, einen virtuellen Adapter zu konfigurieren. Der eingestellte Verbindungstyp entscheidet darüber, wie die VM mit dem LAN kommunizieren kann (Abbildung 7.12):

- *Nicht verbunden* – Die Einstellung *Nicht verbunden* wirkt, als wäre das Kabel von der virtuellen Netzwerkkarte abgezogen worden. Es ist keinerlei Datenverkehr von der VM möglich, der Gast bleibt isoliert.

- ▶ *Externes Netzwerk* – Der Gast kommuniziert über eine physische Netzkarte im Host-PC mit dem externen Netzwerk. Die VM hat vollen Zugriff auf das LAN und ist uneingeschränkt zu erreichen. Der Gast benötigt eine freie IP-Adresse aus dem LAN und erscheint parallel zum Host unabhängig im Netz. Wenn Sie später mit virtuellen Kopien Ihrer Produktionsserver Tests durchführen, dürfen Sie diese auf keinen Fall an Ihr Produktivnetz anbinden!
- ▶ *Internes Netzwerk* – Alle VMs an einem internen Netz können nur intern miteinander kommunizieren, ohne jeden Kontakt zur Außenwelt. Damit können Sie ein virtuelles Testnetzwerk aufbauen, in dem virtuelle Server und Testclients arbeiten, ohne den Betrieb im Unternehmensnetzwerk zu stören – ideal für Ihre Pilotumgebung.

Der Anschlusstyp jeder Netzkarte kann im laufenden Betrieb umgeschaltet werden. Die VM meint dabei, das Patchkabel wurde umgesteckt. So können Sie eine Testmaschine ans LAN anbinden und bei Problemen sofort wieder isolieren. Sie können auch weitere interne Netzwerke anlegen, z.B. um Routing zwischen virtuellen Maschinen zu testen. Viele Hinweise zu virtuellen Netzwerken finden Sie im detaillierten Workshop von *Teil 3, Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“*.

## 7.5 Wiederanlaufpunkte durch Differenzplatten oder Rückgängig-Datenträger

Frisch vernetzt lassen sich im Gast nun Patches aus dem Internet installieren und Daten aus dem LAN holen. Ist die VM fertig konfiguriert und mit allen Patches und Hilfsprogrammen versehen, haben Sie damit eine gute Grundlage für die weitere Testarbeit geschaffen. Diese Grundlage sollten Sie sichern, damit fehlgeschlagene Versuche in Ihrer Pilotumgebung nicht immer wieder zu einer Neuinstallation der Gastsysteme führen müssen. Im Gegensatz zu physischen Maschinen können VMs hier einige Vorteile ausspielen.

### 7.5.1 Mit Differenzplatten den Zustand einer Installation sichern oder weitere Duplikate klonen

**Differenzplatten  
enthalten geänderte  
Sektoren**

Der beste Weg, um eine komplette Grundinstallation eines Gastsystems zu sichern und für die weitere Arbeit immer wieder zu verwenden, sind die so genannten *differenzierenden Platten*, kurz *Differenzplatten*. Eine Differenzplatte ist eine virtuelle Platte, die auf eine andere virtuelle Platte aufsetzt. In der Differenzplatte liegen, wie der Name

schon sagt, nur die Änderungen, die das Gastsystem an der virtuellen Platte vorgenommen hat. Dazu werden vom Virtualisierungslayer alle Schreibzugriffe des Gastes in die Differenzplatte umgeleitet. Lesezugriffe kombinieren dann den Inhalt der Differenzplatte und den Inhalt der zugrunde liegenden virtuellen Platte, ohne dass der Gast etwas davon bemerkt. Die zugrunde liegende Platte wird also nicht mehr verändert, und die Differenzplatte bleibt relativ klein, da sie nur Änderungen enthält (Abbildung 7.13).

Differenzierende Platten haben folgenden Nutzen:

- ▶ Sie können mit einer Differenzplatte einen bestimmten Konfigurationsstand des Gastsystems schützen. Sollte etwas in einem Gast schief gehen, dann lassen sich durch Löschen der Differenzplatte alle Änderungen verwerfen. Dadurch haben Sie wieder einen sauberen Zustand des Systems.
- ▶ Eine fertige Basisinstallation kann von mehreren VMs gleichzeitig verwendet werden, indem Sie einfach mehrere Differenzplatten erstellen, die auf ein und dieselbe virtuelle Platte zeigen. Dadurch sparen Sie sich viel Zeit und Platz beim Klonen von virtuellen Maschinen. Wenn Sie z.B. eine saubere Installation Ihres Windows 2000 Servers für mehrere Testserver benötigen, dann müssen Sie nicht jedes Mal die gesamte virtuelle Platte kopieren, es genügt das Anlegen einer Differenzplatte für jeden Klon (Abbildung 7.13).

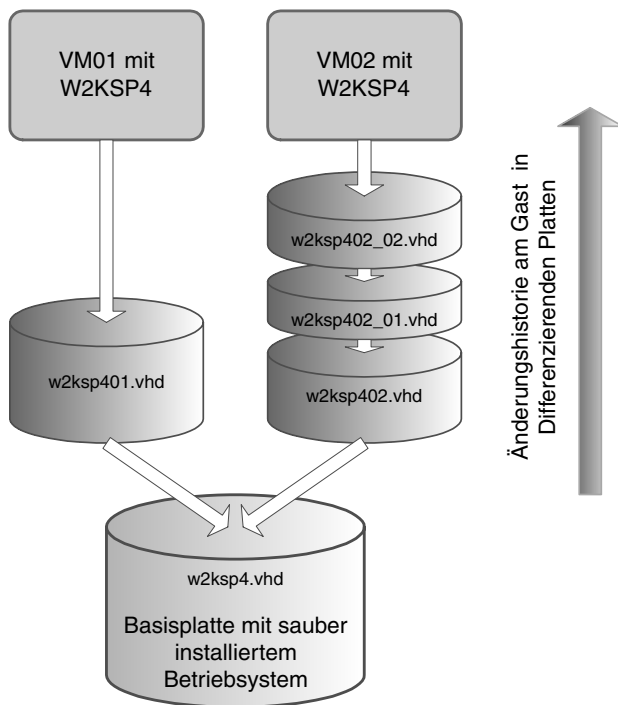


Abbildung 7.13:  
Mit differenzierenden  
Platten können  
Basisinstallationen  
mehrfach verwendet  
und Wiederanlauf-  
punkte gesetzt  
werden

## Erstellen und Zuweisen einer differenzierenden Festplatte

Sie können für Ihren gerade installierten virtuellen Windows 2000 Server eine Differenzplatte erstellen. Damit wird die saubere Grundinstallation von der Test-VM entkoppelt. Die Grundinstallation wird dadurch nicht mehr verändert und kann sogar für weitere VMs mit eigenen Differenzplatten als Basis dienen. Gehen Sie folgendermaßen vor:

1. Schalten Sie die VM ab.
2. Verschieben Sie die Datei der virtuellen Platte *TestVM\_01\_sys.vhd* aus dem Verzeichnis *\vmaschinen\testumgebung\TestVM\_01* in ein neues Verzeichnis, z.B. nach *\vmaschinen\vm\_muster\W2K\_SP4*. Benennen Sie diese Datei um in einen Namen, der auf den Inhalt schließen lässt, z.B. *w2ksp4.vhd*. Mit diesem Schritt beginnen Sie, sich an einer zentralen Stelle einen Satz von Musterinstallationen Ihrer benötigten Betriebssysteme aufzubauen. Windows 2000 Server SP4 ist das erste Muster in diesem Archiv.
3. Wählen Sie im Menü VIRTUELLE FESTPLATTEN/ERSTELLEN den Typ DIFFERENZIERENDE VIRTUELLE PLATTE.
4. Im Dialog zur Erstellung der Platte müssen Sie zuerst einen Namen und ein Ziel für die neu zu erstellende Differenzplatte eingeben (Abbildung 7.14). Sie sollten die neue Differenzplatte im Verzeichnis Ihrer TestVM\_01 erstellen. Der Pfad zu dieser VM ist Virtual Server bekannt, Sie können die Liste neben dem Eingabefeld PFAD aufklappen. Nachdem Sie den Pfad ausgewählt haben, müssen Sie im Feld NAME DER VIRTUELLEN FESTPLATTENDATEI noch einen treffenden Namen anhängen, im Beispiel könnte das *w2ksp4\_01.vhd* sein. Der Name kann eine Versionsnummer enthalten (*\_01.vhd*). Dadurch behalten Sie den Überblick, wenn Sie auf die hier erstellte Differenzplatte später wieder eine erneute Differenzplatte aufsetzen sollten. Die Nummern müssen Sie allerdings selbst pflegen (siehe auch die Zeichnung in Abbildung 7.13).

Abbildung 7.14:  
Eine Differenzplatte  
setzt auf einer  
bekannten virtuel-  
len Festplatte auf

**Differenzierende virtuelle Festplatte**

Eine differenzierende virtuelle Festplatte ist eine virtuelle Festplatte, die einer anderen virtuellen Festplatte in einem Über-/Unterordnungsverhältnis zugeordnet ist. Die differenzierende Festplatte ist untergeordnet, und die zugeordnete virtuelle Festplatte ist übergeordnet.

Geben Sie den Speicherort an, an dem Sie eine differenzierende virtuelle Festplatte erstellen möchten. Sie können einen Speicherort aus einer Liste mit bekannten Speicherorten auswählen oder den vollqualifizierten Pfad eingeben. Die Liste der bekannten Speicherorte schließt alle unter den Suchpfaden oder im Konfigurationsordner gespeicherten Speicherorte ein. Beide Einstellungen werden auf der Seite [Suchpfade](#) angegeben.

Pfad:

Name der virtuellen Festplattendatei:

Geben Sie den Speicherort der virtuellen Festplatte an, die die übergeordnete Festplatte der neuen differenzierenden virtuellen Festplatte darstellen soll. Sie können eine virtuelle Festplatte aus einer Liste mit bekannten VHD-Dateien auswählen oder den vollqualifizierten Pfad eingeben. Beide Einstellungen werden auf der Seite [Virtual Server-Suchpfade](#) angegeben.

Es wird empfohlen, die übergeordnete Festplatte mit Schreibschutz zu versehen oder zu sperren, um Datenverluste zu vermeiden. Weitere Informationen finden Sie in der Hilfe.

Bekannte virtuelle Festplatten:

Vollqualifizierter Pfad zur übergeordneten virtuellen Festplatte:

5. Zusätzlich müssen Sie bei einer Differenzplatte noch den Namen und den Standort der virtuellen Platte angeben, auf die sich die Differenzplatte bezieht. Geben Sie hier die Platte an, die Sie gerade nach `\vmaschinen\vm_muster` verschoben haben und welche die Grundinstallation Ihres Windows 2000 Servers enthält. Wenn der Standort `\vmaschinen\vm_muster` in den Virtual Server-Suchpfaden enthalten ist, können Sie die Platten einfach aus der Liste zum Eingabefeld BEKANNTE VIRTUELLE FESTPLATTEN auswählen, wenn nicht, dann ist wieder tippen angesagt. Zum Abschluss klicken Sie auf ERSTELLEN, um die neue Differenzplatte zu erstellen.
6. Jetzt können Sie die eben erstellte Differenzplatte in der Konfiguration Ihrer VM unter FESTPLATTEN zuweisen. Sie ersetzen damit den noch vorhandenen alten Eintrag. Die neue Differenzplatte lässt sich im Verzeichnis der VM einfach aus der Liste bei BEKANNTE VIRTUELLE FESTPLATTEN auswählen (Abbildung 7.15).
7. Jetzt können Sie Ihre VM wieder starten.

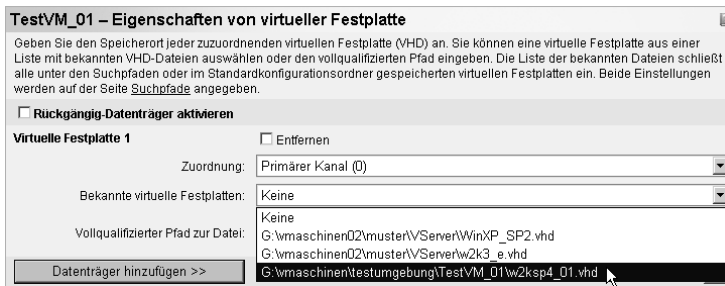


Abbildung 7.15:  
*Eine Differenzplatte kann in die VM wie eine normale virtuelle Platte eingebunden werden*

## 7.5.2 Mehrere Wiederanlaufpunkte mit kaskadierenden Differenzplatten erzeugen

Sie wissen bereits, dass alle Änderungen nur in die Differenzplatte geschrieben werden, die Basisplatte bleibt unberührt. Sie können auch mehrere Differenzplatten aufeinander aufsetzen, sozusagen kaskadieren. Damit können Sie eine Kette von Platten aufbauen, wobei jede jeweils den Änderungsfortschritt eines bestimmten Zeitraumes enthält. Bei Lesezugriffen werden alle Platten der Kette kombiniert, Schreibzugriffe landen nur in der jeweils letzten Differenzplatte (Abbildung 7.13).

Damit lassen sich verschiedene Systemzustände sichern, ähnlich den multiplen Snapshots der VMware Workstation. Um zu einem bestimmten Stand zurückzukehren, binden Sie einfach wieder die entsprechende Differenzplatte ein und löschen die darauf aufsetzen. Es sind sogar Verzweigungen in solch einem Baum möglich, z.B. um ein System mit Service-Pack und ein Referenzsystem ohne Service-Pack zu betreiben. Dazu werden vor der Installation des Service-Packs zwei Differenzplatten auf die gleiche virtuelle Platte aufgesetzt.

In einer Differenzplatte kann das Service-Pack installiert werden, wobei in der anderen Differenzplatte ohne ein solches gearbeitet werden kann. Dazu können Sie zwischen beiden Platten in der gleichen VM durch wechselseitiges Einbinden immer umschalten, oder Sie erstellen zwei separate VMs.



### Der Nachteil von Differenzplatten

Differenzplatten haben auch einen Nachteil. Ist die Basisplatte kaputt oder wurde diese verändert, dann funktionieren alle aufsetzenden Differenzplatten nicht mehr. Versehen Sie die Behälterdateien der Basisplatten am besten mit einem Schreibschutz. In Produktionsumgebungen sollten Sie kritische Server immer mit einer kompletten eigenständigen Kopie einer virtuellen Platte ausstatten.

### Änderungen in den Differenzplatten mit der Basisplatte zusammenführen

#### Verdichten und konsolidieren

Die Änderungen in den Differenzplatten können jederzeit mit der Basisplatte oder mit zugrunde liegenden anderen Differenzplatten zusammengeführt werden. Damit lassen sich die verschiedenen gespeicherten Zustände wieder verdichten und erfolgreiche Änderungen endgültig auf die übergeordnete Platte übernehmen. Damit können Sie auch wieder vollständige unabhängige Kopien von virtuellen Festplatten erzeugen, um sie z.B. weiterzugeben oder um sie in der Produktion zu benutzen.

Das Zusammenführen geschieht mit dem Menüpunkt VIRTUELLE FESTPLATTEN/ÜBERPRÜFEN. Dort wählen Sie eine differenzierende Platte aus (nicht die Basisplatte), und mittels VIRTUELLE FESTPLATTE ZUSAMMENFÜHREN wird deren Inhalt auf die übergeordnete Platte übertragen.



Achten Sie darauf, dass dabei die Daten unwiderruflich auf die zugrunde liegende virtuelle Platte geschrieben werden und diese Platte dadurch verändert wird. Setzen weitere Differenzplatten auf diese Basisplatte auf, werden sie unbrauchbar.

## 7.5.3 Verwendung von Rückgängig-Datenträgern zur Sicherung des Gassystems

Eine weitere Möglichkeit, um den Konfigurationsstand eines Gassystems zu sichern, ist die Verwendung eines Rückgängig-Datenträgers. Dazu setzen Sie in der Konfiguration der VM unter FESTPLATTEN den Haken an RÜCKGÄNGIG-DATENTRÄGER AKTIVIEREN. Ein Rückgängig-Datenträger funktioniert ähnlich wie eine Differenzplatte. Beim Einschalten der VM wird automatisch eine Datei angelegt, in der alle Änderungen an den virtuellen Platten einer VM gespeichert werden.

Im Gegensatz zur Differenzplatte müssen Sie sich um nichts kümmern, das Anlegen und die Verwaltung dieser so genannten *Undo-Logs* übernimmt Virtual Server. Sie finden bei aktiviertem Rückgängig-Datenträger im Verzeichnis Ihrer VM zu jeder virtuellen Platte eine Datei mit einem ähnlichen Namen wie diesem:

VirtualPCUndo\_meine\_Platte\_0\_0\_0\_09563905102006.vud

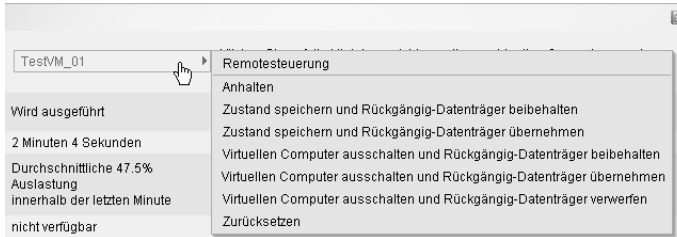


Abbildung 7.16:  
*Änderungen in den Rückgängig-Datenträgern können verworfen, aufgehoben oder festgeschrieben werden*

Im Menü der VM finden Sie bei aktiviertem Rückgängig-Datenträger mehrere Optionen vor (Abbildung 7.16). Im Wesentlichen haben Sie drei Möglichkeiten, mit den Änderungen in den Undo-Logs zu verfahren:

- ▶ *Rückgängig-Datenträger beibehalten* – Die Änderungen an den virtuellen Platten bleiben bis auf weiteres in den Undo-Logs liegen. Sie können später immer noch verworfen werden. Beim erneuten Start der VM werden die Undo-Logs einfach weitergeführt.
- ▶ *Rückgängig-Datenträger übernehmen* – Die Änderungen aus den Undo-Logs werden unumkehrbar auf die virtuelle Platte geschrieben und können danach nicht mehr verworfen werden. Beim erneuten Starten der VM entstehen neue leere Logs.
- ▶ *Rückgängig-Datenträger verwerfen* – Die Änderungen an den virtuellen Platten werden unwiderruflich verworfen. Beim erneuten Starten der VM entstehen neue leere Logs, in welche die neuen Änderungen geschrieben werden.

Abhängig davon, ob Sie den virtuellen Computer einfach *ausschalten* oder den *Zustand speichern* (Suspend-Modus), ergeben sich die Kombinationsmöglichkeiten in Abbildung 7.16.

### Nachteile bei der Verwendung von Rückgängig-Datenträgern gegenüber differenzierender Platten

Der große Nachteil an der Verwendung von Rückgängig-Datenträgern ist die Tatsache, dass damit nicht mehrere Zustände oder Wiederanlaufpunkte gesichert werden können. Entweder man verwirft das Undo-Log oder übernimmt dessen Inhalt auf die virtuelle Platte. Wollen Sie später Änderungen doch noch loswerden, ist das nach dem Übernehmen der Undo-Logs nicht mehr möglich. Übernehmen Sie dagegen Änderungen zu spät, kann es passieren, dass eine fehl-



schlagende Installation die gesamten aufgelaufenen Änderungen in den Logs kompromittiert. In so einem Falle können Sie nur das gesamte Log verwerfen und nicht mehr nur die letzte Änderung.

**Datenverlust  
durch ungewoll-  
tes Verwerfen**

Außerdem lassen sich Änderungen sehr leicht ungewollt verwerfen oder festschreiben, wenn man nicht gut aufpasst und aus Versehen den falschen Menüpunkt anklickt (siehe Abbildung 7.16). Zu guter Letzt ist es nicht ohne weiteres möglich, verschiedene Platten, z.B. Daten und System, unterschiedlich zu behandeln. Entweder es wird alles verworfen oder nichts. Wenn Sie z.B. nur eine fehlerhafte Installation an Ihrer Systemplatte verwerfen wollen, ohne die Daten auf der Datenplatte zurückzusetzen, so ist das nur mit Tricks möglich.



Wollen Sie unter bestimmten Umständen bei aktiven Rückgängig-Datenträgern einmal Änderungen an nur an einer bestimmten Platte verwerfen, die Änderungen an den anderen Platten dagegen erhalten, dann können Sie das Undo-Log manuell löschen, das zur betreffenden Platte gehört. Damit reparieren Sie beispielsweise ein vom Trojaner befallenes System, ohne Änderungen an den Daten zu verlieren.

## 7.6 Klonen virtueller Maschinen und Ausbau der Testumgebung

In Ihrer Testmaschine können Sie die Migration von Windows 2000 Server auf Windows 2003 Server bzw. andere Konstellationen bereits bequem testen. Wiederanläufe sind jederzeit möglich. So können Sie sich mit dem Migrationsvorgang vertraut machen und auch verschiedene Abläufe und Szenarien immer wieder durchspielen, ohne jedes Mal das System komplett neu aufzusetzen oder zeitraubende Sicherungs-Images einzuspielen.

**Eindeutige  
Namen und  
IP-Adressen**

Um ein komplettes Testnetz aufzubauen, könnten Sie weitere Maschinen installieren. Benötigen Sie mehrmals das gleiche Betriebssystem, lassen sich durch einfaches Kopieren des Ordners einer VM oder nur der virtuellen Systemplatte problemlos vollständige Klone erzeugen. In einer Testumgebung eignen sich Differenzplatten sehr gut, um zeit- und platzsparend weitere Maschinen zu klonen (*Abschnitt 7.5.1, „Mit Differenzplatten den Zustand einer Installation sichern oder weitere Duplikate klonen“*). So entstehen in Minuten Netze mit mehreren Clients und Servern. Wie in der realen Welt ist in jedem Klon für eine eindeutige IP-Adresse und für einen eindeutigen Rechnernamen und SID (*Computer Security Identifier*) zu sorgen. Das kann mittels *Sysprep* oder dem Tool *NewSID* erfolgen. Nähere Informationen zum zentralen Thema Klonen finden Sie in Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“.

Natürlich benötigen Sie für alle laufenden virtuellen Maschinen auch Lizenzen der darin gestarteten Betriebssysteme, wenn Sie keine freie Software wie Linux einsetzen. Hier kann Ihnen die Lizenzierung der Windows 2003 R2 Server Enterprise Edition zugute kommen. Mit einer Version haben Sie damit gleichzeitig vier Lizenzen für virtuelle Maschinen auf demselben Host zur Verfügung. Das bedeutet, Sie können eine Instanz auf dem Host selbst laufen lassen und zusätzlich (aber nur auf dem gleichen Host!) in vier virtuellen Maschinen weitere Instanzen.

### 7.6.1 Internes Testnetzwerk aufbauen

Alle virtuellen Maschinen der Testumgebung sollten an einem intern abgeschotteten Netzwerk angeschlossen sein (Abbildung 7.12). Um auch mit dem LAN kommunizieren zu können, etwa um Daten auszutauschen, kann im einfachsten Falle eine VM mit zwei virtuellen Adaptern als Router dienen. Ein Adapter ist an das interne Netzwerk angeschlossen, den zweiten Adapter weisen Sie einem externen Netzwerk zu. Die VM kann damit das interne Netz als separates LAN-Segment an Ihr Firmennetz anbinden.

Wenn Sie aus Sicherheitsgründen auf das Routing verzichten wollen, können Sie alle Dateien auch erst aus dem LAN auf die VM kopieren und dann von den Gästen am internen Netz dort abholen. Es existieren verschiedene weitere Möglichkeiten, so kann etwa auch der Host selbst das Routing übernehmen oder mittels *Internet-Verbindungsfreigabe (ICS)* alle VMs über *NAT (Network Address Translation)* an Ihr LAN anbinden. Mehr zum komplexen Thema Netzwerke finden Sie in *Teil 3, Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“*.

## 7.7 Physische Maschinen in die Pilotumgebung übernehmen

Zwar ist eine Migration Ihres Betriebssystems in einer sauberen Testumgebung sehr lehrreich, aber leider wenig aussagekräftig. Erst mit den realen Applikationen, Dateistrukturen und Benutzern lässt sich das Migrationskonzept auf Herz und Nieren prüfen. Dazu können Sie echte Server in virtuelle Maschinen klonen, um in einem eigenen abgeschotteten Netz die reale Umgebung 1:1 nachzubilden – mitsamt virtueller Clients und Anwendungsprogramme.

Für das Übernehmen einer physischen Maschinen in eine virtuelle Maschine (kurz: P2V) existiert ein separater Workshop in *Teil 3, Kapitel 6, „P2V – physische Server in virtuelle Maschinen übernehmen“*. Microsoft und verschiedene Fremdhersteller bieten für diesen P2V-Vorgang Tools an, z.B. das *Virtual Server Migration Toolkit (VSMT)*, das Microsoft kostenlos zur Verfügung stellt:

[www.microsoft.com/germany/virtualserver/downloads/vsmt.mspx](http://www.microsoft.com/germany/virtualserver/downloads/vsmt.mspx)

**Klonen mit einem Imaging-Tool**

Mit einem Imaging-Tool, wie Acronis oder Ghost, können Sie die meisten Systeme aber auch manuell in Ihre Pilotumgebung übernehmen. Im Prinzip fertigen Sie dazu von der Systemplatte der Quelle ein Image an, das Sie dann in einer Hilfs-VM über das Netzwerk auf eine leere virtuelle Platte zurückspielen. Die benötigten Testdaten für die Pilotumgebung überträgt später die gewohnte Sicherungssoftware per Agent ins laufende Gastsystem.

Im Quellsystem sollten Sie vor dem Klonen des Systems die richtigen Treiber für den virtuellen Controller der Ziel-VM vorinstallieren, damit das System in der VM die Bootplatte findet. Am einfachsten gelingt das mit einem *Standard-PCI-IDE-Controller*. Nach dem Ausdünnen des Quellsystems (Temp-Ordner, Papierkorb, Dump-Files usw.) können Sie das Image anfertigen und in die VM zurückspielen. In vielen Fällen funktioniert das Übertragen auf Anhieb. Allerdings lauern auch verschiedene Stolperfallen, wie das notwendige Anpassen der *Boot.ini* oder der *HAL* (*Hardware Abstraction Layer*) usw. Darauf gehe ich in *Teil 3, Kapitel 6*, sehr ausführlich ein.

### 7.7.1 Ausblick – komplette Virtualisierung der produktiven Umgebung

Nach ausgiebigen Probeläufen in der virtuellen Pilotumgebung können Sie Ihre geplante Migration gut vorbereitet an den echten Produktionsservern durchführen. Vorher ist zu überlegen, ob Sie diese Systeme nicht gleich komplett virtualisieren wollen. Laufen nämlich die Produktionsserver sowieso schon in virtuellen Maschinen, dann kann die Migration genauso bequem durchgeführt werden wie in der Testumgebung.

Läuft etwas schief, ist mit dem Einspielen der gesicherten virtuellen Platten der originalen Maschinen oder im einfachsten Falle mit dem Verwerfen einiger Differenzplatten der alte Zustand viel schneller und komfortabler wiederhergestellt als auf einem physischen Rechner. So hat man zwar das Wochenende mit einem vergeblichen Migrationsversuch verbracht, kann aber für den Montag problemlos die alte Umgebung wiederherstellen. In größeren Umgebungen sollten Sie dabei allerdings immer die Zusammenhänge in komplexen Netzwerken beachten, etwa mehrere Domänencontroller oder voneinander abhängige Dienste, die Sie vor Migrationsversuchen möglichst als Ganzes sichern sollten.

**Eine Pilotumgebung ist die beste Vorbereitung**

Vor der endgültigen Virtualisierung der Produktionsumgebung konnten Sie sich mit dem Umgang Ihres Virtualisierungsproduktes in der Pilotumgebung bereits bestens vertraut machen, und viele potenzielle Fehlerquellen haben Sie beim Übertragen der Systeme in die Testumgebung schon aufgespürt. Wie bereits als Auftakt dieses Workshops erwähnt – eine virtuelle Pilotumgebung ist die beste Vorbereitung auf die Virtualisierung der Produktionssysteme.



# Cluster mit VMs und einem iSCSI-Target als externem Speicher

Sie installieren einen Windows-Cluster mit virtuellen Maschinen. Durch die Verwendung von externem Speicher (SAN) können Sie die Lösung schrittweise aufbauen und erweitern. Als externer Speicher dient in der Testumgebung ein Software iSCSI-Target in einer VM, so dass Sie für den Workshop nicht unbedingt über ein physisches SAN verfügen müssen. Sie starten mit der Testumgebung auf ein und demselben Host. Diesen Aufbau erweitern Sie zur echten Hochverfügbarkeitslösung, in der virtuelle Maschinen auf separaten physischen Hosts einen Cluster bilden und auch ein physisches SAN verwenden können.

**iSCSI-Target als Software-Lösung in einer VM**

## Workshop im Überblick

### Hauptprodukt

- ▶ VMware Server oder Microsoft Virtual Server 2005 R2
- ▶ Umsetzung mit VMware Workstation 5.5 möglich

### Praktische Verwendung

- ▶ Cluster-Konfigurationen ohne zusätzliche Hardware auf einem einzigen Rechner in virtuellen Maschinen testen.
- ▶ Den Umgang mit den Cluster-Diensten in einer Testumgebung erlernen.
- ▶ Hochverfügbarkeit durch die Verteilung der virtuellen Cluster-Knoten auf physisch getrennte Host-Systeme erreichen.

### Schwerpunkte

- ▶ Konzepte virtueller Maschinen als Zusammenfassung – virtuelle Netzwerke und Adapter, virtuelle Festplatten, klonen von VMs usw.
- ▶ Verwendung von iSCSI in einer VM über virtuelle Netzwerkkarten.
- ▶ Installation eines Software-Targets als preiswertes SAN.

### Zielgruppe

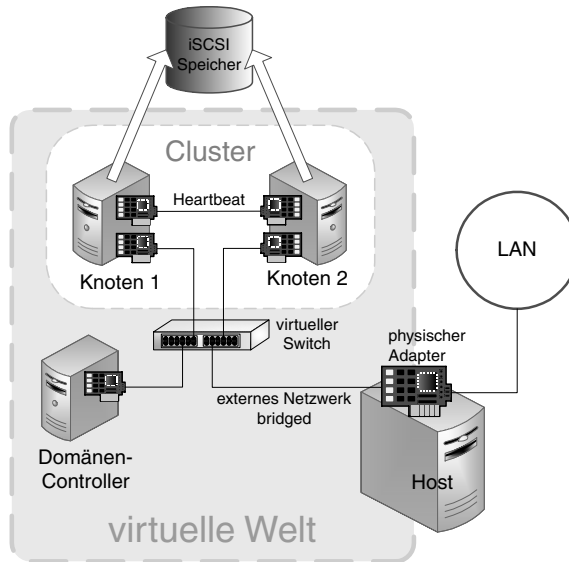
- ▶ Administratoren, Techniker, Consultants, Trainer

## 8.1 Clusterlösungen testen oder produktiv einsetzen

**VMware Server, Workstation und Microsoft Virtual Server**

Der folgende Workshop liefert Ihnen ein komplexes Beispiel für die Verwendung von VMs in Verbindung mit zusätzlichen Virtualisierungstechnologien, wie Speichervirtualisierung mit einem SAN oder die Virtualisierung von Ressourcen durch Cluster. Das Kapitel dient damit gleichzeitig als Zusammenfassung des Buches und zeigt das Zusammenspiel aller Komponenten – von virtuellen Netzwerken über virtuelle Festplatten bis zum Kopieren und Klonen von VMs.

*Abbildung 8.1:  
In der ersten Ausbaustufe entsteht der Cluster auf einem einzigen Host. Später werden die Knoten auf separate Hosts verteilt*



Der Workshop ist nicht unbedingt für Neueinsteiger konzipiert, er geht aber auf die wichtigsten Aspekte im Umgang mit VMs als Überblick nochmals ein. Hauptsächlich konzentrieren wir uns allerdings auf den Aufbau eines Clusters mit zwei virtuellen Maschinen, der gleichermaßen für den VMware Server und für Microsoft Virtual Server beschrieben wird. Die Umsetzung für eine Testumgebung ist auch mit der VMware Workstation möglich, wenn Sie z.B. den Umgang mit einem Cluster erlernen wollen, ohne zusätzliche Hardware anzuschaffen.

### 8.1.1 Was ist ein Cluster?

**Ein Cluster umfasst mehrere Rechner als Knoten**

Stellt sich die Frage – was ist überhaupt ein Cluster, wozu brauche ich das? Ein Cluster ist eine Zusammenfassung von mehreren Rechnern zu einem Verband. Die einzelnen Rechner eines Clusters werden auch als *Knoten* bezeichnet. Jeder Knoten kann eine bestimmte Aufgabe übernehmen bzw. einen bestimmten Dienst anbieten, z.B. im einfachsten Falle eine Dateifreigabe bereitstellen oder Teile einer Rechenaufgabe lösen. Der Cluster mit seinen Knoten tritt nach außen immer

als Gesamtheit auf. Die einzelnen physischen Rechner (Knoten) treten nicht in Erscheinung, wo konkret ein bestimmter Dienst läuft, spielt nach außen keine Rolle. Es gibt verschiedene Arten von Clustern, Sie finden hier einen kurzen Überblick:

- *Cluster für Hochverfügbarkeit* dienen dazu, einen Dienst ausfallsicher bereitzustellen, der beim kompletten Ausfall eines Knotens oder beim Absturz einer Software von einem anderen Knoten übernommen wird. Im besten Falle geschieht das in Echtzeit, ohne dass verbundene Anwender einen Ausfall bemerken. Ist im Cluster z.B. ein Exchange-Server installiert und auf einem Knoten würde der Exchange-Dienst abstürzen, dann könnte die Datenbank (Postfächer, öffentliche Ordner) automatisch vom anderen Knoten übernommen werden.

**Unvorhergesehener Ausfall**

Ein weiterer guter Grund für einen Cluster sind geplante Wartungsarbeiten, etwa das Einspielen eines neuen Service-Packs auf einem der Server. Sie können alle Ressourcen unterbrechungsfrei auf eine andere Maschine verschieben und ohne Störung des Betriebes am freien Knoten administrative Aufgaben erledigen.

**Geplante Wartungsarbeiten**

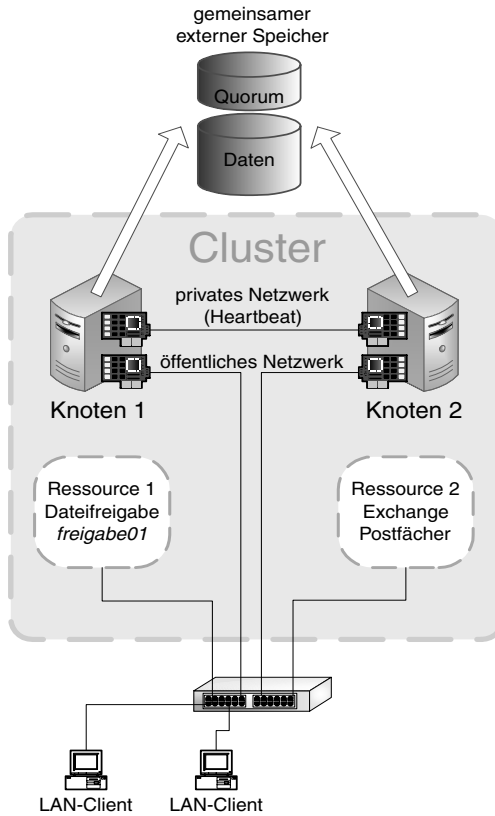
- *Cluster für Lastverteilung (Load Balancing)* dienen dazu, die Last auf mehrere physische Rechner gleichmäßig zu verteilen. Beispiele dafür sind Terminalserverfarmen unter Citrix Presentation Server oder der Netzwerklastenausgleich (*Network Load Balancing, NLB*) von Microsoft. Mit solchen Diensten werden Zugriffe auf mehrere Webserver oder Nutzer auf verschiedene Terminalserver (*Serverfarm*) verteilt.
- *Für das Erreichen hoher Rechenleistungen* können ebenfalls einzelne Computer zu Clustern zusammengefasst werden, etwa um eine rechenintensive Simulation auf viele CPUs aufzuteilen. Ein Beispiel sind Linux-Cluster auf handelsüblichen PCs, die als Verbund die Leistung von Highend-Großrechnern erreichen können.

In diesem Workshop beschreibe ich den Aufbau eines *Hochverfügbarkeits-Clusters* mit zwei virtuellen Maschinen als Knoten unter den *Microsoft Cluster-Diensten*, konkret mit dem Windows Server 2003 R2 Enterprise Edition.

## 8.1.2 Wie funktioniert ein Cluster?

Vor der Umsetzung des Workshops sollten Sie in groben Zügen die Komponenten eines Clusters kennen. An einem einfachen Beispiel eines Clusters, der eine Dateifreigabe für die Nutzer im LAN bereitstellt, erkläre ich die grundlegenden Funktionen (Abbildung 8.2). Sollten Sie bereits Erfahrungen mit den Microsoft Cluster-Diensten haben und die Funktion von iSCSI kennen, dann können Sie sofort mit der eigentlichen Realisierung des virtuellen Clusters beginnen. Die eigentliche Konfiguration beginnt weiter unten bei *Abschnitt 8.2, „Das Konzept – stufenweiser Ausbau eines Clusters mit virtuellen Maschinen“*.

Abbildung 8.2:  
Der prinzipielle Aufbau eines Hochverfügbarkeits-Clusters mit den Microsoft Cluster-Diensten



Auf die Daten einer Ressource muss von jedem Knoten aus zugegriffen werden können.

Ein Knoten wird vom LAN aus nicht direkt verwendet, sondern er stellt logische Ressourcen bereit.

Eine bestimmte Ressource kann von jedem Knoten im Cluster bereitgestellt werden.

Ein Client greift nicht direkt auf einen Knoten, sondern immer auf eine logische Ressource zu.

### Virtuelle (logische) Adressen und Ressourcen eines Clusters

#### Zugriff vom LAN erfolgt auf logische IP-Adressen

Herzstück eines Clusters ist der Cluster-Dienst, der alle Ressourcen verwaltet. Er steuert, auf welchem Knoten (Server) eine bestimmte Ressource aktiv ist. Eine Ressource kann z.B. eine Dateifreigabe, ein Exchange-Postfachspeicher oder im einfachsten Falle eine IP-Adresse sein. Nach außen stellt der Cluster-Dienst diese Ressourcen unter logischen (virtuellen) Namen und Adressen im Netzwerk bereit.

Ein Cluster tritt im LAN und für die Anwender immer als Einheit auf, die einzelnen Knoten werden üblicherweise nicht direkt angesprochen. Zwar hat jeder Knoten im Cluster eine eigene IP-Adresse und einen eigenen Namen, diese dienen allerdings nur der internen Verwaltung. Nach außen verfügt dagegen jede bereitgestellte Ressource im Cluster über einen eigenen virtuellen Namen und eine eigene virtuelle IP-Adresse, die von den Clients angesprochen wird. Dabei spielt es keine Rolle, auf welchem physischen Cluster-Knoten die Ressource wirklich zur Verfügung steht.

Die virtuellen Namen und virtuellen IP-Adressen haben in diesem Kontext nichts mit virtuellen Maschinen zu tun, sie existieren genauso bei Clustern, die nur aus physischen Rechnern bestehen. Die Ressourcen eines Clusters sind gewissermaßen auch virtualisiert, weil der Anwender nicht weiß, auf welcher Hardware sie gerade laufen.



Beispielsweise hat der Cluster-Knoten 1 wie ein normaler Fileserver Zugriff auf eine bestimmte Partition eines Datenspeichers. Knoten 1 stellt den Inhalt dieser Partition, also Ordner und Dateien, unter einer virtuellen IP-Adresse und einem virtuellen Freigabenamen *freigabe01* als Ressource im LAN zur Verfügung (Abbildung 8.2). Ein Benutzer kann sich mit dieser virtuellen Freigabe verbinden und gespeicherte Dokumente bearbeiten. Da die Ressourcen von außen nur über logische (virtuelle) Adressen angesprochen werden, spielt es letztendlich auch keine Rolle, welche physische Maschine die Freigabe gerade bereitstellt. Der Cluster-Dienst muss nur dafür sorgen, dass die richtige Zuordnung der virtuellen IP-Adresse und des Namens (*freigabe01*) nach außen immer gegeben ist.

### Heartbeat-Netzwerk zur Überwachung eines Clusters und öffentliches Netzwerk zur LAN-Kommunikation

Zusätzlich überwacht der Cluster-Dienst ständig, ob alle Knoten noch laufen und alle Ressourcen verfügbar sind. Das geschieht hauptsächlich über den so genannten *Heartbeat*. Das sind Signale, die von jedem Knoten in bestimmten Zeitabständen gesendet werden. Empfängt der Cluster-Dienst kein Signal mehr, kann er davon ausgehen, dass ein Knoten ausgefallen ist. Dazu sind alle Knoten meist über separate Netzwerkkarten und ein extra Netzwerk (*privates Netzwerk* oder *Heartbeat-Netzwerk*) untereinander verbunden. Die Kommunikation mit dem LAN erfolgt dagegen über das *öffentliche Netzwerk* des Clusters. Beide Netzwerke könnten zwar über die gleichen Adapter und Verbindungen betrieben werden. In einer sauberen Cluster-Konfiguration werden aber immer getrennte Netzwerke verwendet, für das Heartbeat-Netzwerk genügt im einfachsten Falle ein Crosslink-Kabel.

**Überwachung  
des Zustandes  
der Knoten**

### Failover von Ressourcen auf einen anderen Knoten

Fällt in unserem Beispiel der Cluster-Knoten 1 aus, z.B. durch einen Hardware-Defekt oder durch geplante Wartungsarbeiten, dann übernimmt Knoten 2 automatisch seine Dienste im Cluster. Dieser Vorgang wird als *Failover* bezeichnet. Wenn die Übernahme schnell genug vonstatten geht, dann bemerkt ein Anwender nicht, dass die physische Hardware ausgefallen ist. Der Anwender war schließlich nicht direkt mit Knoten 1 verbunden, sondern mit einem virtuellen Namen, der Dateifreigabe *freigabe01*. Diese Dateifreigabe steht jetzt auf Knoten 2 zur Verfügung.



Damit der Rechner, der Knoten 2 darstellt, die Arbeit von Knoten 1 übernehmen kann, muss er allerdings Zugriff auf den gleichen Datenspeicher haben. Nur so kann er die Ordner und Dateien für *freigabe01* bereitstellen. Dieser Zugriff auf gemeinsame Datenträger ist ein zentraler Punkt in einem Cluster und unterscheidet die Knoten von üblichen Servern.

### **Shared Storage (gemeinsamer Speicher) – die Voraussetzung zum Aufbau eines Clusters**

#### **Externer Speicher für das Quorum**

Zum einen müssen alle Knoten im Cluster gemeinsam auf den so genannten *Quorumdatenträger* zugreifen können. Das ist ein Datenspeicher, in dem ständig Statusinformationen zu den laufenden Diensten und Ressourcen abgelegt werden. Daraus können später andere Knoten den Status einer Cluster-Anwendung nach einem Ausfall rekonstruieren. Jeder Cluster-Knoten muss Zugriff auf den Quorumdatenträger haben, eine lokale Festplatte genügt also nicht.

Zusätzlich muss jeder Knoten, der einen bestimmten Dienst übernehmen soll, Zugriff auf die Daten zu diesem Dienst haben. Bei einer Dateifreigabe wäre das eine Ordnerstruktur, bei einem Exchange Server ist das die Datenbank mit den Postfächern. Also müssen auch diese Daten in einem gemeinsamen Datenspeicher liegen.

#### **Gemeinsamer Zugriff auf Datenträger**

Im Normalfall sind Betriebssysteme jedoch nicht darauf ausgelegt, gemeinsam von verschiedenen Rechnern auf dieselben Festplatten zuzugreifen. Durch Schreibcashes und vor allem durch Kopien der FAT (*File Allocation Table*, *Dateizuordnungstabelle*) im RAM würde ein direkter gemeinsamer Schreibzugriff früher oder später zum Datenchaos führen. Das liegt daran, dass ein System vom anderen nicht weiß, welche Sektoren gerade beschrieben wurden und welche noch frei sind.

Der gemeinsame Zugriff muss deshalb vom Cluster-Dienst gesteuert werden. Ein Knoten hat immer einen bestimmten Datenträger exklusiv im Zugriff. Erst bei einem Failover wird diesem Knoten der Zugriff entzogen, und dem Knoten, der die Dienste übernimmt, wird der Zugriff gestattet. Mit physischen Maschinen stehen grundsätzlich zwei Varianten für den gemeinsamen Datenspeicher zur Verfügung:

- ▶ Entweder es kommt ein externes Festplattengehäuse mit speziellen Anschlussadaptern (*SCSI-Kits*) zum Einsatz. Diese Adapter übernehmen die problematische Terminierung des SCSI-Busses, an den die Controller beider Knoten gleichzeitig angeschlossen werden.
- ▶ Oder es wird ein externer Speicher (*SAN – Storage-Area-Network*, *Speichernetzwerk*) verwendet. Mehr Informationen zur SAN-Technologie finden Sie in *Teil 1, Kapitel 1, „Grundlagen virtueller Maschinen und Hinweise zur Hardware“*. Auf diesen Speicher erfolgt der Zugriff über ein spezielles Speichernetzwerk mit Glasfasertechnologie und spezieller Hardware (*Fibre-Channel*) oder über eine normale Ethernet-Verkabelung (*iSCSI* – siehe „Die Funktion von iSCSI“).

Grundsätzlich existieren auch bei virtuellen Maschinen beide Anschlussmethoden, es gibt aber ein paar Besonderheiten.

### 8.1.3 Besonderheiten eines Clusters mit virtuellen Maschinen

Wenn ein Cluster zwischen virtuellen Maschinen aufgebaut werden soll, bleibt das Prinzip das gleiche wie bei einem Cluster aus physischen Servern. Nur der Zugriff auf den externen Speicher ist etwas problematisch.

#### Zugriff aus den virtuellen Maschinen auf den gemeinsamen Speicher

In virtuellen Maschinen können Sie ebenfalls mit beiden Ansätzen arbeiten – entweder Sie verwenden eine gemeinsame virtuelle SCSI-Platte oder einen externen Speicher als gemeinsamen Datenträger für die Knoten. Beide Verfahren werden von den Virtualisierungsprodukten unterstützt. Jede Methode hat Vor- und Nachteile.

Verwenden Sie eine virtuelle SCSI-Platte als gemeinsamen Datenträger, dann funktioniert das unter fast allen Virtualisierungsprodukten nur auf ein und demselben Host (außer beim ESX Server mit SAN-Anbindung – siehe Teil 2, Kapitel 9, „VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2“). Durch die gemeinsame Verwendung einer virtuellen Platte auf dem gleichen Host ist ein Cluster-Aufbau bei den Hosted-Produkten sehr unflexibel und kommt eher für Testumgebungen in Frage. Beim Ausfall des Hosts bricht der gesamte Cluster weg. Damit ist höchstens eine bestimmte Anwendung im Gast durch den Cluster vor Software-Abstürzen geschützt (siehe auch Abschnitt 8.1.4, „Cluster-Konstellationen – VM mit VM oder Hardware mit VM“). Ich gehe am Ende des Workshops auf die Einbindung einer gemeinsamen virtuellen SCSI-Platte für reine Testumgebungen ein (Abschnitt 8.4.1, „Cluster mit einer gemeinsamen virtuellen SCSI-Festplatte anstelle von externem Speicher“).

**Virtuelle SCSI-Platte als gemeinsamer Speicher**

Besser wäre also der Zugriff auf externen Speicher (SAN) als gemeinsamen Datenträger, wobei wiederum Fibre-Channel oder iSCSI zum Einsatz kommen kann. Eine schnelle Fibre-Channel-Anbindung kann allerdings nur von VMs unter dem VMware ESX Server als gemeinsamer Datenträger verwendet werden. Also fällt auch diese Möglichkeit für unseren Workshop weg, da sie von zu wenigen Produkten abgedeckt wird.

**SAN mit Fibre-Channel oder iSCSI**

Der beste Kompromiss für unseren Workshop ist eine Anbindung des gemeinsamen externen Datenspeichers über iSCSI. Diese Methode wird von allen Virtualisierungsprodukten unterstützt. Vor allem ist damit auch beim VMware Server oder beim Microsoft Virtual Server ein Cluster über VMs auf unterschiedlichen Hosts oder sogar zwischen einer VM und einem Hardware-Server möglich. Das Besondere an iSCSI ist, dass zur Kommunikation mit dem SAN ganz normale Netzwerkkarten benutzt werden können. Im Gegensatz zu Fibre-Channel ist also keine spezielle Hardware notwendig, es können damit auch die virtuellen Adapter in den Gästen verwendet werden.

**Externer Speicher mit iSCSI**

Dadurch ist iSCSI derzeit die einzige allgemein gültige Lösung, um aus einer VM heraus direkt auf externen Datenspeicher zuzugreifen und einen Cluster über verschiedene Hosts zu konfigurieren.

### Die Funktion von iSCSI

Die Funktion von iSCSI wurde bereits in *Teil 1, Kapitel 1, „Grundlagen virtueller Maschinen und Hinweise zur Hardware“* erklärt. Prinzipiell ermöglicht es iSCSI, über eine vorhandene Ethernet-Verkabelung und die üblichen Netzwerkkarten und Switches einen externen Speicher an einen Server anzubinden. Grundsätzlich spielen zwei Komponenten eine Rolle, das *Target* und der *Initiator*.

- |                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Das Target ist der Speicher</b>    | Ein iSCSI-Target ist der Ort, an dem die Daten liegen und auf den alle angebundenen Rechner zugreifen wollen. Ein iSCSI-Target kann ein dediziertes SAN mit iSCSI-Schnittstelle sein oder eine Software-Lösung auf einem Linux- oder Windows-Server. Die Möglichkeit einer Software-Lösung verwenden wir in diesem Workshop, da ich nicht davon ausgehen kann, dass Sie über freien externen Speicher zum Experimentieren verfügen. Wir setzen einfach unser eigenes Target in einer virtuellen Maschine auf, dazu später mehr.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Der Initiator ist der Client</b>   | Der iSCSI Initiator ist die Clientkomponente, über die der Zugriff auf das Target erfolgt. Über den Initiator benutzt der Rechner den externen Speicher wie eine lokal eingebaute Festplatte. Ein Initiator kann entweder ein so genannter <i>HBA (Host Bus Adapter)</i> sein. Das ist eine physische Steckkarte, die in den Server eingebaut wird. Sie kommuniziert über das Netzwerk mit dem Target und wirkt für den Rechner wie ein RAID-Controller mit lokal angeschlossenen Festplatten. Ein Hardware-Initiator verfügt über einen eigenen Prozessor, der das gesamte Protokollhandling übernimmt. Das entlastet die CPU des Servers und kommt der Performance zugute. Da eine VM nicht auf solche spezielle Hardware zugreifen kann, kommt ein HBA für uns aber nicht in Frage.                                                                                                                                                                                                                                        |
| <b>Software-Initiator in einer VM</b> | Eine weitere Möglichkeit ist ein so genannter <i>Software-Initiator</i> . Dieser wird als Treiber im Betriebssystem eines Clients installiert und verwendet eine verfügbare Netzwerkkarte, um darüber mit dem iSCSI-Target zu kommunizieren. Das hat den Vorteil, dass recht preiswerte Hardware zum Einsatz kommt. Vor allem kann solch ein Software-Initiator auch eine virtuelle Netzwerkkarte in unseren Gastsystemen benutzen. Damit wird es möglich, direkt aus einem Gast auf externen Speicher zuzugreifen. Der Nachteil liegt in der schlechteren Performance, da die CPU des Rechners belastet wird, um den Protokollverkehr zu verwalten. Noch mehr wirkt sich dieser Umstand in einer virtuellen Maschine aus, weil dort keine optimierte Netzwerkkarte mit eigenem Controller ( <i>Hardware-Offload</i> ) die CPU von ihrer Denkarbeit entlasten kann. Im Gegenteil – jede virtuelle Netzwerkkarte belastet die CPU des Hosts zusätzlich, da dieser Adapter vom Virtualisierungslayer erst emuliert werden muss. |

Trotz der genannten Nachteile – in unseren Workshop ist iSCSI mit einem Software-Initiator in den Gastsystemen derzeit die flexibelste Lösung für einen Cluster mit VMs. In Produktionsumgebungen hängt die Praxistauglichkeit stark vom Datenaufkommen und von der eingesetzten Hardware des Hosts ab. Hinweise dazu finden Sie unter *Abschnitt 8.5, „Praxistauglichkeit der vorgestellten Lösung mit iSCSI Software Initiator“*, nachdem ich Sie mit allen Aspekten der Cluster-Konfiguration vertraut gemacht habe.

## Öffentliches und privates Netzwerk sowie Speichernetzwerk des Clusters mit virtuellen Netzwerken

Zusätzlich zum gemeinsam nutzbaren Datenspeicher (*Shared Storage*) benötigt ein Cluster mindestens zwei Netzwerke: eines zur öffentlichen Kommunikation mit dem LAN (*öffentliches Netzwerk*) und eines für die interne Kommunikation als Heartbeat-Netzwerk (*privates Netzwerk*). Rein technisch könnte das private Netzwerk auch über die gleichen Netzwerkkarten wie die für das LAN betrieben werden, das wäre aber keine saubere Cluster-Konfiguration.

**Der virtuelle Cluster benötigt drei Netzwerke**

Die Verwendung verschiedener Netzwerke ist in unserer virtuellen Umgebung kein Problem. Für die öffentliche Anbindung können wir ein *Bridged-Netzwerk* unter VMware bzw. ein *externes Netzwerk* unter Microsoft verwenden. Für das Heartbeat-Netzwerk bietet sich ein unbenutzter *VMnet-Switch* bzw. ein *internes Netzwerk* an. Zum Testen können Sie vorerst ausschließlich interne Netzwerke verwenden.

Der Zugriff auf den externen Speicher über iSCSI sollte in der Praxis aus Performancegründen unbedingt ebenfalls über ein dediziertes Netzwerk erfolgen. Wir halten uns auch in unserer Testumgebung daran. Aus diesem Grunde benötigen die Knoten des Clusters jeweils einen dritten Netzwerkkadapter, über den ausschließlich die iSCSI-Kommunikation zum externen Speicher abläuft. Wir nennen dieses Netzwerk das *Speichernetzwerk* (siehe auch Abbildung 8.3).

**Das Speichernetzwerk**

Detaillierte Informationen zur Konfiguration der virtuellen Netzwerke aller Virtualisierungsprodukte erhalten Sie in *Teil 3, Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“*.

### 8.1.4 Cluster-Konstellationen – VM mit VM oder Hardware mit VM

Grundsätzlich existieren verschiedene Möglichkeiten für den Aufbau eines Clusters mit virtuellen Maschinen. Durch die hohe Flexibilität bei der Verwendungen eines externen Speichers auf Basis von iSCSI können Sie im Grunde jede der folgenden Konstellationen mit dem Wissen aus diesem Workshop nachvollziehen:

**Mit externem Speicher sind alle Konstellationen möglich**

- ▶ *Hardware <> Hardware* – Üblicherweise werden immer noch viele Cluster komplett in Hardware realisiert. Zwei physische Geräte bilden einen Cluster, virtuelle Maschinen spielen dabei keine Rolle.
- ▶ *VM <> VM auf dem gleichen Host* – Auf ein und demselben Host können zwei VMs als ein Cluster betrieben werden. Das wird sehr gerne in Testumgebungen verwendet, um ohne zusätzliche Hardware Cluster-Dienste zu testen.

Als Hochverfügbarkeitslösung hat dieses Modell Mängel, da beim Defekt der Host-Hardware beide virtuellen Knoten ausfallen. Es bleibt aber der Vorteil, für Wartungsarbeiten einen virtuellen Knoten im laufenden Betrieb frei zu machen, um etwa ein Service-Pack im Gastsystem zu installieren. Vor reinen Software-Abstürzen in einer VM schützt diese Art des Clusters ebenfalls.

- ▶ *VM <> VM auf unterschiedlichen Hosts* – Wenn die VMs, die den Cluster bilden, auf unterschiedlichen Hosts liegen, dann bietet diese Lösung echte Hochverfügbarkeit. Die Konstellation nennt man auch *Cluster across boxes*. Fällt ein Host aus und damit die VM, dann übernimmt die VM auf dem noch laufenden Host die Ressourcen. Auf jedem Host können dabei mehrere Knoten verschiedener virtueller Cluster laufen.
- ▶ *Hardware <> VM* – Um Hardware zu sparen und trotzdem optimale Leistung zu erhalten, können die Verfahren kombiniert werden. Alle Dienste laufen dabei auf physischen Knoten, das bietet beste Performance auch in Lastspitzen. Um nicht für jeden Knoten einen weiteren Server als Stand-by-Gerät anschaffen zu müssen, wird für jeden physischen Knoten eine VM als virtueller Ausfallknoten auf einem einzigen physischen Host aufgesetzt. Fällt ein Hardware-Knoten aus, dann werden seine Dienste von einer VM übernommen, bis die Hardware wieder läuft.

Fallen alle Hardware-Knoten aus, was eher unwahrscheinlich ist, dann muss der Host allerdings alle VMs gleichzeitig tragen können, die dann plötzlich zum aktiven Cluster-Knoten geworden sind.

- ▶ *Host <> Host* – Eine Besonderheit ist das so genannte Host-Clustering. Dabei ist der Host selbst ein Cluster-Knoten, und alle laufenden VMs sind jeweils Ressourcen im Cluster. Fällt der Host aus, dann werden alle VMs automatisch auf einem anderen Host neu gestartet. Das hat Vorteile, aber auch Grenzen – siehe *Abschnitt 8.4.2, „Host-Cluster – komplette VMs als Ressourcen von Host zu Host verschieben“*.

Im Workshop beginnen wir mit dem Aufbau der Konstellation *VM <> VM* auf einem einzigen Host und verteilen die VMs später auf unterschiedliche Hosts. Theoretisch könnten Sie auch eine physische Maschine als Knoten zum Cluster hinzufügen, wenn diese Maschine Zugriff auf das gleiche iSCSI-Target hat. Dann kann für diesen Server sogar ein HBA verwendet werden.

## 8.2 Das Konzept – stufenweiser Ausbau eines Clusters mit virtuellen Maschinen

Das war einiges an Vorrede – und noch nicht eine einzige virtuelle Maschine konfiguriert! Wir sollten beginnen, uns Gedanken um ein Konzept zu machen.

### 8.2.1 Der Aufbau des Clusters mit VMs und die eingesetzte Software

Die Cluster-Knoten müssen für einen Microsoft Cluster Mitglied einer Domäne sein. Dazu werden wir auf einem Host eine Infrastruktur aus einem Domänencontroller mit der Domäne *clusdom* und zwei weiteren VMs als Cluster-Knoten aufbauen. Sie benötigen also drei VMs, am einfachsten mit demselben Betriebssystem. Wir nennen sie *clus01*, *clus02* und *srv01* (Abbildung 8.3). Als Software auf den Cluster-Knoten und auf dem Domänencontroller dient der Microsoft Windows Server 2003 R2 Enterprise Edition. Die Einstiegsseite zum Windows Server 2003 R2, inkl. Link zum Download einer Testversion finden Sie hier:

[www.microsoft.com/germany/windowsserver2003/](http://www.microsoft.com/germany/windowsserver2003/)

**Ein Domänencontroller ist Voraussetzung**

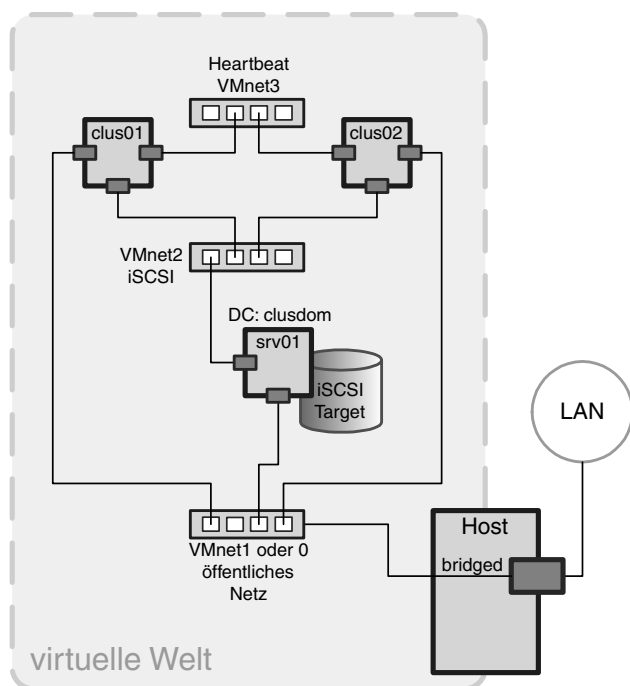


Abbildung 8.3:  
Der Aufbau des Clusters mit Domänencontroller und iSCSI-Target erfolgt vorerst nur auf einem Host als Testumgebung

**iSCSI-Target** Zusätzlich werden wir ein iSCSI-Target einrichten, das als gemeinsamer Speicher (*Shared Storage*) des Clusters dient. Als iSCSI-Target kommt eine Testversion der Software Starwind zum Einsatz, die in der VM mit dem Domänencontroller (*Srv01*) installiert wird. Die Installation auf einem Domänencontroller ist nicht ganz sauber, aber wir sparen uns in der Testumgebung zusätzliche Maschinen. Sie können das Target auch auf einer vierten VM oder auf einem physischen Rechner einrichten bzw. ein vorhandenes physisches Target verwenden, wenn Sie über ein solches verfügen. Die Testversion von Starwind können Sie über die Herstellerwebseite herunterladen:  
[www.rocketdivision.com/download\\_starwind.html](http://www.rocketdivision.com/download_starwind.html)

Als Alternative für das Software-Target kommen noch andere Programme in Frage, Sie finden weitere Alternativen, auch für Linux, in *Teil 1, Kapitel 1, „Grundlagen virtueller Maschinen und Hinweise zur Hardware“*.

**iSCSI Initiator** Als iSCSI Initiator in den beiden Cluster-Knoten dient der Microsoft iSCSI Software Initiator ab Version 2.01. Nur über solch einen Software-Initiator ist aus den VMs aller Produkte heraus der Zugriff auf externe Datenspeicher möglich. Die Einstiegsseite zum Download des Microsoft iSCSI Software Initiators und Informationen zu iSCSI finden Sie hier:  
[www.microsoft.com/windowsserver2003/technologies/storage/iscsi/](http://www.microsoft.com/windowsserver2003/technologies/storage/iscsi/)

Im Microsoft Download Center steht weiterhin ein ausführlicher englischer Artikel zur Cluster-Konfiguration bereit. Suchen Sie einfach nach *confclus.doc* (auch Downloads für englischsprachige Versionen anzeigen!):

<http://www.microsoft.com/downloads/details.aspx?FamilyID=a5bbb021-0760-48f3-a53b-0351fc3337a1&DisplayLang=en>



Für eine einfache Testumgebung, nur auf einem einzigen Host, können Sie auf iSCSI auch verzichten. VMware Server und auch Microsoft Virtual Server können virtuelle SCSI-Platten als gemeinsamen Datenträger verwenden, aber nur auf dem gleichen Host. Lesen Sie dazu die Vorgehensweise in *Abschnitt 8.4.1, „Cluster mit einer gemeinsamen virtuellen SCSI-Festplatte anstelle von externem Speicher“*.

### 8.2.2 Die einzelnen Ausbaustufen des virtuellen Clusters und das Vorgehen zur Realisierung

Wie schon bei der virtuellen DMZ in *Teil 2, Kapitel 3, „Virtuelle DMZ mit Firewall und Webserver im Internet“*, werden wir uns wieder stufenweise dem etwas komplexeren Thema nähern. Die ersten Punkte sind reines Handling virtueller Maschinen. Sie sehen noch einmal sehr schön das Zusammenwirken aller grundlegenden Funktionen. In den Stufen 4 und 5 gehen wir dann ausführlich den Aufbau des Clusters an.

- ▶ *Stufe 1* – Sie erstellen drei unabhängige VMs mit einer sauberen Installation von Windows Server 2003 R2 Enterprise Edition. Dazu wird in einer Basis-VM das System installiert, gepatcht und vorbereitet. Aus dieser Basis-VM erstellen Sie dann, mittels Differenzplatten (Microsoft), linked Clones (VMware) oder durch komplette Kopien, drei geklonte virtuelle Maschinen.
- ▶ *Stufe 2* – Sie bauen aus den VMs eine Infrastruktur, indem Sie alle Gäste in einem virtuellen Testnetzwerk vernetzen (*öffentliches Cluster-Netzwerk*). Sie installieren auf einem der Gäste einen Domänencontroller und nehmen die beiden anderen Gäste als Mitglied in diese Domäne auf.
- ▶ *Stufe 3* – Sie erweitern die Infrastruktur um ein iSCSI-Target, das als Software zusätzlich auf dem Domänencontroller installiert wird. Dazu fügen Sie ein zweites Netzwerk (*Speichernetzwerk*) hinzu, über das die Kommunikation mit dem Target läuft. In den beiden Cluster-Knoten-VMs installieren Sie die iSCSI Software-Initiatoren und testen dann den Zugriff auf den externen Speicher.
- ▶ *Stufe 4* – Jetzt kommen die Cluster-Dienste ins Spiel. Auf beiden Knoten richten Sie ein drittes Netzwerk für die Heartbeat-Kommunikation ein (*privates Netzwerk*). Der Zugriff auf den Quorumdatenträger wird vorbereitet, und die Cluster-Dienste werden installiert. Sie testen den ersten Failover.
- ▶ *Stufe 5* – Im Cluster richten Sie als Ressource eine Dateifreigabe ein. Von einem Testclient (virtueller PC oder physischer LAN-Client) greifen Sie darauf zu. Dann testen Sie die Failover-Funktion und das Verhalten des Clients.
- ▶ *Stufe 6* – Sie verfügen bereits über eine voll funktionsfähige Testumgebung auf einem einzigen Host. Zum Abschluss verteilen Sie die virtuellen Cluster-Knoten auf verschiedene physische Hosts und erreichen damit echte Hochverfügbarkeit. Das zeigt noch einmal in vollem Umfang die Flexibilität virtueller Maschinen.

## 8.3 Realisierung der einzelnen Ausbaustufen des virtuellen Clusters

Das Konzept steht, wir können beginnen. Die ersten beiden Punkte zum Erstellen der VMs werde ich nicht bis in die Tiefe beschreiben. Sie finden Hinweise zur Bedienung der Produkte in *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“* und in den Praxis-Workshops von *Teil 2* des Buches.



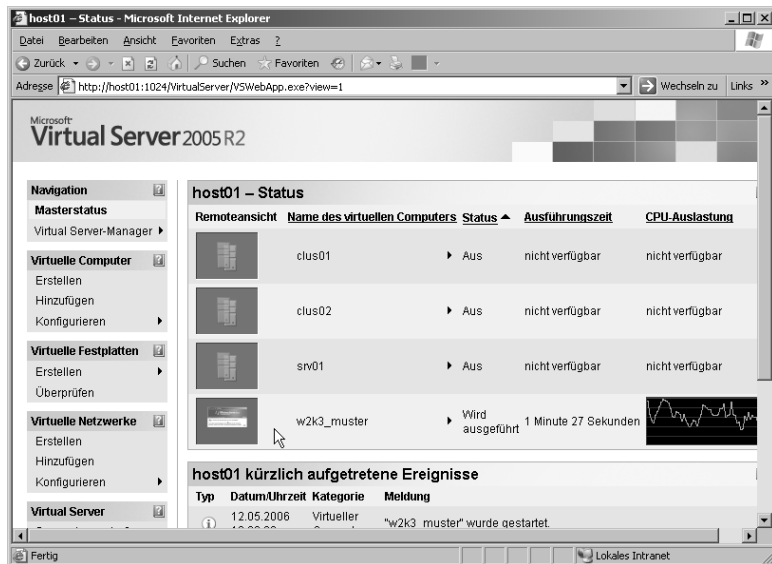
### 8.3.1 Stufe 1 – Installation von Windows 2003 und Klonen unabhängiger VMs

Erstellen Sie unter dem VMware Server, der Workstation oder Microsoft Virtual Server eine neue VM mit dem Namen *w2k3\_muster*. Korrekterweise müsste die VM eigentlich *w2k3\_r2e\_muster* heißen (für Windows 2003 R2 Enterprise), aber im Workshop ist der kürzere Name einfach handlicher. Die virtuelle Maschine sollte im Verzeichnis *\vmaschinen\vm\_muster\w2k3\_muster* liegen. Die VM muss über eine virtuelle Zuwachsplatte von mindestens 5 GB Größe für das Betriebssystem verfügen.

Abbildung 8.4:  
Drei virtuelle  
Maschinen mit  
Windows Server  
2003 bilden die  
Infrastruktur für den  
virtuellen Cluster



Abbildung 8.5:  
Die drei VMs für den  
Cluster können unter  
VMware Server oder  
MS Virtual Server  
laufen



Folgen Sie beim Erstellen einfach den Vorgaben der Produkte. Verwenden Sie bei VMware TYPICAL, und entfernen Sie beim VMware Server bei der Plattenerstellung den Haken an ALLOCATE ALL DISKSPACE NOW, um Zeit und Platz zu sparen. Ändern Sie vorerst noch nichts an der Hardware, fügen Sie auch noch keine weiteren Netzwerkkarten hinzu als die automatisch zugewiesene. Wir bauen die Hardware später im Workshop Schritt für Schritt aus.

In dieser neu erstellten Muster-VM installieren Sie den Windows Server 2003 R2 Enterprise Edition – entweder von der CD oder direkt von einem ISO-Image. Nach der Installation schließen Sie die Konfiguration des Gastsystems mit den üblichen Schritten zur Erstellung einer Muster-VM ab, z.B. VMware Tools oder Virtual Machine Additions sowie Patches installieren, defragmentieren und eventuell SYSPREP, siehe Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“.

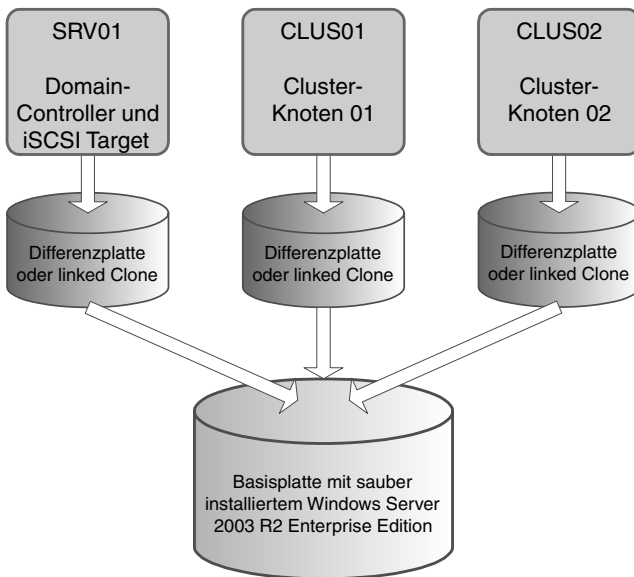


Abbildung 8.6:  
Alle Maschinen  
der Testumgebung  
können platz- und  
zeitsparend auf die-  
selbe Basisinstalla-  
tion zugreifen

Sind Sie mit Ihrem Gastsystem zufrieden, dann können Sie es vervielfältigen. Sie benötigen drei unabhängige VMs mit den Namen *Clus01*, *Clus02* und *Srv01* (Tabelle 8.1 und Abbildung 8.3). Dazu können Sie drei Kopien des kompletten Verzeichnisses der eben installierten Muster-VM *w2k3\_muster* machen oder nur die virtuelle Platte dreimal kopieren und in neue VMs einbinden. Am besten für eine Testumgebung sind allerdings die speziellen Methoden, welche die jeweiligen Virtualisierer bieten, um platz- und zeitsparend zu klonen (Abbildung 8.6):

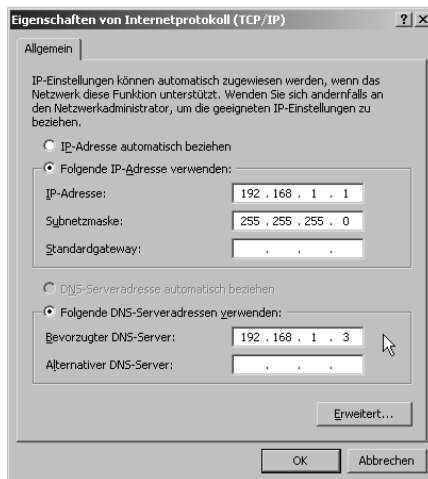
- Unter VMware Workstation schalten Sie den *Template-Modus* in der Muster-VM ein und erstellen drei *Linked Clones* von Ihrer VM (siehe Teil 3, Kapitel 4, „Die Snapshot- und Clone-Funktion der VMware Produkte“).

- ▶ Unter Microsoft Virtual Server erstellen Sie drei neue VMs ohne virtuelle Festplatte. Dazu setzen Sie beim Erstellen den Punkt an VIRTUELLE FESTPLATTE SPÄTER ZUORDNEN (KEINE). Danach erstellen Sie in den Verzeichnissen dieser VMs jeweils eine Differenzplatte, die auf die Platte der Muster-VM *w2k3\_muster* zeigt. Diese Differenzplatten binden Sie in die neuen VMs ein. Versehen Sie die zugrunde liegende Platte aus *w2k3\_muster* zur Vorsicht mit dem Attribut *Schreibgeschützt* (siehe Teil 2, Kapitel 7, „Eine virtuelle Pilotumgebung als Testfeld für produktive Einsätze“).
- ▶ Unter VMware Server wird es etwas komplizierter. Entweder Sie verwenden den Trick mit den multiplen Redo-Logs aus dem Teil 3, Kapitel 4, um drei linked Clones zu erstellen. Oder Sie kopieren am einfachsten dreimal die vollständige virtuelle Festplatte von *w2k3\_muster* und binden diese Kopien jeweils in neu erstellte VMs ein.



Wenn Sie auch die Ausbaustufe 6 nachvollziehen wollen (VMs auf mehreren Hosts), dann sollten Sie für alle VMs die Festplatten komplett kopieren, damit Sie die VMs ohne Probleme auf andere physische Hosts transportieren können. Ansonsten dürfen Sie später nicht vergessen, auch die zugrunde liegende Festplatte, bzw. bei der VMware Workstation das Template, mitzukopieren.

Abbildung 8.7:  
Der erste virtuelle  
Adapter in jedem  
Gast bildet das  
öffentliche Netz-  
werk an VMnet1



Haben Sie in der Muster-VM kein Sysprep durchgeführt, dann sollten Sie das Tool NEWSID in jedem Klon laufen lassen (siehe Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“). In den Gastsystemen der Klone müssen Sie den Rechnernamen ändern und eine eindeutige IP-Adresse für den ersten virtuellen Adapter festlegen, der beim Erstellen automatisch hinzugefügt wurde (siehe Tabelle 8.1). Als DNS-Server legen Sie dabei gleich die Adresse 192.168.1.3 fest (Abbildung 8.7). Diese IP-Adresse hat später der Domänencontroller, der auch den notwendigen DNS-Dienst in der Testdomäne übernimmt.

|                                            | Clus01<br>(Knoten 1) | Clus02<br>(Knoten 2) | Srv01 (DC und<br>iSCSI-Target) |
|--------------------------------------------|----------------------|----------------------|--------------------------------|
| Adapter01,<br>öffentlich (LAN)<br>VMnet1   | 192.168.1.1          | 192.168.1.2          | 192.168.1.3                    |
| Adapter02,<br>Speichernetz<br>VMnet2       | 192.168.2.1          | 192.168.2.2          | 192.168.2.3                    |
| Adapter03,<br>privat (Heartbeat)<br>VMnet3 | 192.168.3.1          | 192.168.3.2          | nicht verwendet                |

Tabelle 8.1:  
Die Netzwerkadapter in den virtuellen Maschinen mit den zugehörigen Adressen. Das Subnet lautet immer 255.255.255.0

8.3.2      Stufe 2 – Aufbau einer Infrastruktur mit virtuellem Netzwerk und Domänencontroller

Nach dem Klonen verbinden Sie den derzeit noch einzigen virtuellen Adapter aller drei VMs mit einem internen virtuellen Netzwerk. Dieses Netzwerk wird zum öffentlichen Netzwerk der Cluster-Umgebung. Sie könnten die VMs auch direkt mit Ihrem physischen LAN verbinden (*Bridged* oder *externes Netz*). Im Workshop gehe ich aber davon aus, dass wir die gesamte Umgebung als Testnetz aufbauen. Detaillierte Informationen zu den virtuellen Netzwerken finden Sie im ausführlichen Workshop von Teil 3, Kapitel 2, „*Virtuelle Netzwerke Teil 2 – die ganze Wahrheit*“.

Das öffentliche Netzwerk des Clusters

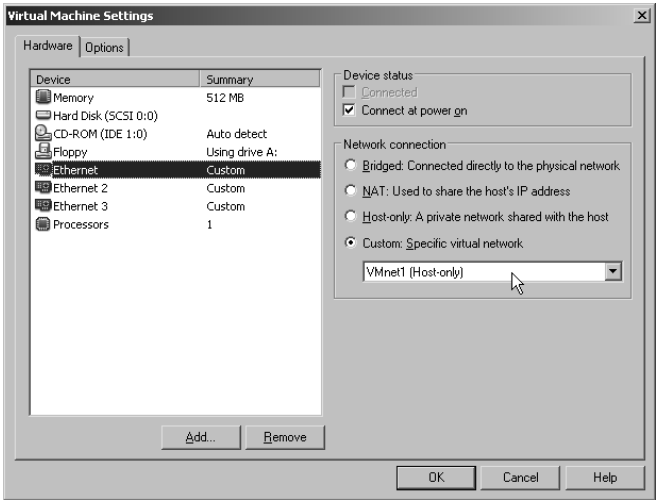


Abbildung 8.8:  
Der erste Adapter gehört zum öffentlichen Netz des Clusters und wird mit VMnet1 verbunden, weitere Adapter folgen später

Unter VMware verwenden Sie *VMnet1* (Abbildung 8.8), dadurch könnte der Host über das Host-only-Netzwerk ebenfalls auf den Cluster zugreifen. Ich wähle VMnet1 aber hauptsächlich deswegen, weil die Nummerierung dann gleich zur Nummer des Adapters und zum

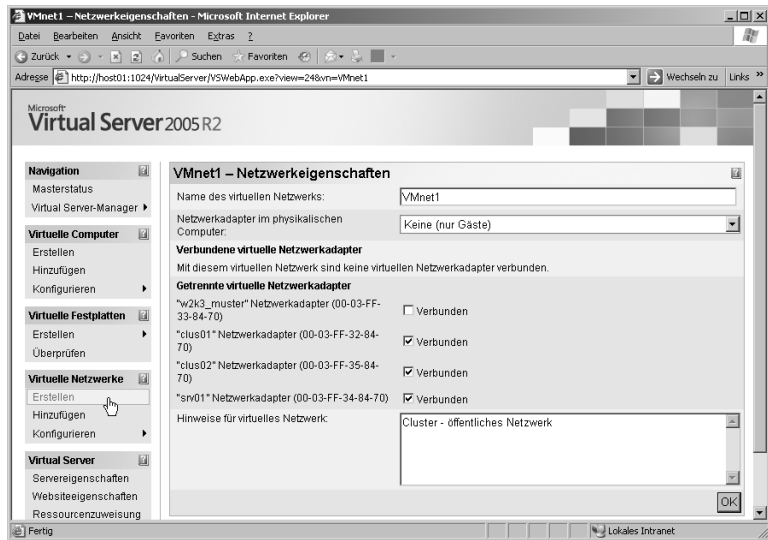
Netzwerk mit VMware

IP-Netzwerk passt (Tabelle 8.1). Sie können auch VMnet0 (Bridged-Netzwerk) benutzen, dadurch stehen das öffentliche Netzwerk und die Ressourcen des Clusters auch in Ihrem LAN zur Verfügung.

### Netzwerk mit Microsoft

Unter Microsoft Virtual Server legen Sie über VIRTUELLE NETZWERKE/ERSTELLEN eine neues internes Netzwerk mit dem Namen *VMnet1* an (Abbildung 8.9). Ich muss Sie dadurch im Verlauf des Workshops nicht ständig mit einer Doppelnennung beider Virtualisierungswelten verwirren, VMnet1 gilt für VMware und Microsoft gleichermaßen. Wenn Ihnen die Bezeichnung nicht zusagt, dann können Sie selbstverständlich einen anderen Namen für dieses interne Netzwerk wählen.

Abbildung 8.9:  
Unter MS Virtual  
Server sollten Sie  
ebenfalls ein inter-  
nes Netz mit dem  
Namen VMnet1  
erstellen



Da Sie in den Gästen die richtigen IP-Adressen bereits in Schritt 1 zugewiesen haben, können Sie den gesamten Aufbau mit ein paar Ping-Befehlen in alle Richtungen testen. Jede VM sollte mit den anderen beiden im internen virtuellen Netzwerk kommunizieren können.



Schalten Sie zum Testen Firewalls in den Gastsystemen ab.

### Den Domänencontroller in der VM Srv01 aufsetzen

Es ist an der Zeit, in der VM *Srv01* einen neuen Domänencontroller mit einer neuen Active Directory-Struktur aufzusetzen. Wenn Sie wollen, können Sie später beide Cluster-Knoten auch in eine schon vorhandene Domäne in Ihrem LAN aufnehmen, dann können Sie sich den virtuellen Domänencontroller sparen.

Im Workshop gehe ich davon aus, dass Sie für die Testumgebung einen eigenen virtuellen Domänencontroller betreiben. Starten Sie das Kommando *dcpromo* von der Kommandozeile, und folgen Sie den Anweisungen des *Assistenten zum Installieren von Active Directory*. Beantworten Sie die Dialoge mit den vorgegebenen Antworten:

- ▶ Domänencontroller für eine neue Domäne
- ▶ Domäne in einer neuen Gesamtstruktur
- ▶ Vollständiger Name für die Domäne: *clusdom.virtual*
- ▶ NetBIOS-Domänenname: *CLUSDOM*
- ▶ Der DNS-Test bringt einen Fehler, da noch kein DNS-Server in unserer virtuellen Infrastruktur existiert, worauf der Assistent auf dem Server automatische einen DNS-Server einrichtet (Abbildung 8.10).
- ▶ Wählen Sie **NUR MIT WINDOWS 2000/2003 KOMPATIBLE BERECHTIGUNGEN**.
- ▶ Legen Sie ein Kennwort für den Wiederherstellungsmodus fest.

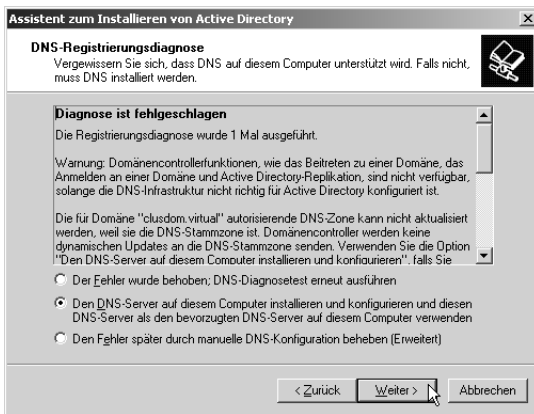


Abbildung 8.10:  
Der Assistent für die  
ADS-Installation  
richtet auf *Srv01*  
gleich den DNS-  
Server ein

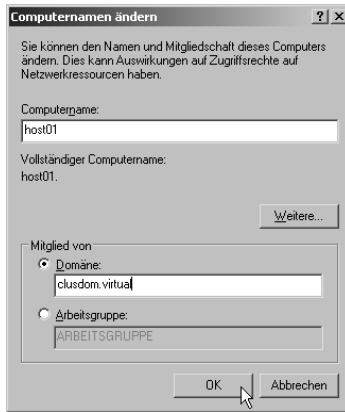
Die Einrichtung des Active Directorys dauert ein Weilchen. Sie benötigen dazu die Windows Server-CD – praktisch, wenn Sie diese gleich als ISO-Image abgelegt haben. Nach der Installation des Domänencontrollers und einem Neustart des Gastes können Sie die beiden VMs *Clus01* und *Clus02* über **NETZWERKVERBINDUNGEN/ERWEITERT/NETZWERKIDENTIFIKATION** in die neue Domäne *clusdom.virtual* aufnehmen (Abbildung 8.11). Beachten Sie dabei, dass der DNS-Eintrag in der IP-Konfiguration der beiden Server vor dem Aufnehmen bereits auf die Adresse *192.168.1.3 (Srv01)* zeigt (Abbildung 8.7), sonst funktioniert das Aufnehmen in die ADS-Domäne nicht.

**Knoten als Mitgliedsserver aufnehmen**

Achten Sie darauf, sich nach dem Neustart auch wirklich in der Domäne und nicht mehr lokal anzumelden (Abbildung 8.12).



Abbildung 8.11:  
Die beiden Cluster-  
Knoten müssen  
Mitglied einer  
Domäne sein, bevor  
die Cluster-Dienste  
eingrichtet werden  
können



### Zwischenstand sichern mit Snapshot

Nach allen notwendigen Neustarts können Sie die vorbereitete Umgebung mit Snapshots (VMware) oder mit einer weiteren Differenzplatte (MS Virtual Server) in jeder VM sichern. Geht später irgendetwas schief, müssen Sie nicht jedes Mal wieder von vorn beginnen, die Einrichtung des Domänencontrollers ist etwas langwierig.

Abbildung 8.12:  
Die beiden Cluster-  
Knoten müssen  
Mitglied in einer  
Domäne sein



### 8.3.3 Stufe 3 – Installation des iSCSI-Targets und Einrichten des Zugriffes

In allen drei VMs können Sie jetzt den zweiten virtuellen Netzwerkadapter hinzufügen. Sie verbinden ihn unter VMware mit *VMnet2*. Unter Virtual Server legen Sie ein weiteres internes Netzwerk mit dem Namen *VMnet2* an. *VMnet2* wird unser Speichernetzwerk, in dem der Datentransfer über iSCSI abläuft. Vergeben Sie die in der Tabelle 8.1 ersichtliche IP-Adresse, und testen Sie die Funktionalität mit ein paar Ping-Befehlen. Entfernen Sie an diesen beiden neuen Adaptern in den Gästen sämtliche Bindungen bis auf TCP/IP (Abbildung 8.13). Die Adapter werden nicht zur Kommunikation im Windows-Netzwerk verwendet, sondern dienen später ausschließlich dem iSCSI Initiator zur Kommunikation mit dem Target.

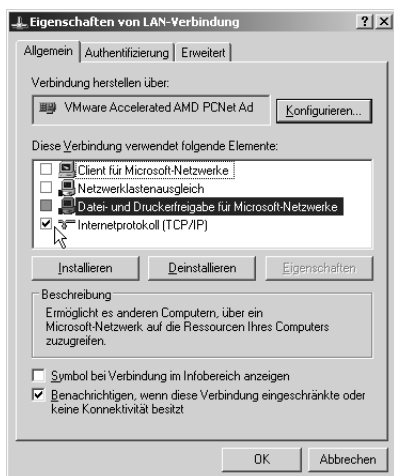


Abbildung 8.13:  
Alle unnötigen  
Bindungen an den  
virtuellen Adaptern  
in den Gästen soll-  
ten entfernt werden

Für die VM Srv01 erstellen wir jetzt noch eine zusätzliche virtuelle Platte. Auf diesem Datenträger werden später die Daten liegen, die das iSCSI-Target bereitstellt. Ich habe ja im Buch bereits mehrfach propagiert, System und Daten einer VM immer sauber zu trennen. In einer einfachen Testumgebung ist das nicht unbedingt nötig. Aber bereits beim Zurücksetzen Ihrer VM mittels REVERT (VMware) oder durch Löschen einer Differenzplatte (Microsoft) ist es praktisch, eine separate Platte zu haben, auf der die Daten liegen. So können Sie das System bei Fehlern zurücksetzen und die Daten erhalten. Unter VMware sollten Sie diese Platte über ADVANCED in den Modus *persistent* bringen, was aber nur funktioniert, wenn kein Snapshot vorhanden ist (siehe Teil 3, Kapitel 4, „Die Snapshot- und Clone-Funktion der VMware-Produkte“).

**Virtuelle Platte  
für das Target**

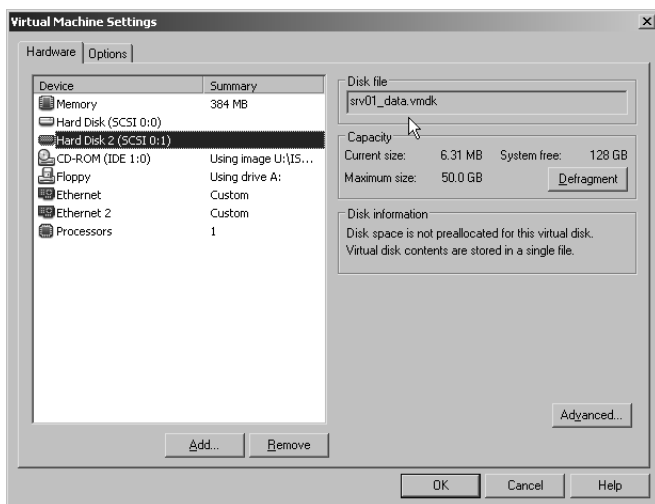
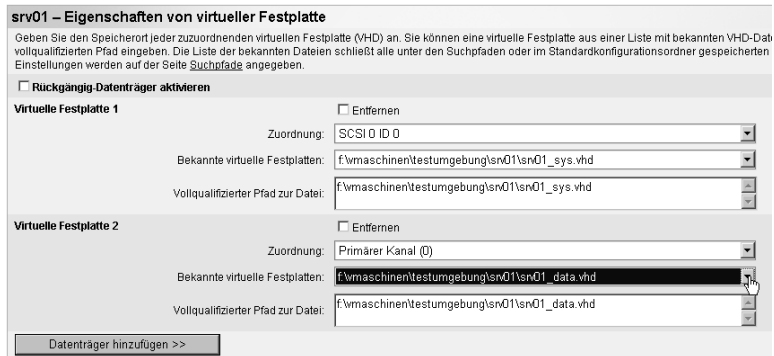


Abbildung 8.14:  
Eine zweite virtu-  
elle Platte in der  
VM Srv01 dient als  
Ablage für die Daten  
des iSCSI-Targets



Erstellen Sie im Verzeichnis `vmachines\testumgebung\srv01` Ihrer VM `Srv01` eine neue Platte für die Daten mit dem Namen `srv01_data.vmdk` (für VMware Abbildung 8.14) bzw. `srv01_data.vhd` (für Microsoft Abbildung 8.15). Nach dem Start der VM müssen Sie im Gast in der Datenträgerverwaltung auf dieser Platte noch eine NTFS-Partition erstellen und formatieren.

Abbildung 8.15:  
Unter Virtual  
Server sollten Sie  
ebenfalls eine sepa-  
rate virtuelle Daten-  
platte anlegen und  
in die VM `Srv01`  
einbinden



### Einrichtung der iSCSI-Targets in der virtuellen Maschine Srv01

#### Speicher für Quorum und Daten

Jetzt können Sie das Software-Target im Server `Srv01` installieren und einen Datenspeicher konfigurieren. Wenn Sie bereits ein SAN mit iSCSI-Schnittstelle besitzen, dann können Sie auch dieses für den Cluster benutzen. Wie bereits erwähnt, verwenden wir eine Evaluierungsversion der Software Starwind, um eine Testlösung für den Workshop zu haben. Der Cluster benötigt zwei Speicher, einen für das Quorum und einen für die Daten. Gehen Sie zur Einrichtung folgendermaßen vor:

1. Starten Sie das Setup von Starwind, und folgen Sie den Vorgaben, wählen Sie eine FULL INSTALLATION.
2. Nach der Installation startet Starwind automatisch. Es existieren auch Einträge im Startmenü unter PROGRAMME/ROCKET DIVISION SOFTWARE, worüber Sie Starwind manuell starten können.
3. Sobald Starwind läuft, erscheint unten rechts in der Taskleiste ein kleines Symbol. Mit der rechten Maustaste öffnet sich ein Menü, worüber Sie mit START MANAGEMENT die Konfiguration aufrufen können.
4. Wir verwenden die schon vorhandene Verbindung `localhost:3260`. Sie können sich dort mit der rechten Maustaste über CONNECT anmelden (Abbildung 8.16). Der Nutzer der Trialversion ist `test` mit dem Passwort `test`.

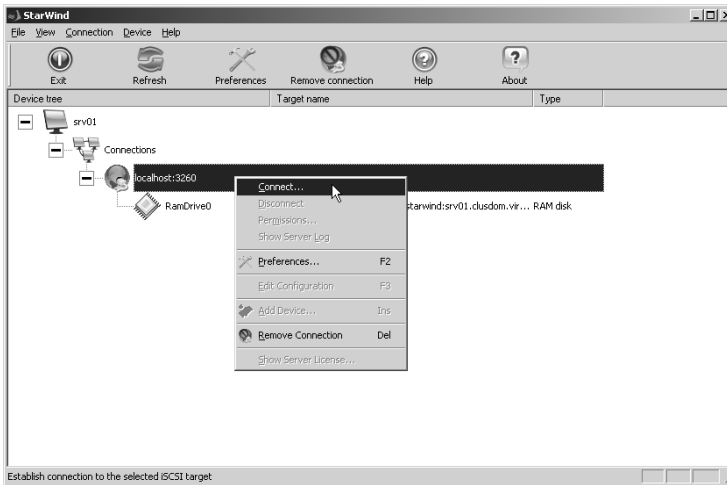


Abbildung 8.16:  
Nach der Installation  
können Sie sich an  
einer Verbindung  
anmelden und neue  
Targets erstellen

5. Es existiert bereits ein *RamDrive0* als Target, wir legen aber zwei neue Targets an, die wir auf der virtuellen Datenfestplatte von *Srv01* ablegen. Das Anlegen funktioniert mit der rechten Maustaste auf die Verbindung und dem Menüpunkt **ADD DEVICE**.
6. Wählen Sie ein **IMAGE FILE DEVICE**.

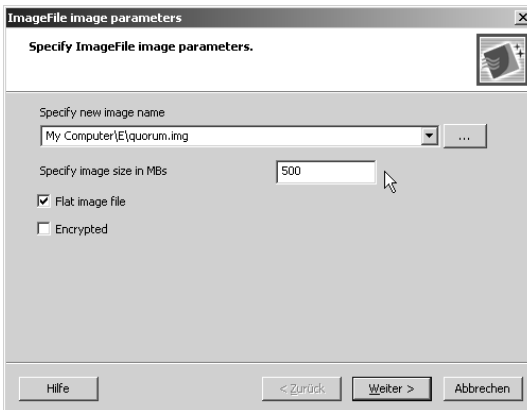
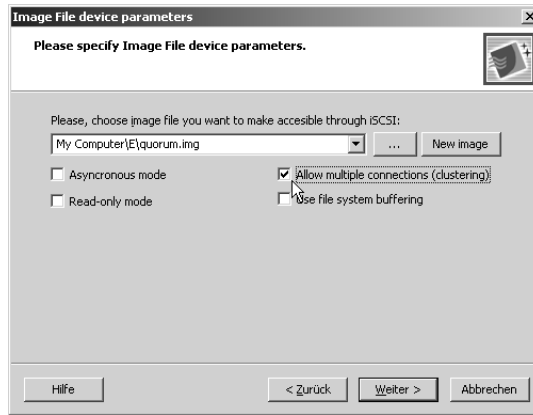


Abbildung 8.17:  
Die Daten der  
Targets liegen in  
Image-Dateien

7. Über den Button **NEW IMAGE** müssen Sie erst ein neues Image erstellen, in dem Starwind die Daten des Targets ablegt (Abbildung 8.17). Dabei wählen Sie als Zielverzeichnis *My Computer\E*, wobei *E* der Laufwerksbuchstabe Ihrer zweiten virtuellen Festplatte ist, die Sie extra als Datenplatte in die VM eingebaut haben. Die erste Image-Datei können Sie *quorum.img* nennen. Achten Sie auf die Endung *\*.img*, ohne diese kann Starwind das Imagefile nicht erstellen. Für das Quorum-Image genügt eine Größe von 500 MB.

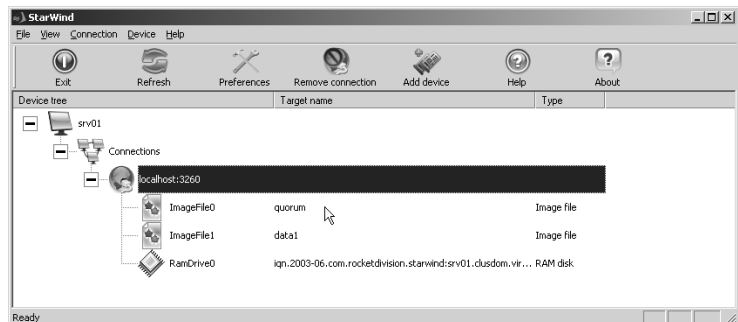
8. Jetzt können Sie das erzeugte Image als Datenspeicher für ein Target verwenden. Setzen Sie dabei den Haken an ALLOW MULTIPLE CONNECTIONS (CLUSTERING) (Abbildung 8.18), damit später mehrere Server auf dieses Target zugreifen können.

Abbildung 8.18:  
Ein neues Target  
muss für die Verwen-  
dung in einem Clus-  
ter mehrere Verbin-  
dungen erlauben



9. Wählen Sie im nächsten erscheinenden Fenster als Namen für das neu erstellte Target ebenfalls *quorum*.
10. Nach dem Fertigstellen steht das neue Target in der Liste unter der Verbindung bereit (Abbildung 8.19).
11. Wiederholen Sie den Vorgang, und erstellen Sie ein weiteres Target mit dem Namen *data1*. Achten Sie darauf, in den Namen keine Sonderzeichen zu verwenden, sonst scheitert später die Verbindung mit dem Initiator! Erstellen Sie für das Target *data1* ein gleichnamiges Image mit der Größe vom 10000 MB, und setzen Sie ebenfalls den Haken bei ALLOW MULTIPLE CONNECTIONS (CLUSTERING).
12. Das Target *RamDrive0* können Sie mittels REMOVE entfernen, wir benötigen es nicht.

Abbildung 8.19:  
Zwei Targets dienen  
später als Quorum-  
datenträger und als  
Datenspeicher für  
den Cluster



Sie haben jetzt zwei Targets erstellt (Abbildung 8.19). Wie die Namen bereits aussagen, wird das eine als Quorumdatenträger für unseren Cluster dienen, das andere wird als Cluster-Ressource Daten für die Anwender bereitstellen.

Wenn Sie in der VM Srv01 einmal auf die virtuelle Festplatte schauen, die Sie als Ablageort für die Targets verwendet haben, dann sehen Sie dort zwei Image-Dateien, *quorum.img* und *data1.img*. In diesen Image-Dateien liegen später die Daten der Targets. Das ist bei genauerer Betrachtung fast schon etwas kurios, weil mittels Speichervirtualisierung über das iSCSI-Target Daten in Image-Dateien abgespeichert werden, die wiederum auch nur in einer virtuellen Festplatte liegen, sozusagen Virtualisierung in der Virtualisierung. Für eine Produktivumgebung macht das natürlich kaum Sinn, aber zum Nachvollziehen unseres Workshop ist diese Lösung äußerst praktisch.

**Virtuell in virtuell**

### Einrichten des Zugriffes auf das Target mittels Microsoft Initiator in dem ersten Cluster-Knoten Clus01

Von den beiden Servern *Clus01* und *Clus02* können Sie nun eine Verbindung mit den Targets auf Srv01 herstellen. Dazu installieren Sie in beiden Gastsystemen den Microsoft iSCSI Initiator zum Zugriff auf den externen Speicher. Gehen Sie folgendermaßen vor:

**iSCSI Initiator einrichten**

1. Starten Sie das Setup des Microsoft iSCSI Initiators. Folgen Sie einfach den Vorgaben.
2. Nach der Installation gelangen Sie im Startmenü unter PROGRAMME/MICROSOFT iSCSI INITIATOR zur Konfiguration (Abbildung 8.20).

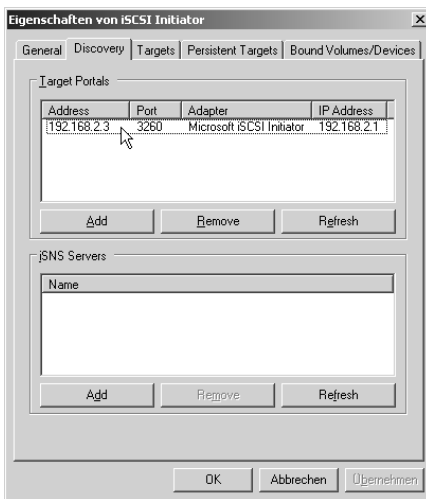
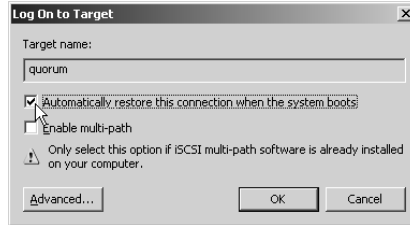


Abbildung 8.20:  
Als Portal sollte die IP-Adresse des Speichernetzes von Srv01 eingetragen werden

3. In der Konfiguration des Initiators können Sie im Reiter DISCOVERY ein Target-Portal festlegen, über das Sie dann alle verfügbaren Targets erreichen. In unserem Falle ist das Portal 192.168.2.3 (Srv01) auf dem Port 3260 (Abbildung 8.20). Da Sie extra als Speichernetzwerk separate Netzwerkkarten in jede VM eingebaut haben, sollten Sie die Adresse 192.168.2.3 explizit angeben, damit der Verkehr nicht über eines der anderen Netze abgewickelt wird.

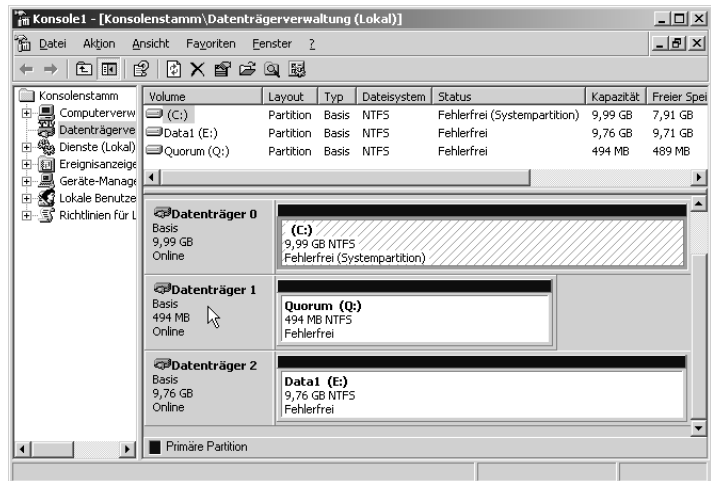
- Über den Reiter TARGETS können Sie jetzt bereits beide freigegebenen Targets von Srv01 sehen. Sie können sich mit dem Button LOGON verbinden. Dabei müssen Sie den Haken an AUTOMATICALLY RESTORE THIS CONNECTION setzen, damit bei jedem Neustart des Systems die Verbindung automatisch wiederhergestellt wird (Abbildung 8.21). Unter dem Reiter PERSISTENT TARGETS müssten jetzt beide Verbindungen zu sehen sein.

Abbildung 8.21:  
Die beiden Targets  
sollten beim Neu-  
start der Knoten  
automatisch ver-  
bunden werden



- In der Datenträgerverwaltung von Windows sind jetzt beide verbundene Targets als lokale Laufwerke sichtbar. Auf beiden Laufwerken können Sie eine NTFS-Partition erstellen, diese formatieren und einen Laufwerksbuchstaben zuordnen. Dem Quorumdaten-träger sollten Sie gleich den Laufwerksbuchstaben Q: zuordnen (Abbildung 8.22). Achten Sie darauf, dass die Laufwerke Basis-datenträger sind! Sollten es dynamische Datenträger sein, können Sie diese über die rechte Maustaste zurückkonvertieren.

Abbildung 8.22:  
Beide eingebundene  
Targets werden von  
den Servern verwen-  
det wie lokale Fest-  
platten



- Jetzt wechseln Sie nochmals zum Microsoft iSCSI Initiator, und unter dem Reiter BOUND VOLUMES fügen Sie beide Laufwerksbuchstaben, die Sie gerade erstellt haben, hinzu. Dadurch wartet Windows beim Systemstart erst ab, bis beide Laufwerke zur Verfügung stehen (Abbildung 8.23).

7. Sie können jetzt im Windows-Explorer auf beide Laufwerke zugreifen und dort testweise einen Ordner oder eine Textdatei anlegen. Für Windows handelt es sich um eine lokale Festplatte, die Daten liegen aber in der Image-Datei von Starwind auf dem virtuellen Server Srv01. Sie gelangen über das iSCSI-Protokoll dorthin.

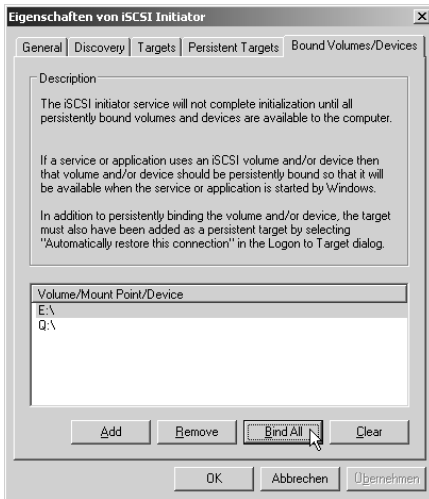


Abbildung 8.23:  
Der iSCSI Initiator  
sollte warten, bis  
beide Targets zur  
Verfügung stehen

### Einrichten des Zugriffes auf das Target im zweiten Cluster-Knoten Clus02

Wenn alles auf dem ersten Knoten funktioniert, fahren Sie die VM Clus01 herunter. Dann wiederholen Sie alle Schritte in der VM Clus02. Sobald Sie dort die beiden Targets (AUTOMATICALLY RESTORE nicht vergessen – Abbildung 8.21) angebunden haben, weisen Sie ihnen in der Datenträgerverwaltung die gleichen Laufwerksbuchstaben zu wie auf Clus01. Sie müssen keine neuen Partitionen anlegen und die Datenträger auch nicht formatieren, das haben Sie bereits von Server Clus01 aus getan. Wenn alles funktioniert, sollten Sie die Ordner oder die Textdateien sehen, die Sie vom Server Clus01 bereits testweise angelegt haben.

Die komplette Infrastruktur für den Cluster steht damit bereit. Sie verfügen über einen virtuellen Domänencontroller, eine Domäne *clusdom.virtual* und über externen Speicher für die Daten und den Quorumdatenträger mit iSCSI-Anbindung. Beide Cluster-Knoten sind Mitglied der Domäne und haben Zugriff auf den externen Speicher. Zurzeit existieren zwei Netzwerke: einmal das öffentliche Netzwerk für die Kommunikation in der Domäne und später optional auch mit dem LAN (VMnet1); weiterhin das Speichernetzwerk für den Datentransfer zwischen den iSCSI-Initiatoren und dem Target (VMnet2). Das Ganze ist völlig flexibel in virtuellen Maschinen installiert, transportabel und auf jedem anderen Rechner zu Demo-Zwecken jederzeit verwendbar.

**Die Infrastruktur  
ist fertig**



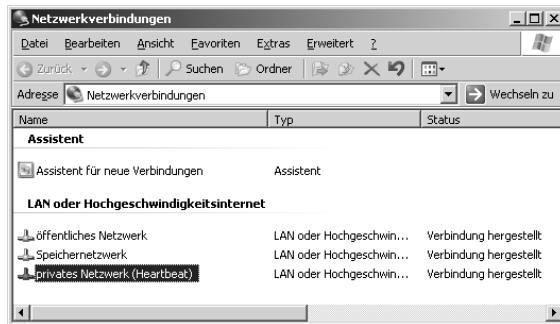
Sie können von diesem Stand in jeder VM wieder Snapshots setzen oder eine weitere Differenzplatte zuschalten oder die Umgebung als Muster komplett kopieren.

### 8.3.4 Stufe 4 – Installation und Test des Clusters auf einem einzigen Host

#### Die virtuelle Netzwerkkarte der Knoten

Es ist fast geschafft – die Infrastruktur steht! Sie können nun die Cluster-Dienste auf den beiden Knoten einrichten. Dazu müssen Sie beiden Servern *Clus01* und *Clus02* noch eine dritte Netzkarte für das private Cluster-Netzwerk (Heartbeat) zuweisen und ans interne Netzwerk *VMnet3* anbinden. Unter Microsoft Virtual Server sollten Sie dazu ein weiteres internes Netzwerk mit dem Namen *VMnet3* anlegen. Die VM *Srv01* benötigt diesen dritten Adapter nicht. Vom neuen dritten Adapter in den Gästen *Clus01* und *Clus02* entfernen Sie wieder alle Bindungen bis auf TCP/IP (Abbildung 8.13) und vergeben die IP-Adressen aus der Tabelle 8.1. für das Heartbeat-Netz (*VMnet3*). Vergessen Sie nicht ein Ping zum Testen der Verbindung. Zur besseren Übersicht sollten Sie die Netzwerkverbindungen in den Gästen entsprechend umbenennen (Abbildung 8.24).

Abbildung 8.24:  
Die Netzwerkverbindungen in allen Gästen sollten zur besseren Übersicht nach der Funktion benannt werden



#### Nutzer für die Cluster-Dienste anlegen

Es fehlt noch ein Nutzer für die Cluster-Dienste, Sie werden während der Cluster-Einrichtung danach gefragt. Erstellen Sie vorher einen Nutzer *clusman*, und setzen Sie das Kennwort auf KENNWORT LÄUFT NIE AB (Abbildung 8.25). Durch die beim Setup der Active Directory-Domäne automatisch eingestellten Kennwortrichtlinien muss das Kennwort mindestens sechs Zeichen lang sein und einige Ziffern, Kleinbuchstaben und zusätzlich Großbuchstaben oder Sonderzeichen enthalten. Mit einem Passwort, das nicht den Richtlinien entspricht, lässt sich der Nutzer nicht anlegen. Weiterhin ist es wichtig, dass der neue Benutzer Mitglied der Gruppe *Administratoren* ist.

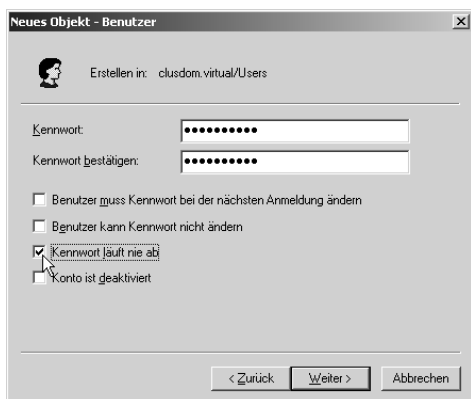


Abbildung 8.25:  
Für den Betrieb des Clusters sollte ein separater Nutzer mit Administratorrechten angelegt werden

## Konfiguration der Cluster-Dienste auf dem Knoten Clus01

Die Verwaltung des Clusters erfolgt über die Cluster-Verwaltung. Dort lässt sich auch ein neuer Cluster erstellen. Wir beginnen mit dem Knoten 1.

Der Cluster-Knoten 2 sollte während der Konfiguration ausgeschaltet sein.



1. Starten Sie über PROGRAMME/VERWALTUNG/CLUSTERVERWALTUNG die Cluster-Verwaltung, und wählen Sie NEUEN CLUSTER ERSTELLEN.
2. Wählen Sie die Domäne *clusdom.virtual*, und vergeben Sie als Namen für den Cluster *cluster01* (Abbildung 8.26).



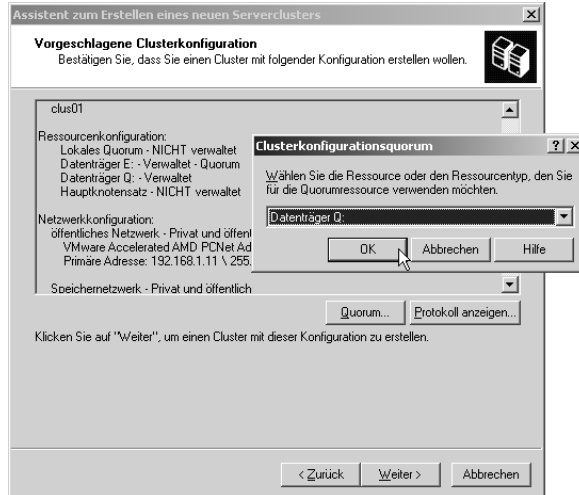
Abbildung 8.26:  
Beim Erstellen eine neuen Clusters werden die Domäne und der gewünschte Name des Clusters abgefragt

3. Als ersten Knoten des Clusters wählen Sie *clus01*. Anschließend erfolgt die automatische Überprüfung der verfügbaren Ressourcen auf Cluster-Tauglichkeit.



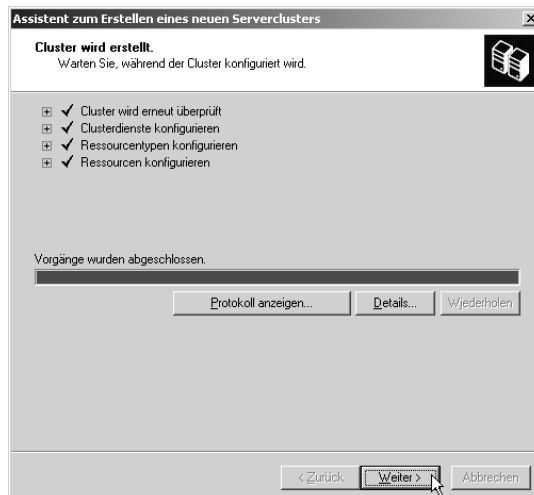
4. Geben Sie im nächsten Bildschirm eine freie IP-Adresse aus dem öffentlichen Netzwerk ein, unter welcher der Cluster erreichbar sein soll. In unserem Beispiel verwenden wir 192.168.1.5. Diese Adresse dient unter anderem der Verwaltung des Clusters.
5. Danach kommt der vorhin angelegte Benutzer zum Tragen. Sie können ihn als Konto für die Cluster-Dienste zuweisen.

Abbildung 8.27:  
Der Datenträger Q:  
muss als Quorum-  
datenträger verwendet  
werden, eventuell  
ist das zu korrigieren



6. Im abschließend erscheinenden Protokoll sollten Sie unbedingt überprüfen, ob der richtige Datenträger als Quorum ausgewählt wurde. Sie haben bereits zwei externe Datenspeicher mit dem iSCSI-Initiator zugewiesen, deshalb kann es passieren, dass jenes Target als Quorum verwendet wird, das eigentlich für die Daten zuständig ist. Wenn nicht Laufwerk Q: gewählt wurde, dann können Sie das mit der Schaltfläche QUORUM noch korrigieren (Abbildung 8.27).

Abbildung 8.28:  
Der Cluster ist  
fertig. Ein Protokoll  
zeigt das Ergebnis



7. Jetzt erfolgt die automatische Einrichtung der Cluster-Dienste. Beendet wird die Installation mit einem abschließenden Protokoll (Abbildung 8.28).
8. In der Cluster-Verwaltung erscheinen bereits die vorhandenen Ressourcen und CLUS01 als erster Knoten. Ich gehe weiter unten noch ausführlicher darauf ein (Abbildung 8.31). Vorerst räumen Sie unter CLUSTERKONFIGURATION/NETZWERKE noch etwas in den Netzwerken des Clusters auf. Mit der rechten Maustaste gelangen Sie zu den Eigenschaften der einzelnen Netzwerkeinträge. Setzen Sie das private Netzwerk auf NUR INTERNE CLUSTERKOMMUNIKATION (Abbildung 8.29). Alle anderen Netzwerke erhalten die Einstellung NUR CLIENTZUGRIFF.

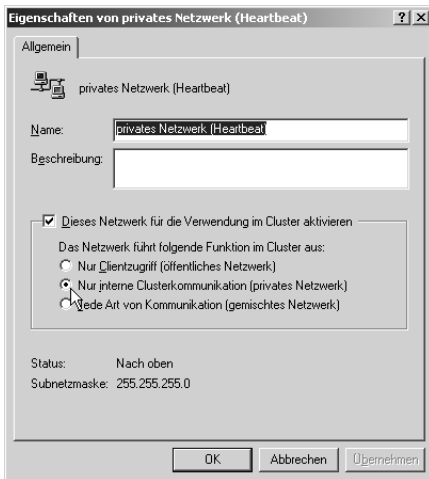


Abbildung 8.29:  
Nur ein Netzwerk  
wird explizit als  
privates Netzwerk  
(Heartbeat) reser-  
viert

## Konfiguration der Cluster-Dienste auf dem Knoten Clus02

Sie können jetzt den zweiten Knoten Clus02 wieder hochfahren. Clus01 können Sie eingeschaltet lassen, da die Cluster-Verwaltung bereits die gemeinsamen Datenträger kontrolliert. Auf Clus02 starten Sie die Cluster-Verwaltung über PROGRAMME/VERWALTUNG/CLUSTER-VERWALTUNG. Dort wählen Sie den Punkt VERBINDUNG MIT CLUSTER ÖFFNEN und geben den Namen *cluster01* an (Abbildung 8.30). In der Cluster-Verwaltung sehen Sie die bereits vorhandenen Ressourcen und den ersten Knoten CLUS01. Mit DATEI/NEU/KNOTEN können Sie jetzt den Knoten 2 (*clus02*) hinzufügen, dabei benötigen Sie das Kennwort des Benutzers *clusman*.

Wundern Sie sich nicht, dass Sie auf Clus02 die beiden Laufwerke Q: und E: des externen iSCSI-Speichers nicht sehen. Das liegt am Cluster-Dienst, der bereits die Kontrolle über diese Ressourcen übernommen hat. Clus02 kann erst wieder darauf zugreifen, wenn er durch ein Failover der Besitzer dieser Ressource geworden ist.



Abbildung 8.30:  
Bevor neue Knoten  
angelegt werden  
können, muss erst  
eine Verbindung  
zum Cluster herge-  
stellt werden

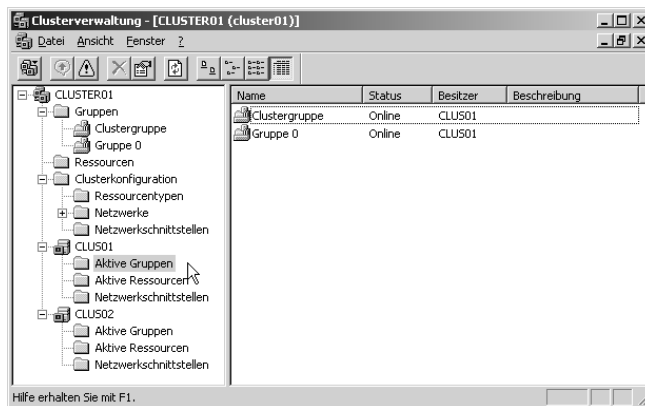


### Testen des fertig konfigurierten Clusters

Mit dem Erstellen des neuen Knotens Clus02 ist der Cluster fertig. Sie sehen in der Verwaltung beide Knoten CLUS01 und CLUS02 (Abbildung 8.31). Die Organisation der Ressourcen erfolgt über Gruppen. Eine Ressource (z.B. Laufwerk E:) gehört immer zu einer Gruppe, und eine Gruppe ist immer auf einem bestimmten Knoten aktiv.

Unter GRUPPEN erkennen Sie zwei Einträge. CLUSTERGRUPPE ist die Gruppe mit den Ressourcen der Cluster-Verwaltung, z.B. des Quorumdatenträgers. Diese Gruppe ist bei jedem Microsoft Cluster mindestens vorhanden. Die GRUPPE 0 enthält den externen Speicher, den wir für die Daten angelegt haben. Da wir diesen Speicher bereits vor der Cluster-Konfiguration mit dem iSCSI Initiator eingebunden hatten, wurden automatisch eine Ressource und eine Gruppe dafür erstellt. Normalerweise richtet man die Anwendungsressourcen erst später ein.

Abbildung 8.31:  
In der Cluster-  
Verwaltung lassen  
sich die Gruppen,  
Ressourcen und  
Knoten des Clusters  
überwachen und  
verwalten



**Das erste Failover** Wenn Sie sich die beiden Einträge AKTIVE GRUPPEN unter den beiden Knoten anschauen, dann sehen Sie, dass Knoten 1 alle Ressourcen hält, während sich Knoten 2 im Leerlauf befindet (Abbildung 8.31). Sie können jetzt mit der rechten Maustaste, z.B. auf die Gruppe 0, mittels GRUPPE VERSCHIEBEN Ihr erstes geplantes Failover mit dem neuen Cluster durchführen. Gruppe 0 erscheint kurz darauf unter AKTIVE GRUPPEN von Knoten 2.

Sie sehen den Erfolg auch daran, dass Sie im Windows Datei-Explorer von Server Clus02 plötzlich wieder auf Laufwerk E: zugreifen können, auf dem Server Clus01 dagegen nicht mehr. Gruppe 0, wozu als Ressource der externe Speicher im Target data1 (E:) gehört, wird jetzt von Clus02 verwaltet.

### 8.3.5 Stufe 5 – Einrichten einer Dateifreigabe und einer IP-Adresse als Cluster-Ressource

Unser Cluster funktioniert bereits, allerdings hat ein Anwender aus dem öffentlichen Netzwerk (später das LAN) noch nichts davon. Wir sollten erst noch einige Ressourcen konfigurieren, die im öffentlichen Netzwerk erscheinen. Das könnten Postfächer und öffentliche Ordner der Exchange-Dienste sein oder eine Datenbank wie SQL. Als einfaches Beispiel verwenden wir im Workshop eine simple Dateifreigabe, über die Anwender Zugriff auf die Daten des iSCSI-Targets *data1* haben sollen.

Dieses Target steht bereits als Laufwerk E: auf dem aktiven Knoten zur Verfügung. Sie könnten theoretisch das Laufwerk E: direkt an dem Server, auf dem es gerade bereitsteht (z.B. Clus02), im LAN freigeben. Allerdings ergibt damit der Cluster keinerlei Sinn. Wenn der Knoten ausfällt, dann ist auch die Freigabe nicht mehr zu erreichen. Sie wollen aber Ausfallsicherheit.

#### Mit einer logischen Dateifreigabe des Clusters verbinden sich Benutzer aus dem LAN

Wie schon ganz zu Beginn des Workshops erwähnt, muss die Verbindung aus dem LAN mit den Cluster-Ressourcen über virtuelle (logische) Adressen erfolgen. Um solche Adressen zu erstellen, erweitern Sie die vorhandene Gruppe 0 und fügen drei Ressourcen hinzu – eine virtuelle IP-Adresse, unter der die Ressource vom LAN aus erreichbar ist, einen Netzwerknamen zu dieser IP-Adresse und eine Dateifreigabe, mit der sich Nutzer verbinden können. Nur über diese logische Dateifreigabe sollte ein Anwender aus dem LAN auf das Laufwerk E: zugreifen. Fällt ein Knoten aus, dann wird diese Freigabe von einem anderen Knoten übernommen und weiterhin im LAN bereitgestellt.

Am bequemsten funktioniert das Konfigurieren der benötigten Ressourcen mit Klick der rechten Maustaste auf GRUPPE 0 und den Punkt ANWENDUNG KONFIGURIEREN. Folgen Sie dem Assistenten:

1. Wählen Sie NEUEN VIRTUELLEN SERVER ERSTELLEN.

**Einrichten weiterer Ressourcen**

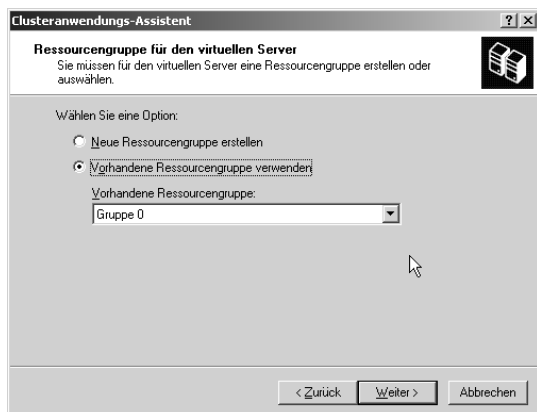


Abbildung 8.32:  
In der vorhandenen  
Gruppe 0 können  
weitere Ressourcen  
konfiguriert werden

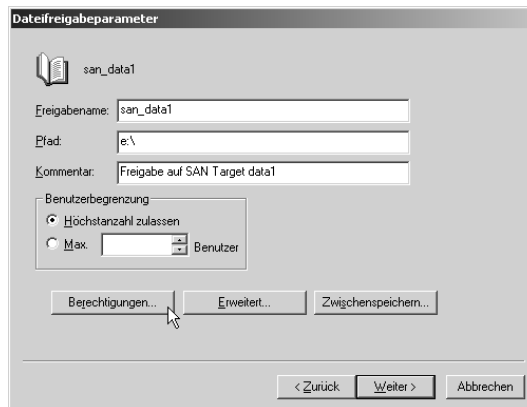
2. Vorhandene Ressourcengruppe verwenden: *Gruppe 0* (Abbildung 8.32).
3. Name der Ressourcengruppe: *Gruppe 0* (müssen Sie nicht verändern).
4. Zugriffsinformationen: Netzwerkname *GRUPPE0*, IP-Adresse z.B. *192.168.1.100* (Abbildung 8.33).

Abbildung 8.33:  
Als neue Ressourcen werden ein Netzwerkname und eine virtuelle IP-Adresse konfiguriert, später kommt eine Freigabe dazu



5. Erweiterte Eigenschaften: nicht ändern und WEITER.
6. Cluster-Ressource erstellen: *Ja, Clusterressource erstellen*
7. Typ der Anwendungsressource: *Dateifreigabe*
8. Name der Anwendungsressource: *san\_data1*
9. Die Dateifreigabeparameter können Sie der Abbildung 8.34 entnehmen. An dieser Stelle sollten Sie für die Testumgebung über *BERECHTIGUNGEN* für *jeder* Vollzugriff auf die Freigabe erlauben.

Abbildung 8.34:  
Eine Dateifreigabe kann als Cluster-Ressource den unterbrechungs-freien Zugriff auf Anwendungsdaten bereitstellen



10. Damit das Verschieben auf einen anderen Knoten auch immer sauber funktioniert, sollten Sie noch auf der entstandenen Ressource *san\_data1* (Abbildung 8.35) über *EIGENSCHAFTEN/ABHÄNGIGKEITEN* eine Abhängigkeit von der Ressource *Datenträger E:* festlegen. Dadurch geht die Freigabe erst dann online, wenn Laufwerk E: auf dem Knoten wirklich zur Verfügung steht.

11. Mit einem rechten Mausklick auf Gruppe 0 können Sie alle neu entstandenen Ressourcen ONLINE schalten (Abbildung 8.35).

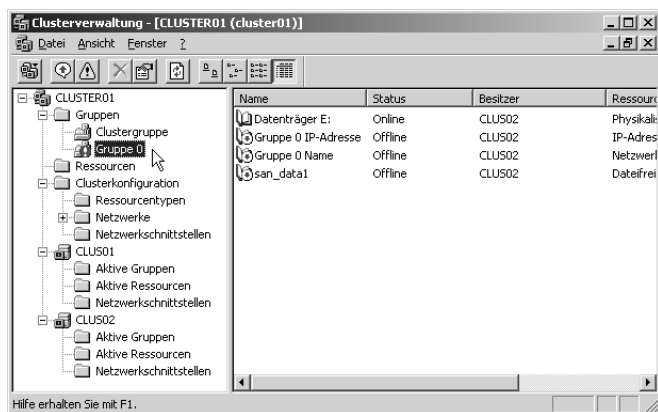


Abbildung 8.35:  
Für Gruppe 0  
können weitere  
Ressourcen erstellt  
und online geschal-  
tet werden

Jetzt können Sie sich von einem Client aus dem öffentlichen Netzwerk (zum Testen kann das bereits der Domänencontroller Srv01 sein) auf die Freigabe `\\gruppe0\san_data1` verbinden und mit den Daten arbeiten. Wenn Sie jetzt die Gruppe 0 in der Cluster-Verwaltung auf einen anderen Knoten verschieben, ist die Freigabe nach einer minimalen Unterbrechung sofort wieder verfügbar. Das entspricht einem geplanten Failover, z.B. für Wartungsarbeiten an einem Knoten.

#### Geplantes Failover

Wenn Sie dabei in einer DOS-Box auf dem Client ein `ping gruppe0 -t` laufen lassen, sehen Sie sehr schön, mit welcher geringen Verzögerung das Verschieben funktioniert.



Für die Simulation eines Knotenausfalls können Sie auch einfach die virtuelle Maschine Clus01 bzw. Clus02 (je nachdem, wer die Ressource gerade verwaltet) mit `POWEROFF` ausschalten. Es dauert etwas länger, bis der andere Knoten die Ressourcen übernimmt, aber nach einigen Sekunden startet automatisch das Failover, und die Freigabe steht wieder im öffentlichen Netz zur Verfügung.

#### Ausfall eines Knotens

### 8.3.6 Stufe 6 – Verteilen der virtuellen Maschinen auf verschiedene Hosts und weitere Möglichkeiten

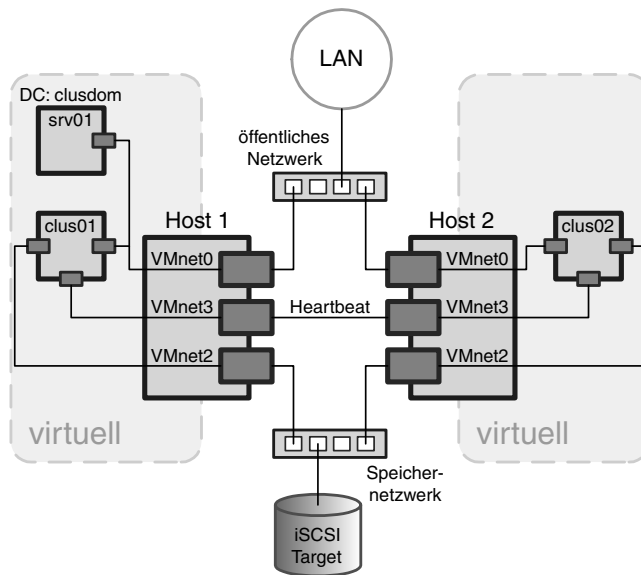
Ihr Cluster funktioniert, und Anwendungen im Cluster sind damit vor Software-Abstürzen geschützt oder können für Wartungsarbeiten am System auf einen anderen Server verschoben werden. Ein Problem ist allerdings noch nicht gelöst – was passiert, wenn der Host ausfällt?

**Hardware-Ausfall des Hosts**

Ein Hardware-Fehler betrifft den gesamten Cluster, da sich alle Maschinen auf dem gleichen Host befinden. Durch die Verwendung von virtuellen Maschinen und externem Speicher als gemeinsamen Datenträger ist der gesamte Aufbau aber sehr flexibel. Im Grunde genommen können Sie sämtliche Maschinen, den Domänencontroller, die beiden Cluster-Knoten und auch das iSCSI-Target auf jedem beliebigen anderen Host laufen lassen. Sie müssen dazu nur die VMs kopieren (Abbildung 8.36).

Da der Cluster schon funktioniert, können Sie das Kopieren sogar im laufenden Anwenderbetrieb erledigen. Zuerst verschieben Sie mit einem geplanten Failover alle Ressourcen auf einen Knoten. Dann können Sie den frei gewordenen Knoten herunterfahren, die VM auf einen anderen Host kopieren und dort wieder starten. Jetzt lassen sich die Ressourcen wieder auf beide Knoten verteilen.

Abbildung 8.36:  
Alle VMs und alle  
Dienste der Testum-  
gebung können  
flexibel auf andere  
Hosts oder direkt auf  
Hardware verscho-  
ben werden

**Änderungen am virtuellen Netzwerk beim Betrieb auf verschiedenen Hosts**

Vor dem Betrieb auf getrennter Hardware sind noch ein paar Änderungen an der Netzwerkkonfiguration nötig, da bisher die Kommunikation nur in internen virtuellen Netzwerken auf dem gleichen Host erfolgte. Aber auch dabei sind Sie mit virtuellen Maschinen sehr flexibel.

**Verbindung der VMs übers physische LAN**

Sie müssen den virtuellen Netzen VMnet1, VMnet2 und VMnet3 entsprechende physische Netzkarten auf dem Host zuweisen, um eine Verbindung über das physische Netzwerk zu ermöglichen. Dadurch funktioniert z.B. das Heartbeat-Netzwerk beider Knoten auch über die Grenzen eines Hosts hinaus, z.B. mit einem Crosslink-Kabel.

Sollten Sie nicht über genügend physische Netzwerke in beiden Hosts verfügen, um jedem Netzwerk (öffentlich, privat, Speichernetz) eine eigene Karte dediziert zuzuweisen, können Sie zur Not auch alle Netzwerke über ein und dieselbe Netzwerkverbindung betreiben. Durch die erfolgte Konfiguration mit verschiedenen IP-Netzwerken ist zumindest eine logische Trennung gegeben, später können weitere physische Netzwerkkarten flexibel zugewiesen werden.

Die Zuweisung physischer Netzwerkadapter zu den virtuellen Netzwerken erfolgt unter VMware über HOST/VIRTUAL NETWORK SETTINGS/HOST VIRTUAL NETWORK MAPPING bzw. unter Microsoft über VIRTUELLE NETZWERKE/KONFIGURIEREN/NAME DES NETZWERKS/NETZWERKEINSTELLUNGEN (siehe auch Netzwerk-Workshop in *Teil 3, Kapitel 2*).

### Beispielkonfiguration mit zwei physischen Hosts

Die Abbildung 8.36 verdeutlicht eine mögliche Konstellation. Zur besseren Übersicht sind in der Zeichnung nur die physischen Switches des LAN dargestellt.

Alle virtuellen Netzwerke sind mit drei dedizierten physischen Netzwerkkarten der Hosts verbunden. Dadurch können die Gäste unterschiedlicher Hosts über physische Verbindungen miteinander kommunizieren. An der Konfiguration der virtuellen Maschinen müssen Sie keinerlei Veränderungen vornehmen, nur den virtuellen Netzwerken sind die entsprechenden physischen Host-Netzwerke zuzuweisen. Haben Sie nur eine physische Netzwerkkarte im Host zur Verfügung, dann müssen Sie alle Adapter der VMs ans gleiche interne virtuelle Netzwerk (z.B. VMnet2) anschließen und diesem Netzwerk den physischen Adapter des Hosts zuweisen. Damit kommunizieren alle Adapter der Gäste über die gleiche physische Netzwerkverbindung.

**Flexible Zuweisung der virtuellen Netzwerkkarten**

Auf Host 1 laufen im Beispiel noch der Cluster-Knoten Clus01 und der Domänencontroller Srv01. Auf Host 2 läuft nur der Knoten Clus02. Das iSCSI-Target wurde ausgelagert auf eine Hardware-Lösung, z.B. ein SAN. Ein SAN in einer virtuellen Maschine kommt in einer produktiven Umgebung nicht in Frage.

Auch einer der Cluster-Knoten könnte direkt auf einem Hardware-Server laufen, um z.B. einen HBA (hardwarebasierter iSCSI-Initiator) für maximale Performance zu verwenden. Nur für den Failover-Fall wird dann ein virtueller Knoten auf einem der Hosts im Leerlauf betrieben.

Auf beiden Hosts können natürlich noch weitere Gäste laufen, um die virtuelle Infrastruktur auch richtig auszunutzen. So würde sich z.B. ein zusätzlicher Domänencontroller auf Host 2 zur weiteren Ausfallsicherheit anbieten, genauso ein Intranet-Server oder auch DHCP- und DNS-Dienste.



## 8.4 Besonderheiten und Ergänzungen zum Thema Cluster und VMs

Zum Abschluss gibt es noch ein paar Ergänzungen zum gesamten Thema Cluster mit virtuellen Maschinen.

### 8.4.1 Cluster mit einer gemeinsamen virtuellen SCSI-Festplatte anstelle von externem Speicher

**Für reine Tests  
wird kein iSCSI  
benötigt**

Sie haben an den Ausbaumöglichkeiten gesehen, dass die Verwendung des externen Speichers mit iSCSI-Anbindung den Aufbau des Cluster sehr flexibel macht. Wollen Sie allerdings nur einmal die Funktion eines Clusters in einer Testumgebung nachvollziehen, dann ist das zusätzliche Installieren des iSCSI-Speichers etwas umständlich. Als Alternative können Sie für die gemeinsamen Datenträger (Quorum und Daten) auch eine virtuelle SCSI-Platte verwenden. Ihre VMs können dadurch aber nur auf ein und demselben Host betrieben werden. Nur der VMware ESX-Server beherrscht das Handling eines gemeinsamen SCSI-Busses auch über physisch getrennte Hosts, wenn die virtuelle Platte auf einer LUN im SAN liegt.

#### **Vorgehensweise zum Erstellen und Einbinden der gemeinsamen Platte**

**Gemeinsamen  
Zugriff einrichten**

Im Prinzip können Sie eine virtuelle SCSI-Festplatte erstellen und diese in beiden Knoten-VMs als virtuelle Platte einbinden. Normalerweise können Sie aber eine VM nicht starten, wenn eine virtuelle Platte bereits von einer anderen VM verwendet wird. Das hat auch gute Gründe. Wenn auf die gleiche Platte von verschiedenen Gästen zugegriffen würde, dann würde das schnell zu Datenkorruption führen. Da wir aber einen Cluster installieren, der den Zugriff korrekt regeln kann, können Sie dem Virtualisierer mitteilen, dass die Platte von zwei Gästen gleichzeitig verwendet werden darf. Das geschieht auf folgende Art und Weise:

1. Erstellen Sie eine neue leere virtuelle SCSI-Platte für den Quorum-datenträger mit mindestens 500 MB Größe. Verwenden Sie keine Zuwachsplatten, sondern eine Platte mit fester Größe (bei VMware ALLOCATE ALL DISK SPACE NOW).
2. Binden Sie die Platte in der ersten VM an den SCSI-Bus 1 mit der ID 0 (SCSI1:0) ein. Unter Microsoft Virtual Server müssen Sie erst einen SCSI-Controller hinzufügen. Verwenden Sie nicht den SCSI-Bus 0, an dem eventuell schon Ihre bootfähige Systemplatte angeschlossen ist. Legen Sie die Platte wegen der besseren Übersicht nicht im Verzeichnis der VM ab, sondern an einer zentralen Stellen für beide VMs.

3. Fügen Sie in der zweiten VM die gleiche virtuelle Platte als vorhandene Platte hinzu. Sie können in beide VMs weitere Platten für die Daten hinzufügen, verwenden Sie für alle gemeinsam verwendeten Platten immer den SCSI-Bus 1.

Starten Sie noch keine der VMs, Sie müssen vorher noch ein paar Einstellungen treffen, um auf die virtuellen Platten von beiden Knoten aus zugreifen zu können. Diese Einstellungen sind von Produkt zu Produkt verschieden, Sie finden sie hier:

- ▶ *VMware Server* unterstützt das so genannten SCSI Reservation-Protokoll, das es ermöglicht, zwei Rechner (VMs) auf den gleichen SCSI-Bus zugreifen zu lassen. Dieses Protokoll können Sie einschalten, indem Sie mit einem Texteditor in der *vmx*-Datei der beiden Knoten-VMs folgende Zeile eintragen – diese Einstellung wirkt für alle Platten am SCSI-Bus 1:

```
scsil.sharedBus = "virtual"
```

Jetzt müssen Sie erlauben, dass virtuelle Platten der VM nicht für andere laufende VMs gesperrt werden (Locking). Diese Einstellung wirkt für alle Platten der VM:

```
disk.locking = "false"
```

- ▶ *VMware Workstation* unterstützt den gemeinsamen Zugriff nicht offiziell, aber mit einigen Einträgen in der *vmx*-Datei können Sie trotzdem damit arbeiten. Dabei wird aber kein richtiges Protokoll zum Bus-Sharing aktiviert, sondern nur dafür gesorgt, dass keine Daten in Puffern von VMware verbleiben und immer sofort auf die Platte geschrieben werden. Ob diese Methode in jeder Version von VMware Workstation immer sauber funktioniert, kann nicht garantiert werden, in einer Testumgebung ist es einen Versuch wert.

```
disk.locking = "false"
diskLib.dataCacheMaxSize = "0"
diskLib.dataCacheMaxReadAheadSize = "0"
diskLib.dataCacheMinReadAheadSize = "0"
diskLib.dataCachePageSize = "4096"
diskLib.maxUnsyncedWrites = "0"
```

- ▶ *Microsoft Virtual Server* unterstützt ebenfalls offiziell das gemeinsame Benutzen von virtuellen SCSI-Platten. Dazu müssen Sie zuerst in der Konfiguration beider Knoten-VMs mittels SCSI-ADAPTER/SCSI-ADAPTER HINZUFÜGEN einen neuen SCSI-Controller hinzufügen und dabei den Haken an SCSI-BUS FÜR CLUSTER FREIGEBEN setzen.

Hier gibt es eine Besonderheit zu beachten – jeder Controller muss in den VMs auf eine unterschiedliche SCSI-ID gesetzt werden, z.B. in Clus01 auf ID 7 und in Clus02 auf ID 6. Die gemeinsame Festplatte kann dann wieder auf ID 0 in beiden Gästen hinzugefügt werden.

Beide Knoten verfügen jetzt als gemeinsamen Datenträger über eine virtuelle SCSI-Platte. Sie können den ersten Knoten einschalten und auf der Platte eine NTFS-Partition erstellen und formatieren. Gehen Sie im weiteren Verlauf genauso vor, wie es weiter oben unter *Abschnitt 8.3.4, „Stufe 4 – Installation und Test des Clusters auf einem einzigen Host“*, bereits beschrieben wurde. Der einzige Unterschied ist, dass Sie auf die Installation des iSCSI Initiators verzichten können. Denken Sie daran, ein Aufteilen des Clusters auf unterschiedliche Hosts ist mit dieser Konfiguration nicht möglich.

### 8.4.2 Host-Cluster – komplette VMs als Ressourcen von Host zu Host verschieben

Eine weitere Besonderheit beim Thema Cluster ist die Option, die virtuellen Maschinen selbst als eine Ressource in die Cluster-Dienste einzubinden. Dazu müssen vor der Installation des Virtualisierungsproduktes die Cluster-Dienste auf den physischen Hosts installiert werden. Die Wirte sind dann praktisch die Knoten eines Clusters. Die virtuellen Maschinen liegen auf externem Speicher, der mit Fibre-Channel, iSCSI oder externen SCSI-Gehäusen angebunden sein kann.

#### **Failover bei Host-Ausfall**

Dadurch können ganze VMs bei geplanter Wartung am Host einfach auf andere Hardware verschoben werden. Wenn der Host ausfallen sollte, dann starten alle VMs automatisch auf einem anderen Host neu. Theoretisch ist es dadurch nicht mehr nötig, in jedem Gast separate Cluster-Dienste einzurichten, da der gesamte Gast, samt aller Dienste und Applikationen, auf einen anderen Host verschoben wird. So genial sich das anhört, einen Haken hat die Lösung: Fällt ein Host aus, dann werden die VMs auf dem anderen Host neu gestartet. Das bedeutet, alle offenen Verbindungen und ungespeicherten Änderungen in den Gästen gehen verloren. Das entspricht dem harten Abschalten und Neustarten eines Servers.

#### **Geplantes Failover bei Wartung**

Echtes Failover, wie das mit clusterfähigen Anwendungen möglich ist, kann diese Lösung nur bei geplanten Wartungsarbeiten bieten. Dabei werden die VMs samt Status auf dem einen Host eingefroren (*Suspend*) und auf dem anderen Host wieder aufgetaut (*Resume*). Geschieht das schnell genug, dann bemerkt weder das Gastsystem noch ein verbundener Client einen Ausfall.

## Host-Cluster mit den verschiedenen Serverprodukten

Microsoft Virtual Server 2005 R2 unterstützt offiziell einen Host-Cluster. Im Prinzip wird das mit einem Skript erreicht, das als *Generic Resource* (nicht von Haus aus clusterfähige Anwendung) eingebunden wird. Dieses Skript übernimmt das ordnungsgemäße Beenden von Virtual Server inkl. aller VMs (wahlweise Suspend oder Herunterfahren) beim geplanten Herunterfahren des Hosts. Für Wartungszwecke können allerdings nur alle VMs gleichzeitig auf den zweiten Knoten verschoben werden. Sie finden das benötigte Cluster-Skript *havm.vbs* und die ausführliche Anleitung *Virtual Server Host Clustering Step-by-Step Guide for Virtual Server 2005 R2* auf den Microsoft-Webseiten unter:

<http://www.microsoft.com/windowsserversystem/virtualserver/techinfo/default.mspx>

Eine deutschsprachige Anleitung finden Sie hier:

<http://www.microsoft.com/austria/technet/articles/hostclustering.mspx>

Aber auch für den VMware Server existieren Lösungen und Fremdherstellerprodukte. Notfalls können Sie selbst mit ein paar Skripten und mit *Suspend/Resume* die VMs zwischen den Hosts automatisiert verschieben. Das funktioniert sogar völlig ohne clusterfähiges Host-System, wenn die Dateien der virtuellen Maschinen auf einer LAN-Freigabe oder einem NAS liegen, wodurch der gemeinsame Zugriff der Hosts gewährleistet ist. Eine experimentelle Anleitung finden Sie hier:

<http://www.vmaschinen.de/vmscluster/>

Ein professionelles Produkt, um den VMware Server (oder GSX Server) clusterfähig zu machen, bietet die Firma VM6 mit *Virtual Machine Ex*:

<http://www.vm6.ca>

Der VMware ESX Server 3 verfügt mit einer SAN-Anbindung und einigen zusätzlichen Diensten der Virtual Infrastructure 3 über die ausgereiftesten Möglichkeiten zum Clustering. Da er den direkten Zugriff auf LUNs eines SAN aus den virtuellen Maschinen heraus unterstützt, sind alle Arten von Clustern, auch Hardware <> VM, fast ohne Performanceverluste möglich.

Der Dienst *VMotion* unterstützt das Verschieben laufender Gäste von einem Host auf den anderen in Echtzeit völlig ohne Ausfall, VMware DRS (*Distributed Resource Scheduler*) verteilt virtuelle Maschinen anhand ihrer Auslastung automatisch auf mehrere ESX Server-Hosts, und VMware HA (*High Availability*) erkennt Ausfälle laufender virtueller Maschinen und startet diese auf einem alternativen ESX Server-Host automatisch neu (ausführliche Beschreibung der Funktionen siehe Teil 2, Kapitel 9, „VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2“).

**Microsoft Virtual Server 2005 R2**

**VMware Server**

**VMware ESX Server 3**

## 8.5 Praxistauglichkeit der vorgestellten Lösung mit iSCSI Software Initiator

In erster Linie soll Ihnen der Workshop nachvollziehbar mit einfachen Mitteln alle Aspekte der Cluster-Konfiguration mit virtuellen Maschinen nahe bringen. Die Lösung eignet sich nicht nur als reine Testumgebung, aber wo liegen die Grenzen?

Einen stark belastete Exchange- oder Datenbankserver über einen iSCSI Software Initiator an den Speicher anzubinden ist sicherlich keine gute Idee. Für die Ausfallsicherheit eines kleinen Webservers oder wichtiger Dienste, wie DNS-, DHCP- bzw. Lizenzserver oder eines mäßig belasteten Domänencontrollers, ist dieser Weg dagegen durchaus praktikabel. Beim Einsatz von Jumbo Frames im iSCSI-Speichernetzwerk kommen akzeptable Leistungswerte zustande (*Teil 1, Kapitel 1, „Grundlagen virtueller Maschinen und Hinweise zur Hardware“*).

Mit der iSCSI Lösung können Sie auch ohne teuren ESX Server einen gemischten Cluster zwischen Hardware-Servern und virtuellen Maschinen betreiben. Die geringere Performance des Software-Initiators in einer VM kommt dabei nur im Notfallszenario zum Tragen, sobald ein Hardware-Knoten ausfällt und die VM die Arbeit übernimmt. Die Lösung ist interessant, wenn Sie für mehrere physische Server, die über schnelle Netzwerkkarten mit Offload-Einheit verfügen, virtuelle Maschinen nur als Stand-by-Knoten für das Ausfallszenario oder bei kurzen Wartungsarbeiten einsetzen.

In großen Umgebungen dürfte die Verwendung von iSCSI zur Speicheranbindung, selbst mit einem HBA, kein Thema sein. Hier sollten Sie eher zu Fibre-Channel mit 2 oder besser 4 Gigabit greifen. Dann ist für eine Cluster-Konfiguration zwischen Gästen auf unterschiedlichen Hosts aber auch unbedingt ein ESX Server nötig, nur er beherrscht den direkten Zugriff von Gästen auf LUNs in einem SAN als gemeinsamen Datenträger, das so genannte *Raw Device Mapping* (siehe auch *Teil 2, Kapitel 9*).

## 8.6 Fazit – konsequenter Einsatz von Virtualisierung auf allen Ebenen

Sie sehen an diesem Beispiel in vollem Umfang die Flexibilität, die der konsequente Einsatz von Virtualisierung auf allen Ebenen bringt. Virtuelle Maschinen sind dabei nur ein Aspekt. Speichervirtualisierung oder die Virtualisierung von Ressourcen durch Cluster kommt hinzu. Auf diese Weise löst sich die Abhängigkeit der Dienste und Anwendungen mehr und mehr von der Hardware und von den Räumlichkeiten, was einem reibungslosen unterbrechungsfreien Betrieb zugute kommt. Weitere Informationen zum Thema Ausfallsicherheit finden Sie in *Teil 3, Kapitel 5, „Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs“*.

# 9 VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2

Dieses Kapitel gibt Ihnen einen Überblick über die Funktionen und Begriffe von VMware Infrastructure 3 und VMware ESX Server 3. Es würde problemlos ein Buch für sich füllen, alle technischen Aspekte in der Tiefe vorzustellen, die das Flaggschiff aus der VMware-Produktreihe zu bieten hat. Ich konzentriere mich deshalb auf die Grundfunktionalität von ESX Server 3 und stelle die Möglichkeiten und das Zusammenspiel der zusätzlichen Module von VMware Infrastructure 3 vor.

Dieses Kapitel liefert Ihnen eine Entscheidungsgrundlage, welche Anforderungen der ESX Server gegenüber den kostenlosen Virtualisierungslösungen besser abdecken kann und durch welche Funktionen er sich vom VMware Server bzw. Microsoft Virtual Server abhebt.

Weiterhin bekommen Sie einen detaillierten Schnellstart und viele Tipps für die Einrichtung und Verwaltung Ihres ersten ESX Servers. Wollen Sie sich selbst über eine Evaluierungsversion mit dem Produkt vertraut machen, gibt es, im Gegensatz zum unkomplizierten Einstieg mit dem VMware Server, einige kleinere Klippen zu umschiffen. Wenn man diese nicht kennt, kann der erste Eindruck leicht getrübt werden. Ich zeige Ihnen beispielsweise, wie Sie einen vorhandenen Gast von VMware Workstation oder VMware Server auf dem ESX Server zum Laufen bekommen oder wie Sie den Zugriff auf externen Speicher über iSCSI einrichten.

**Überblick über  
VMware Infra-  
structure 3**

**Schnellstart zum  
ESX Server 3**

Eine Diskussion über lokale und externe Datenträger mit Begriffen, wie SAN, Fibre-Channel, iSCSI und NAS finden Sie in Teil 1, Kapitel 1, „Grundlagen virtueller Maschinen und Hinweise zur Hardware“. Diese Funktionen spielen beim VMware ESX Server eine große Rolle.

Um die Netzwerkoptionen besser zu verstehen, können Sie im Vorfeld die Einführung in Teil 3, Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“ durcharbeiten, dort erfahren Sie z.B. die Funktion eines virtuellen Switches und Konzepte der Vernetzung.



## 9.1 Begriffe und Funktionen der VMware Infrastructure 3

Spricht man vom VMware ESX Server 3, dann fällt im selben Atemzug auch der Begriff VMware Infrastructure 3 mit Schlagwörtern wie *VMotion*, *Virtual SMP* (*symmetrisches Multiprocessing*), *VMware DRS* (*Distributed Resource Scheduler*) oder *VMware HA* (*High Availability*). Ich werde gleich an erster Stelle den Begriffsdschungel lichten, um Ihnen einen Überblick zu geben, was sich hinter jeder Funktion im Detail verbirgt und wozu die einzelnen Komponenten dienen.

### ESX Server 3 und Virtual Center 2

VMware bietet mit seiner Infrastructure 3 ein Portfolio aus Produkten und Lösungen, das im Kern aus dem ESX Server 3 und VMware Virtual Center 2 besteht. Der ESX Server ist die Virtualisierungsbasis, auf der die Gäste laufen, und Virtual Center ist die Managementplattform, die mehrere Hosts mit Ihren virtuellen Maschinen zentral verwaltet. Sie können auch einzelne ESX Server völlig ohne Virtual Center betreiben, damit verschenken Sie aber viele der weiter unten geschilderten besonderen Möglichkeiten, die den Preis eines ESX Servers erst rechtfertigen.

### 9.1.1 Die Komponenten von Virtual Infrastructure 3 im Überblick

Bevor ich ins Detail gehe, erhalten Sie hier einen kurzen Überblick über alle Begriffe der Virtual Infrastructure 3:

- ▶ *ESX Server 3* – ist das Betriebssystem, das auf jedem einzelnen Host als Basis für die virtuellen Maschinen dient. Er ist der grundlegende Bestandteil der Virtual Infrastructure 3.
  - ▶ Der *VMkernel* und der *Virtual machine monitor* (*VMM*) bilden das eigentliche Betriebssystem des ESX Servers.
  - ▶ Die *Service Console* ist eine privilegierte VM unter RedHat Linux zur Steuerung und Verwaltung des VMware Kernels. Sie ist der sichtbare Teil des ESX Servers an der Konsole.
- ▶ *Dateisystem VMFS 3* – ist ein clusterfähiges Dateisystem des ESX Servers, wo virtuelle Platten abgelegt werden können. VMFS kann auf folgenden Datenträgern angelegt werden:
  - ▶ lokaler Plattenspeicher, aber nur mit unterstützten SCSI- oder RAID-Controllern, kein IDE oder SATA
  - ▶ SAN (Storage Area Network) mit Fibre-Channel-Anbindung
  - ▶ iSCSI-Target, erreichbar über einen physischen Host Bus Adapter (HBA) im ESX oder mit dem integrierten Software-Initiator des ESX Servers über einen normalen Ethernet-Adapter

NAS – seit dem ESX Server 3 können virtuelle Platten und virtuelle Maschinen auch auf einer Netzwerkfreigabe eines NAS (Network Attached Storage) liegen, dabei wird allerdings kein VMFS verwendet, da auf dem NAS bereits ein Dateisystem existiert.



- ▶ *Virtual SMP* – so nennt sich die Multiprozessorunterstützung von VMware. VMware ESX Server 3 kann jeder VM bis zu vier virtuelle CPUs durchreichen.
- ▶ *Virtual Infrastructure Client (VI Client)* – die grafische Oberfläche, die zur Verwaltung eines einzelnen ESX Servers oder der kompletten Infrastruktur dient. Der VI Client kann auf einem LAN-PC installiert werden und ermöglicht eine ähnlich komfortable Bedienung, wie Sie es bereits vom VMware Server oder der Workstation kennen.
- ▶ *VMware Virtual Center 2 (VC2)* – Virtual Center ist eine umfassende Managementlösung zur zentralen Verwaltung von Hosts, Gästen und Ressourcen. Virtual Center ist der zweite grundlegende Bestandteil der Virtual Infrastructure 3, wird aber für einen einzelnen ESX Server nicht unbedingt benötigt.
  - ▶ Der *Virtual Center Management Server* ist der zentrale Server von Virtual Center mit einer Datenbank zur Verwaltung aller Hosts und VMs.
  - ▶ Der *Virtual Center Agent* ist die Komponente auf einem Host, über die dieser vom Virtual Center verwaltet wird. Der Agent ist beim ESX Server 3 integriert.

Zusätzlich bietet der ESX Server 3 in Verbindung mit Virtual Center 2 ein paar ganz besondere Funktionen, die aber nur mit externem Speicher (SAN oder NAS) zum Tragen kommen:

- ▶ *VMotion* – ermöglicht das Verschieben laufender VMs von einem Host auf einen anderen ohne Ausfallzeit.
- ▶ *VMware DRS (Distributed Resource Scheduler)* – verteilt VMs anhand der CPU-Last und RAM-Verwendung automatisch auf unterschiedliche Hosts zur Lastverteilung. Dazu wird ebenfalls VMotion verwendet.
- ▶ *VMware HA (High Availability)* – dient als Hochverfügbarkeitslösung und startet virtuelle Maschinen von einem ausgefallenen Host auf einem anderen Host automatisch wieder neu.
- ▶ *VMware Consolidated Backup (VCB)* – dient als zentrale Datensicherung für die Gastsysteme. VCB ermöglicht die schnelle Sicherung von Daten virtueller Platten direkt vom SAN über das Speichernetzwerk. Dazu dient ein dedizierter Windows-Server als so genannter *Backup Proxy*. Die gesicherten Gäste können dabei weiterarbeiten (*Hot Backup*).



### 9.1.2 Der ESX Server 3 als Basis für die virtuellen Maschinen

#### VMkernel und Virtual machine monitor

Im Gegensatz zu allen anderen im Buch vorgestellten Produkten benötigt der ESX Server kein Host-Betriebssystem, auf dem er aufsetzt, sondern er läuft direkt auf der Hardware. Das bietet Vorteile, beispielsweise bessere Performance, auf die ich in *Teil 1, Kapitel 2, „Welches Virtualisierungsprodukt ist das richtige für Sie?“* bereits im Vergleich zu den anderen Produkten eingegangen bin. Der ESX Server besteht im Wesentlichen aus einem eigenen Kernel, dem *VMkernel* und einer *Service Console*, auch *COS (Console Operating System)* genannt.

Der Kernel übernimmt mit eigenen Treibern die Ansteuerung und Virtualisierung der Hardware, teilt den Gästen die Ressourcen zu und lässt die virtuellen Maschinen laufen, er ist sozusagen das Wirtsbetriebssystem. Der Kernel verwaltet die gesamte Hardware eines Hosts, von RAM und CPU über die Netzwerkkarten bis zu allen angeschlossenen Speichersystemen, egal ob Fibre-Channel, iSCSI oder NAS. Ein *Virtual machine monitor (VMM)* übernimmt die Virtualisierung der physischen CPUs für die virtuellen Maschinen.

#### Die Service Console zur Verwaltung des ESX Servers

Die *Service Console* dient der Verwaltung des Kernels und ermöglicht die Kommunikation mit dem Anwender. Wenn Sie am ESX Server sitzen und die Kommandozeile bedienen, arbeiten Sie genau genommen mit der Service Console. Die Konsole ist selbst eine Art virtueller Maschine, die über einige erweiterte Privilegien und Schnittstellen zum Kernel verfügt.

In der Service Console von ESX Server 3 wird dazu als Betriebssystem RedHat Enterprise Linux (RHEL) auf einer *ext3*-Partition verwendet. Hin und wieder führt diese Tatsache zu der Behauptung, der ESX Server liefere unter einem modifizierten Linux, was aber falsch ist. Vielmehr übernimmt nach dem Bootvorgang der VMkernel die Kontrolle über den Host. Die Service Console läuft dann unter dem VMkernel, wobei die Konsole den Kernel und die Gäste steuern und verwalten kann.

#### Kommandozeile und Netzwerkdienste

Das RedHat Linux in der Konsole liefert unter anderem eine Kommandozeile und dient als Basis für verschiedene Dienste. Die Service Console stellt z.B. Befehle zur Verwaltung virtueller Platten und virtueller Maschinen oder zur Lastauswertung bereit. Weiterhin laufen Anwendungen wie eine Firewall, sFTP-Server, SSH oder SMB-Client und zusätzliche Agenten für die Kommunikation mit dem Host über das Netzwerk. Zur Verwaltung des Servers spielt die kommando-basierte Service Console allerdings nicht mehr die Rolle wie noch beim ESX Server 2. Die Verwaltung erfolgt beim ESX Server 3 zum größten Teil im Netzwerk über einen komfortablen Client mit grafischer Oberfläche (siehe *Abschnitt 9.1.5, „Der Virtual Infrastructure Client zur Bedienung aller Komponenten über das LAN“*).

### 9.1.3 Das clusterfähige Dateisystem VMFS 3 als Ablage für die virtuellen Maschinen

VMFS (*VMware Filesystem*) ist ein spezielles Dateisystem, auf dem der ESX Server die virtuellen Platten der Gäste oder auch ISO-Images von CDs ablegt. VMFS wurde auf die Anforderungen von virtuellen Maschinen zugeschnitten und für die Verwaltung großer Dateien optimiert. Virtuelle Platten der Gäste können ausschließlich auf VMFS-formatierten Datenträgern liegen, mit einer Ausnahme, einem NAS – siehe Abschnitt 9.1.4, „Festplattenspeicher ohne VMFS verwenden“.

Eine VMFS-Partition kann im einfachsten Falle auf lokalen SCSI-Festplatten bzw. auf einem RAID-System erstellt werden, aber nicht auf IDE-Datenträgern. Einige Features des ESX Servers, z.B. VMotion zum Verschieben laufender VMs auf einen anderen Host, funktionieren allerdings nur mit externem Speicher (Abbildung 9.1). Dazu unterstützt der VMware ESX Server 3 neben Fibre-Channel für kleinere Umgebungen auch die preiswerte Speicheranbindung mit iSCSI oder ein NAS. Es muss also nicht mehr unbedingt ein teures Fibre-Channel-SAN sein, um externen Speicher zu nutzen.

**Lokaler oder externer Speicher**

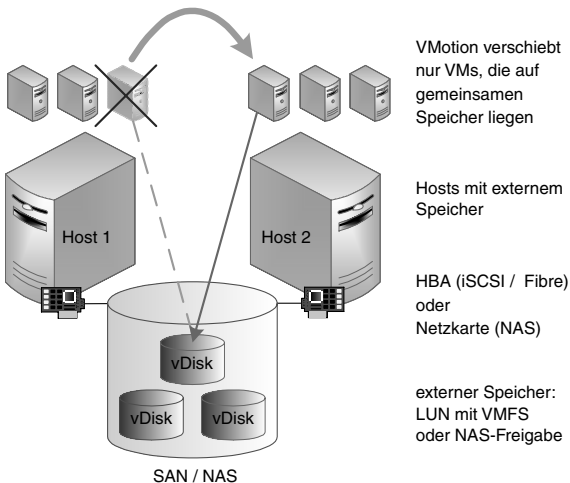


Abbildung 9.1:  
Gemeinsamer externer Speicher ist eine zentrale Komponente einer virtuellen Infrastruktur mit ESX Servern

VMware stellt im Kernel sogar einen Software iSCSI Initiator bereit, so dass für ein erstes Kennenlernen aller Funktionen ein kompatibler Ethernet-Adapter (z.B. Intel 1000) genügt, der in den meisten Servern heute bereits vorhanden ist. Für die nötige Performance in größeren Produktionsumgebungen empfiehlt sich allerdings ein physischer iSCSI-Host Bus-Adapter (HBA) oder eher ein SAN mit schneller 2- bzw. 4-Gbit-Fibre-Channel-Anbindung.

## Gemeinsamer Zugriff von Hosts auf externen Speicher und Cluster-Fähigkeit

Eine Besonderheit von VMFS ist seine Cluster-Fähigkeit. Das bedeutet, es ermöglicht den konkurrierenden Zugriff verschiedener Hosts auf das gleiche Dateisystem und damit auf die dort liegenden virtuellen Platten der Gäste. Voraussetzung dafür ist, dass die Hosts mit demselben externen Speicher (SAN) arbeiten. Mehrere ESX Server können sich das gleiche VMFS-Volumen auf einer LUN teilen. Dadurch wird es möglich, eine virtuelle Maschine abzuschalten und auf einem anderen Server einfach neu zu starten, weil beide Hosts Zugriff auf die Dateien, sprich, die virtuellen Platten der VM haben (Abbildung 9.1). Mit zwei VMware Servern unter Windows und einer NTFS-Partition im SAN würde das nicht funktionieren, weil immer nur ein Host auf die NTFS-Partition zugreifen dürfte, auf der die virtuellen Platten der Gäste liegen. Sie müssten einen der Windows-Hosts immer erst abschalten, Cluster-Dienste einrichten, oder die virtuellen Platten langwierig über das Netzwerk auf eine andere Partition kopieren.

### Zugriffskontrolle auf Dateiebene

Dass mehrere Hosts denselben Gast nicht versehentlich gleichzeitig starten können, dafür sorgt der ESX Server selbst, indem er jede benutzte virtuelle Platte mit einer Sperre (*Lock*) versieht, die erst bei abgeschalteter VM wieder aufgehoben wird. Damit gewährleistet VMware, dass eine virtuelle Platte einem Gast auf einem bestimmten Host exklusiv zugeordnet bleibt, solange der Gast läuft.



### IDE Platten verwenden

Sie können den ESX Server auch auf einer IDE-Platte installieren und starten, vorausgesetzt der IDE-Controller wird bei der Installation erkannt. SATA-Platten können nur an Controllern mit ATA-Emulation verwendet werden. Ein kurze Testinstallation des ESX 3 gibt gleich zu Beginn Aufschluss darüber, ob der Controller kompatibel ist und das System mit der IDE Platte läuft.

Für die virtuellen Maschinen ist allerdings immer ein Datenträger mit VMFS oder ein NAS zwingend, also kein IDE möglich. Um bereits mit geringem Budget eine Evaluierung einiger weiter unten beschriebenen Funktionen der Virtual Infrastructure 3 durchführen und das Handling des VMFS-Dateisystems kennen zu lernen, genügt aber bereits der integrierte Software-Initiator des ESX Servers und ein iSCSI Software Target unter Linux oder Windows als SAN-Ersatz (z.B. Starwind aus dem Cluster-Workshop in *Teil 2, Kapitel 8*, „Cluster mit VMs und einem iSCSI-Target als externem Speicher“). Erwarten Sie sich aus einer solchen Konfiguration aber keinesfalls gültige Aussagen über die Leistung und Stabilität eines ESX Servers. Offiziell wird eine Installation auf IDE-Platten von VMware nicht unterstützt und sollte auch keinesfalls in produktiven Umgebungen eingesetzt werden! Zum Testen kann man das im Notfall verwenden.

Mit dem ESX Server 3 ist VMFS in der Version 3 erschienen. Unter anderem kennt VMFS 3 jetzt Unterordner, was sich eigentlich nach nichts Besonderem anhört. Beim Vorgänger VMFS 2 lagen jedoch alle Dateien immer zusammen in der Wurzel eines Datenträgers, was schnell unübersichtlich werden konnte. Die Konfigurationsdateien der Gäste wurden separat auf einer Linux-Partition der Service Console abgelegt. Seit VMFS 3 lassen sich jetzt alle Dateien eines Gastes übersichtlich in einem gemeinsamen Ordner unterbringen, so wie Sie das von den Hosted-Produkten bereits kennen.

### 9.1.4 Festplattenspeicher ohne VMFS verwenden

Zusätzlich zum Dateisystem VMFS existieren zwei weitere Möglichkeiten, virtuellen Maschinen Datenträger zuzuweisen. Einmal kann das Gastsystem eine LUN direkt als Datenträger verwenden. Zum anderen können virtuelle Platten seit dem ESX Server 3 auch auf einer Netzwerkfreigabe eines NAS liegen.

#### Direkter Zugriff des Gastsystems auf eine LUN

VMware ESX Server ermöglicht den direkten Zugriff von Gästen auf eine LUN. Ein Windows-Gast kann die LUN beispielsweise mit einer NTFS-Partition formatieren, ohne den Umweg über eine Behälterdatei. Dazu wird kein VMFS benötigt. Den Zugriff bezeichnet man als *Raw Device Mapping*. Auf diese Weise können VMs auf unterschiedlichen Hosts eine LUN als gemeinsamen Datenträger für einen Cluster verwenden. Damit können Sie sogar einen Cluster aus einem physischen Server mit einer VM als Stand-by-Knoten konfigurieren. Bei den Hosted-Produkten, wie VMware Server oder Virtual Server, ist dazu der leistungsfressende Umweg über iSCSI –Software Initiatoren in den Gästen notwendig, wie es im Cluster-Workshop von *Teil 2, Kapitel 8*, beschrieben ist.

**Cluster zwischen VMs und Hardware**

Der ESX Server 3 unterstützt als gemeinsamen Datenträger für einen Cluster über verschiedene physische Hosts (*Cluster across Boxes*) keine virtuellen Platten mehr, sondern nur noch eine gemeinsame LUN über *Raw Device Mapping*.



#### NAS-Freigaben als externen Speicher verwenden

VMware ESX Server 3 akzeptiert als externen Speicher auch NAS (*Network Attached Storage*), allerdings nur mit NFS (*Network File System*) Version 3 über TCP. Windows SMB (*Server Message Block*) oder CIFS (*Common Internet File System*) wird nicht unterstützt. Sie können also keine einfache Dateifreigabe auf einem Windows Server als gemeinsamen Speicher für einen ESX Server verwenden, es sei denn, Sie installieren die kostenlosen *Microsoft Windows Services für Unix*,

die NFS-Freigaben unter Windows bereitstellen. Der Windows Server 2003 R2 bringt das Paket bereits mit. Ebenso würde sich ein Linux-Server mit NFS anbieten.

Mit VMs auf einem NAS funktionieren auch die Module der Virtual Infrastructure, wie VMotion, HA und DRS. Das ergibt neben iSCSI eine weitere preiswerte Möglichkeit, in kleinen Umgebungen alle Funktionen der Virtual Infrastructure 3 zu nutzen.



### **Worin unterscheidet sich im Wesentlichen ein SAN von einem NAS?**

In Teil 1, Kapitel 1, „Grundlagen virtueller Maschinen und Hinweise zur Hardware“, finden Sie eine detaillierte Beschreibung der verschiedenen Datenträgeranbindungen, hier eine kurze Zusammenfassung:

#### **Dateiorientierter Zugriff**

Auf einem NAS kann der ESX Server kein VMFS-Volumen anlegen, da NFS bereits ein eigenes Dateisystem ist. Die virtuellen Maschinen liegen also direkt auf einer Netzwerkfreigabe des NAS, und der Zugriff erfolgt dateiorientiert. Um die Verwaltung der Datenblöcke auf dem physischen Datenträger, also um die Speicherung der Dateien und Verzeichnisse, kümmert sich das NAS. Der ESX Server greift über das Netzwerk darauf zu wie ein LAN-Client auf einen Fileserver.

#### **Blockorientierter Zugriff**

Im Gegensatz zum NAS ist beim blockorientierten Zugriff auf eine LUN über Fibre-Channel oder iSCSI der zugreifende Rechner (in unserem Falle der ESX Server) für die Verwaltung der Datenblöcke und des Dateisystems selbst verantwortlich. Eine LUN erscheint dabei auf dem ESX Server wie eine lokal eingebaute Festplatte, auf der erst eine Partition angelegt und formatiert werden muss – beim ESX Server mit VMFS, unter Windows z.B. mit NTFS. Protokollbedingt ist der blockorientierte Zugriff meist schneller als der dateiorientierte.

### **9.1.5 Der Virtual Infrastructure Client zur Bedienung aller Komponenten über das LAN**

Das zentrale Werkzeug zur Bedienung von ESX Server 3 ist der *Virtual Infrastructure Client*, kurz *VI Client* (Abbildung 9.2). Mit dieser grafischen Benutzeroberfläche, ähnlich der Remote Console des VMware Servers, erfolgt sowohl die unmittelbare Bedienung eines einzelnen ESX Servers als auch die Verwaltung ganzer Serverfarmen über das *VMware Virtual Center* (siehe Abschnitt 9.1.6, „*VMware Virtual Center 2 zur zentralen Verwaltung von Hosts, Gästen und Ressourcen*“). Im Virtual Infrastructure Client können Sie virtuelle Maschinen erstellen, konfigurieren und steuern, Sie können virtuelle Netzwerke auf dem Host einrichten und physische Netzwerkkarten zuweisen

bzw. externen und internen Plattenspeicher verwalten. Weiterhin haben Sie Zugriff auf die Ressourcensteuerung und -auswertung Ihres Hosts sowie der Gäste. Kurz – mit dem Client erhalten Sie die Kontrolle über die gesamte virtuelle Infrastruktur. Der Client ist eine entscheidende Verbesserung beim Umgang mit dem ESX Server im Gegensatz zum Web-Interface des ESX Servers 2.

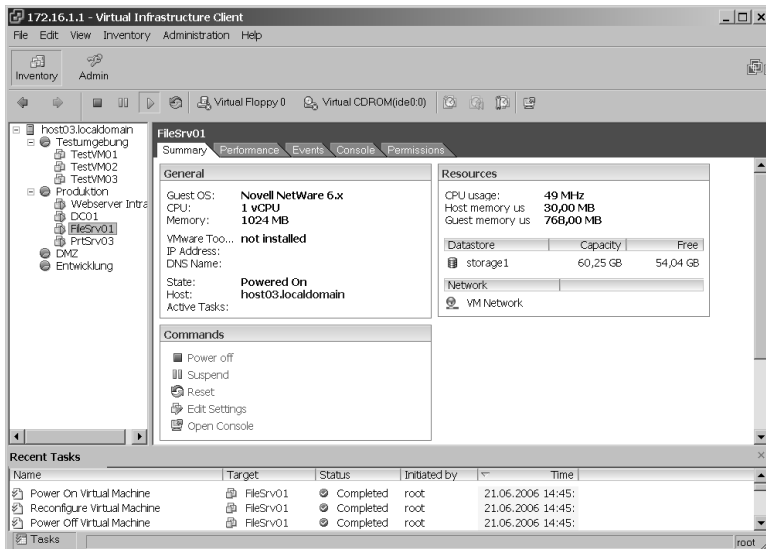


Abbildung 9.2:  
Mit dem Virtual  
Infrastructure Cli-  
ent kann ein einzel-  
ner ESX Server oder  
die gesamte Struk-  
tur komfortabel ver-  
waltet werden

Der Client muss auf einem PC im LAN unter Windows installiert werden. Wenn Sie nur einen einzelnen ESX Server betreiben bzw. auf einige der besonderen Funktionen der Virtual Infrastructure vorläufig verzichten können, dann genügt der Client bereits ohne Virtual Center zur vollständigen Verwaltung von Host und Gästen.

Zur Bedienung der virtuellen Maschinen stellt VMware auch ein Web-Interface bereit. Damit können Sie Gäste über einen Browser fernsteuern oder diesen Zugriff Anwendern ermöglichen, ohne gleich den Infrastructure Client zu installieren. Eine Verwaltung der Hosts ist allerdings nicht möglich. Jeder ESX Server stellt ein eigenes Web-Interface zur Verfügung, Sie erreichen es über die Begrüßungswebseite des Hosts mittels [https://mein\\_host/](https://mein_host/). Der *Virtual Infrastructure Web Access*, der zum Virtual Center mitgeliefert wird, bietet ein zentrales Web-Interface für alle VMs einer Infrastruktur.



### 9.1.6 VMware Virtual Center 2 zur zentralen Verwaltung von Hosts, Gästen und Ressourcen

Wenn Sie mehrere ESX Server betreiben, dann können Sie diese ins *VMware Virtual Center 2* einbinden. Virtual Center fasst die Hosts zu einem so genannten *Datacenter* zusammen und ermöglicht die zentrale Verwaltung aller Hosts und ihrer virtuellen Maschinen. Virtual Center bietet Funktionen zur Überwachung von Hosts und Gästen mit der Möglichkeit, Warnmeldungen zu versenden bzw. automatisch Skripte auszuführen. Sie erhalten einen Überblick über die Auslastung einzelner Komponenten oder der gesamten Umgebung. Sie können Maschinen manuell zwischen den Hosts verschieben oder automatische Lastverteilung und Hochverfügbarkeit zwischen einzelnen Host konfigurieren. Eine Verwaltung von Vorlagen, so genannte *Templates*, für virtuelle Maschinen ermöglicht Ihnen, in kurzer Zeit durch automatisierte Klonvorgänge neue Gäste zu erzeugen. Kurz: Virtual Center fasst einzelne Hosts erst zur Virtual Infrastructure zusammen.

#### Virtual Center Management Server

Die zentrale Komponente ist der *Virtual Center Management Server*, der auf einem Rechner unter Windows installiert wird. Er verwaltet über die *Virtual Center Agents* alle eingebundenen Hosts in einer Datenbank. Im Gegensatz zu den Vorgängerversionen sind die Agents bereits im ESX Server 3 enthalten und müssen nicht mehr für jeden Host erworben werden. Der Management Server ist dagegen weiterhin als separates Produkt zu lizenzieren, Kosten für die verwalteten ESX Hosts fallen nicht an.



In der derzeitige Version von Virtual Center 2 ist noch keine Einbindung des VMware Servers möglich, was in der Vorgängerversion, dem Virtual Center 1.4, möglich ist. Eine Unterstützung ist laut VMware in Zukunft geplant.

Sobald die Hosts im Virtual Center integriert sind, verbinden Sie den Virtual Infrastructure Client nicht mehr direkt mit den einzelnen Hosts, sondern zentral mit dem Virtual Center Management Server. Die Hosts und ihre virtuellen Maschinen können zu *Datacentern* mit *Clustern* oder zu *Ressourcenpools* zusammengefasst werden und lassen sich in einer Ordnerstruktur, ähnlich dem Inventory des VMware Servers, verwalten.

Jede virtuelle Maschine läuft zwar weiterhin auf einem bestimmten ESX Server, ist aber nicht mehr an ihn gebunden. VMs können jederzeit, auch im laufenden Betrieb, auf andere Hosts verschoben werden, bei Bedarf sogar automatisch nach bestimmten Auslastungswerten. Für solche Funktionen stellt VMware einige herausragende Zusatzmodule bereit, die nur zusammen mit Virtual Center und externem Speicher funktionieren.

### 9.1.7 VMotion verschiebt laufende VMs zwischen unterschiedlichen Hosts

VMotion ermöglicht es, Gäste per Mausklick von einem Host auf einen anderen zu verschieben. Das Besondere daran ist, dass diese Migration ohne Unterbrechung im laufenden Betrieb des Gastsystems erfolgt. Mit VMotion können Sie z.B. für Wartungsarbeiten an der Hardware eines Hosts alle Gäste ohne Ausfallzeiten kurzfristig auf einen anderen Server verschieben.

Bei einem VMotion-Vorgang kopiert VMware den RAM-Inhalt des Gastes vom aktuellen Host auf den Ziel-Host. Im Gegensatz zum Suspend-Modus von VMware Server oder Microsoft Virtual Server friert VMware den Gast aber nicht sofort ein, sondern kopiert zuerst den gesamten RAM-Inhalt, während der Gast weiterarbeitet. Erst nach dem Abschluss der Übertragung friert VMware die VM ein und überprüft, welche Speicherseiten der Gast mittlerweile geändert hat. Nur diese Differenz wird jetzt noch kopiert, und auf dem Ziel-Host arbeitet das Gastsystem fast augenblicklich weiter. Der Übertragungsvorgang geht meist so schnell, dass die Anwender keinerlei Ausfälle bemerken.

Für VMotion benötigen beide beteiligte Hosts Zugriff auf den gleichen externen Speicher, um nahtlos die virtuellen Platten übernehmen zu können. Allein mit lokalem Speicher funktioniert VMotion nicht, weil sonst erst sehr umfangreiche Kopiervorgänge für die virtuellen Platten stattfinden müssten. Mit der Version 3 des ESX Servers ist es, dank der Unterstützung von iSCSI und NAS, nicht mehr nur Rechenzentren mit teurem Fibre-Channel-SANs vorbehalten, VMotion zu nutzen.

Auch mit dem kostenlosen VMware Server ist in gewissen Grenzen über den Suspend-Modus das Verschieben laufender VMs von einem Host zum anderen möglich, vorausgesetzt die VMs liegen auf einer gemeinsamen LAN-Freigabe oder einem NAS. Bringen Sie die VM auf einem Host in den Suspend-Modus, können Sie den Gast auf dem anderen Host relativ schnell wieder zum Leben erwecken (siehe <http://www.vmaschinen.de/vmscluster/>).



### 9.1.8 VMware DRS zur Verteilung von Gästen zwischen den Hosts mittels Load Balancing

VMotion kann auch dazu dienen, Gäste anhand der Auslastung automatisch zwischen den Hosts im Datacenter zu verschieben, damit eine optimale Ressourcenverteilung erreicht wird. Das übernimmt ein Dienst namens *VMware DRS (Distributed Resource Scheduler)*. Er überwacht die Auslastung von CPU und Hauptspeicher der Hosts sowie der virtuellen Maschinen und erkennt, wann bestimmte Limits



überschritten werden. Der Dienst entscheidet, welche Hosts über genügend Kapazitäten verfügen, um weitere Gäste aufzunehmen, und welche Hosts entlastet werden sollten. Die Parameter dafür können Sie über so genannte *Resource Pools* für bestimmte Gruppen von VMs festlegen (siehe auch Abschnitt 9.3.7, „Die erste virtuelle Maschine erstellen und einen Resource Pool anlegen“).

Sobald Ressourcen knapp werden, migriert VMware DRS die Gäste entweder vollautomatisch auf andere Hosts oder generiert nur Meldungen mit Empfehlungen zum manuellen Verschieben. Sie können auch festlegen, dass VMware DRS nur beim ersten Start einer VM entscheidet, auf welchem Host der Gast laufen soll, ohne danach weitere automatisierte Migrationen vorzunehmen. Damit genügt es, wenn ein Anwender eine VM erstellt und startet, er muss sich nicht darum kümmern, ob der Host über genügend Kapazitäten verfügt. Ob alle Funktionen automatisch oder nur rein manuell ablaufen, können Sie anhand von Parametern den Gegebenheiten Ihrer Umgebung anpassen.

#### Keine ungenutzte Leistung mehr

Durch automatisches Load Balancing mit DRS wird eine hohe Auslastung der physischen Hosts möglich, da es bei Lastspitzen einzelner VMs jederzeit möglich ist, diese umzulagern. Sie müssen nicht mehr auf jedem Wirt genügend freie Kapazität für seltene Lastspitzen einzelner Gäste einplanen, was bisher in Farmen aus mehreren ESX Servern zu einem hohen Verschnitt an ungenutzter Kapazität führte. Vielmehr genügt es, wenn im gesamten Datacenter auf einigen Hosts Leistung zur Verfügung steht, die dann flexibel verteilt werden kann.

### 9.1.9 VMware HA als Hochverfügbarkeitslösung für virtuelle Maschinen

Ein weiterer neuer Dienst ist *VMware HA (High Availability)*. VMware HA erkennt Ausfälle eines Hosts und startet die Gäste auf einem alternativen ESX Server automatisch neu. Damit können herkömmliche Cluster-Lösungen ergänzt oder sogar ersetzt werden. Der große Vorteil ist, dass selbst Anwendungen oder Betriebssysteme, die gar keine Cluster-Funktionen besitzen, damit in den Genuss der Hochverfügbarkeit kommen.

Der Nachteil ist allerdings, dass die Gäste nach einem Ausfall auf einem anderen Host immer neu gestartet werden. Alle offenen LAN-Verbindungen und alle nicht abgespeicherten Änderungen geöffneter Anwendungen in den Gastsystemen gehen dabei verloren. Im Gegensatz zu einem geplanten Verschieben mit VMotion konnten vor dem Absturz der RAM-Inhalt und der Status der VMs natürlich nicht gesichert werden. Ein nahtloser Übergang, wie das mit manchen clusterfähigen Anwendungen, etwa Microsoft Exchange, in bestimmten

Grenzen möglich ist, findet nicht statt. Trotzdem sorgt VMware HA für eine sehr geringe Ausfallzeit und macht manuelle Eingriffe der Administratoren seltener notwendig.

Die beteiligten Hosts überwachen sich gegenseitig mittels LAN- und SAN-Heartbeat, eine Überwachung einzelner VMs erfolgt allerdings nicht. Das bedeutet, dass eine abgestürzte Anwendung in einem Gast kein Failover auslöst, sondern nur der Ausfall eines kompletten ESX Servers.

Weitere Informationen und Konzepte zur Redundanz, Disaster Recovery und Ausfallsicherheit finden Sie in *Teil 3, Kapitel 5, „Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs“*.



### 9.1.10 VMware Consolidated Backup als zentrale Datensicherung für die Gastsysteme

Zur Datensicherung virtueller Maschinen stellt *VMware Consolidated Backup* einige interessante neue Ansätze bereit. In vielen virtuellen Umgebungen werden die Gäste weiterhin wie physische Rechner durch Datensicherungsprogramme über das LAN gesichert. Das kostet während der Sicherungsvorgänge Leistung auf den Hosts und Bandbreite im LAN. Außerdem benötigen Sie gegebenenfalls Sicherungsagenten in jedem Gastsystem. Weitere Ansätze sind das komplette Wegkopieren der virtuellen Platten über die Service Console, wie es z.B. der bekannte ESX Ranger der Firma Vizioncore tut. Auf Sicherungskonzepte virtueller Maschinen gehe ich in *Teil 3, Kapitel 5, „Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs“*, detaillierter ein.

#### Zentraler Backup-Proxy direkt am SAN

VMware Consolidated Backup ermöglicht das Sichern der virtuellen Maschinen von einem zentralen Backup-Proxy aus, direkt vom SAN, ohne Umwege über das LAN. Der Proxy ist ein physischer Rechner unter Microsoft Windows Server 2003, der Zugriff auf das gleiche SAN haben muss, mit dem auch die ESX Server arbeiten. Dazu ist in diesem Proxy ein Fibre-Channel-HBA einzubauen, da Consolidated Backup derzeit nur in Verbindung mit einem Fibre-Channel SAN unterstützt wird.

Zusätzlich sollte der Rechner über einen eigenen Streamer bzw. eine Bandbibliothek verfügen, oder er hat Zugriff auf ein entferntes Sicherungsmedium, z.B. Plattenplatz auf einem NAS. Eine Sicherungssoftware, wie NTBackup, Backup Exec, Tivoli Storage Manager, oder eigene Kopierlösungen müssen ebenfalls auf dem Proxy eingerichtet werden.

VMware Consolidated Backup ist selbst kein Sicherungsprogramm, es stellt nur den Zugriff auf die virtuellen Platten der Gäste bereit. Dazu liefert VMware eine Reihe Skripte und Tools, die automatisiert bestimmte Aktionen auslösen, um den Inhalt virtueller Platten zugänglich zu machen. Den eigentlichen Sicherungsvorgang übernehmen dann wieder die üblichen Backup-Lösungen.



Sollten Sie mittels *Raw Device Mapping* bestimmten Gästen LUNs direkt zugewiesen haben, dürfen diese LUNs nicht für den Backup-Proxy sichtbar werden, bevor Sie nicht das automatische Zuordnen von Laufwerksbuchstaben unter Windows unterbunden haben. Sonst kann es passieren, dass der Proxy eine NTFS-Partition auf einer LUN unter einem Laufwerksbuchstaben einbindet und darauf schreibt, was im Gast zu Datenverlust führt. Bevor Sie das Kabel an Ihren HBA des Proxys anschließen, starten Sie an einer Kommandozeile das Programm *diskpart*, und geben Sie folgende Kommandos ein:

```
automount disable
automount scrub
exit
```

Jetzt können Sie Windows herunterfahren und das Kabel an Ihren HBA anschließen.

### Ablauf einer Sicherung mit VMware Consolidated Backup

#### Sicherung auf Dateisystem- ebene

Die Sicherung erfolgt unmittelbar von den mit VMFS formatierten LUNs, auf denen die virtuellen Platten liegen. Dabei können nicht nur kompletten Kopien der virtuellen Festplatten einer VM erstellt werden, was dem Image eines physischen Servers entsprechen würde. Vielmehr ermöglicht VMware Consolidated Backup den Zugriff auf das Dateisystem der Gäste. Sie können dazu im Sicherungsjob Ihres Datensicherungsprogramms auf dem Backup-Proxy Skripte hinterlegen, die in den gesicherten VMs bestimmte Aktionen auslösen. Im Prinzip erfolgt die Sicherung in folgenden Schritten:

1. Der Sicherungsjob auf dem Backup-Proxy startet ein Skript, das Sie hinterlegen und konfigurieren müssen. VMware liefert bereits Muster. Dieses Skript signalisiert über Virtual Center einer bestimmten VM, dass eine Sicherung ansteht.
2. In der VM werden über die VMware Tools automatisch weitere Skripte ausgelöst, in denen Sie beispielsweise das Herunterfahren einer Datenbank oder des Exchange Servers hinterlegen können, um diese in einen konsistenten Zustand zu bringen.
3. Jetzt wird in der zu sichernden VM die so genannte *Quiescing*-Funktion ausgelöst, die NTFS kurz einfriert und offene Transaktionen beendet. Das sorgt für die Konsistenz des Windows-Dateisystems. Datenbanken kann die *Quiescing*-Funktion nicht bedienen.

4. Erst jetzt wird ein Redo-Log erzeugt, das die virtuelle Platte vor Schreibzugriffen der VM schützt.
5. Nach dem Erzeugen des Redo-Logs wird im Gast ein weiteres Skript abgearbeitet, worüber Sie beispielsweise eine heruntergefahrte Datenbank wieder starten können.
6. Jetzt kann der Gast sofort weiterarbeiten, er schreibt nur noch in die Redo-Logs. Dadurch befinden sich die zugrunde liegenden virtuellen Platten in einem konsistenten unveränderlichen Zustand und können in Ruhe gesichert werden.
7. Das Backup-Skript bindet die zu sichernde virtuelle Platte ins NTFS-Dateisystem am Backup-Proxy ein, ähnlich dem Tool *VMware Diskmount* für die Hosted-Produkte (siehe Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“).
8. Das Backup-Skript ist beendet, und die Sicherungssoftware hat jetzt lesenden Zugriff auf einen konsistenten, unveränderlichen Zustand des Inhaltes einer virtuellen Platte und kann auf Dateibasis eine Sicherung durchführen.
9. Nach dem Ende der Sicherung kann die Backup-Software ein weiteres Skript starten, das Sie ebenfalls im Sicherungsjob hinterlegen müssen. Dieses Skript hängt die virtuelle Platte am Backup-Proxy wieder ab und addiert den aufgelaufenen Inhalt des Redo-Logs zur virtuellen Platte (*Commit*). Das Redo-Log wird danach eliminiert. Der Gast schreibt bis zum nächsten Backup wieder direkt auf die virtuelle Platte.

#### Verwendung von Redo-Logs

### Vorteile von Consolidated Backup

Durch die zentrale Sicherung sind nur noch in speziellen Fällen herkömmliche Backup-Agenten in den VMs notwendig. Weiterhin erfolgt die Sicherung nicht mehr aus der VM heraus über das LAN, sondern über das schnellere Speichernetzwerk, an dem das SAN angebunden ist. Ein weiterer wichtiger Vorteil ist die Unabhängigkeit von einem Sicherungsfenster, da durch die Snapshot-Technik jederzeit eine Sicherung laufender Maschinen möglich ist.

### Probleme von Consolidated Backup

Ein größeres Problem können bestimmte Anwendungen sein, die sich nicht ohne weiteres in einen kurzzeitigen konsistenten Zustand vor dem Snapshot versetzen lassen, etwa Datenbanken. Für diesen Fall können Sie vor und nach dem Snapshot über die VMware Tools im Gast benutzerspezifische Skripte abarbeiten lassen, die dann gegebenenfalls Datenbanken vor dem Snapshot kurz herunterfahren und danach gleich wieder starten. Viele Datenbanken ermöglichen über spezielle Kommandos oder APIs, Transaktionen abzuschließen und Puffer zu leeren. Diese Funktionalität ist allerdings von der entsprechenden Anwendung abhängig.

Im Zweifelsfalle müssen Sie in manchen Gästen zusätzlich zu VMware Consolidated Backup mit einem Backup Agenten arbeiten, der die spezielle Anwendung unterstützt. Eine Lösung können auch Drittanbietertools sein, die für konsistente Datenbanken verschiedener Applikationen in der VM sorgen, z.B. FalconStor Application Snapshot Director for VMware ([www.falconstor.com](http://www.falconstor.com)).

Das Wiederherstellen einzelner Dateien im Gastsystem kann der Backup-Proxy ebenfalls nicht leisten, da er auf die virtuelle Platte einer laufenden VM nicht schreiben kann. Rücksichern erfolgt immer wie gewohnt über das LAN.

Weiterhin sind keine inkrementellen Backups auf Basis des Archivbits möglich, da auf die gesicherte Platte nur lesend zugegriffen wird. Für inkrementelle Backups müssen Sie Ihre Backup-Software auf die Verwendung von Dateiänderungszeiten umstellen.



Eine detaillierte Diskussion zu allen Aspekten der Datensicherung, von Hot-Backup über Disaster Recovery bis zu Volumenschattenkopien in Gästen finden Sie in Teil 3, Kapitel 5, „Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs“.

### 9.1.11 Weitere besondere Eigenschaften des ESX Servers 3

Im Grunde genommen sind alle oben genannten Features bereits Alleinstellungsmerkmale, die den ESX Server mit Virtual Center deutlich von VMware Server und Microsoft Virtual Server abheben. Das Zusammenspiel aller Features und Komponenten unter Virtual Center macht die virtuellen Maschinen in hohem Maße von der Hardware unabhängig. Aber bereits ein einzelner ESX Server verfügt über einige sehr interessante Funktionen, auf die ich im Folgenden noch eingehe.

#### Ressourcenkontrolle über Speicher, CPU und Bandbreite

##### 16 GB RAM und vier CPUs pro VM

Seit dem ESX Server 3 können Sie jedem Gast maximal 16 GB Hauptspeicher zuweisen, entgegen den 3,6 GB, die von allen anderen Produkten bereitgestellt werden. Weiterhin kann der ESX Server bis zu vier virtuelle CPUs in eine VM durchreichen, alle anderen VMware-Produkte ermöglichen maximal zwei virtuelle CPUs, die Microsoft-Produkte nur eine.

Ressourcen wie CPU, RAM, Plattenperformance und Netzwerkbandbreite lassen sich pro VM mit Minimum-/Maximumwerten (*Reservation/Limit*) begrenzen bzw. zusichern oder proportional mittels *Shares* unter mehreren Gästen verteilen. Shares sind Wichtungswerte, die angeben, welche Gäste mehr und welche Gäste weniger von aktuell vorhandenen Ressourcen abbekommen. So erhält ein Gast mit 200

CPU-Shares prozentual mehr Anteile von der verfügbaren CPU-Leistung als ein Gast mit 100 Shares. Sind die gesamten verfügbaren CPU-Ressourcen ausgeschöpft, dann laufen die Anwendungen in dem Gast mit den meisten CPU-Shares am schnellsten. Die Änderung und Steuerung dieser Werte sind im laufenden Betrieb möglich, über *Resource Pools* können Ressourcen bestimmten Gruppen von VMs zugewiesen werden. Sind beispielsweise alle Ressourcen eines Pools der Testumgebung aufgebraucht, dann können in anderen Pools für produktive Anwendungsgruppen durchaus noch genügend Ressourcen zur Verfügung stehen, um Gäste mit der nötigen Leistung laufen zu lassen.

### Netzwerkfunktionen wie Teaming und VLAN

Der ESX Server unterstützt Teaming von Netzwerkkadaptern zur Zusammenfassung der Bandbreite oder zur Ausfallsicherheit. Sie können, im Gegensatz zu den Hosted-Produkten, einem virtuellen Switch mehrere physische Adapter zuweisen. Während ein Gast an diesem virtuellen Switch Daten über das Netzwerk sendet, kann einer der zugewiesenen physischen Adapter ausfallen, ohne dass ein Abbruch der Verbindung erfolgt. Ich gehe weiter unten an einem praktischen Beispiel noch darauf ein. Der Gast merkt dabei nichts vom Teaming der physischen Adapter, er arbeitet nur über eine virtuelle Netzwerkkarte am virtuellen Switch.

Weiterhin können die virtuellen Switches VLANs bilden. Hier kann der ESX Server alle Vorteile seiner eigenen Treiber und Hardware-Verwaltung ausspielen, für diese Funktionen werden keine speziellen Herstellertreiber oder Zusatzsoftware benötigt.

Die Verwaltung der Netzwerkkadaptern und der virtuellen Switches erfolgt im Virtual Infrastructure Client in einem sehr übersichtlichen grafischen Interface. Den ESX 2-Nutzern wird angenehm auffallen, dass es möglich ist, für die Service Console und für die LAN-Anbindung der Gäste ein und dieselbe Netzwerkkarte zu verwenden. Dazu müssen keine Konfigurationsdateien mehr editiert werden, um den Gästen über spezielle Treiber den physischen Adapter der Service Console zugänglich zu machen, wie das beim ESX Server 2 noch notwendig war.

Wenn der Host nur über zwei Netzwerkkarten verfügt, lassen sich dadurch brachliegende Ressourcen des Adapters der Service Console einigen VMs zur Verfügung stellen, und ein Test-Host kann sogar mit nur einer Netzwerkkarte betrieben werden.



### Zugriff auf Datenträger und externen Speicher

Das Gleiche wie für die Netzwerkkarten gilt in Sachen Ausfallsicherheit für den SAN-Zugriff. Der ESX Server unterstützt *Multipathing*, um zu einem bestimmten externen Speicher mehrere redundante Wege bereitzustellen. Fällt z.B. ein Fibre-Channel-HBA im Host aus, kann ein Ersatzadapter weiterhin die Kommunikation aufrechterhalten.

#### Hotplug von virtuellen Platten

Eine neue Funktion von ESX Server 3 ist die Möglichkeit, virtuelle Platten im laufenden Betrieb einem Gast hinzuzufügen (*Hotplug*), um damit beispielsweise Kapazitätsengpässe ohne das Herunterfahren des Gastsystems zu beheben. Das Gastsystem muss natürlich einen nachträglich hinzugefügten Datenträger erkennen, bei Windows erfolgt das beispielsweise über die Datenträgerverwaltung mit einem Neueinlesen der Festplatten.

#### Boot from SAN

Wie bereits weiter oben erwähnt, können Gäste unter dem ESX Server direkt auf eine LUN im SAN zugreifen (*Raw Device Mapping*). Zu guter Letzt kann der ESX Server selbst direkt auf einer SAN-LUN installiert werden und von dieser booten (*boot from SAN*), wodurch Sie auf lokale Platten völlig verzichten können. Das ist z.B. beim Einsatz von Blade-Servern interessant. Dadurch lässt sich die ESX-Basisinstallation sogar über das SAN sichern, etwa mit SAN-Snapshots. Allerdings ist grundsätzlich die Systeminstallation des ESX Servers auf eine lokale Festplatte mit Spiegelung oder Raid5 empfehlenswerter, um zur Fehlersuche den ESX Server auch ohne SAN starten zu können.

## 9.2 Editionen von ESX Server 3 – Starter, Standard und Enterprise

Alle herausragenden Funktionen des ESX Servers haben auch ihren Preis. Sie müssen sich entscheiden, ob Sie nur eine Testumgebung aufsetzen wollen oder ein hochverfügbares Rechenzentrum konzipieren. Für eine Testumgebung bzw. für die Virtualisierung einiger weniger Maschinen ist eine moderate Hardware mit dem kostenlosen VMware Server oftmals schon ausreichend und vor allem beim Einstieg auch handlicher.

Zusätzlich zum Kaufpreis der reinen Software des ESX steht zu bedenken, dass die meisten der besonderen Funktionen der Virtual Infrastructure 3 erst mit externem Speicher möglich werden und dass der ESX Server im produktiven Umfeld nur auf zertifizierter Hardware betrieben werden sollte. Der hohe Aufpreis für die Anschaffung eines SAN wird durch die Unterstützung preiswerterer Technologien, wie iSCSI, in kleinen Umgebungen zwar gemildert, es entstehen aber trotzdem Zusatzkosten.

Die VMware Infrastructure 3 ist in drei Editionen erhältlich, die vom Einsteiger bis zum Rechenzentrum alles abdecken. Die Editionen unterscheiden sich durch die mitgelieferten und lizenzierten Module und natürlich im Preis. Zusätzlich muss mindestens einmal der Virtual Center Management Server lizenziert werden, wenn Sie Funktionen des Virtual Centers (VMotion HA, DRS usw.) nutzen wollen.

### **VMware Infrastructure Starter**

Diese Edition enthält im Grunde genommen nur einen beschnittenen ESX Server 3, ohne Features wie VMotion, VMware HA, VMware DRS oder Consolidated Backup. Noch dazu fehlt die Möglichkeit, auf externen Speicher über Fibre-Channel oder iSCSI zuzugreifen. Als externer Speicher kann nur ein NAS verwendet werden, damit entfällt die Möglichkeit, Cluster über unterschiedliche Hosts zu konfigurieren. Maximal kann die Starter Edition 8 GB RAM und bis zu vier CPUs im Host verwenden, allerdings ohne Virtual SMP für die Gäste. Übrig bleibt ein leicht eingeschränkter ESX Server mit sehr guter Performance, mit allen Möglichkeiten zur Ressourcenkontrolle der Gäste und mit der Option zur Verwaltung über Virtual Center. Nutzer eines vorhandenen GSX Servers mit aktiver Subskription können kostenlos auf die Starter Edition wechseln, müssen dazu aber ein Jahr Support mitkaufen – ganz kostenlos geht es also nicht.

### **VMware Infrastructure Standard**

Die Standard Edition enthält einen vollwertigen ESX Server ohne Einschränkungen, allerdings fehlen die Lizenzen für die erweiterten Funktionen VMotion, VMware HA, VMware DRS oder Consolidated Backup. Diese können je nach Bedarf später einzeln nachgekauft werden. Der gemeinsame Zugriff auf externen VMFS Speicher und auch Cluster zwischen den Gästen sind mit der Standard Edition bereits in vollem Umfang möglich, ebenso die Einbindung zur Verwaltung ins Virtual Center.

### **VMware Infrastructure Enterprise**

Die Enterprise Edition enthält neben einem vollwertigen ESX Server alle beschriebenen Module und Funktionen in der vollen Ausbaustufe bis auf den Virtual Center Management Server, der immer einmalig zusätzlich erworben werden muss.

### **Lizenzierung aller Editionen pro zwei CPUs**

Die Lizenzierung erfolgt jeweils pro zwei Prozessoren, wobei nur physische CPUs gelten (pro Sockel). Das bedeutet, dass ein Host mit zwei Dualcore-CPU's inkl. Hyperthreading nur als Maschine mit zwei CPUs zu lizenzieren ist, obwohl unter VMware acht logische Prozessoren auftauchen (zwei CPUs mal zwei Kerne nochmals verdoppelt).



durch Hyperthreading). Zum reinen Kaufpreis muss mindestens ein Jahr Support miterworben werden, was je nach gewählter Stufe zusätzlich mit ein paar hundert Euro zu Buche schlägt. Ein Virtual Center Management Server ist ebenfalls separat zu lizenzieren, er ist in keiner der Editionen enthalten, nicht zu verwechseln mit dem Virtual Center Agent.

## 9.3 Den ersten ESX Server installieren und einrichten

### Voll funktionsfähige Evaluierungsversion

Sie wissen jetzt, was Sie vom ESX Server erwarten können, also schauen wir uns den Einsatz des Produktes einmal praktisch an. Sie können eine Evaluierungsversion direkt bei VMware beziehen, zu den Links und der Vorgehensweise der Lizenzierung komme ich im Detail weiter unten. Wenn Sie bereits mit der VMware Workstation oder dem kostenlosen VMware Server in das Thema eingestiegen sind, haben Sie sich in die Grundlagen virtueller Maschinen schon gut eingearbeitet. Ich werde in diesem Kapitel deshalb nur noch sehr knapp darauf eingehen, was z.B. ein virtueller Switch ist.

Dank des neuen Virtual Infrastructure Clients ist der Umstieg von einem Hosted-Produkt auf den ESX Server 3 nicht mehr ein so starker Schnitt wie noch beim ESX Server 2. Trotzdem tut sich eine andere Welt auf, in der Sie sich erst einmal umsehen müssen. Wie bereits im Vorwort zu diesem Kapitel erwähnt, kann ich hier unmöglich die gesamte Funktionalität der Virtual Infrastructure 3 abhandeln. Ich beschränke mich auf einen einzelnen ESX Server 3, der auf lokalen Festplatten installiert ist und zusätzlich externen VMFS-Speicher über den integrierten iSCSI Software Initiator oder über Fibre-Channel verwendet.

Dieser Workshop klärt die häufigsten Probleme von der Installation der Lizenzen über das Freischalten des iSCSI Initiators bis zum Datenaustausch mit dem ESX Server im Windows-Netz. Sind diese ersten Klippen umschifft, steht einem selbstständigen Erforschen aller weiteren Funktionen nichts mehr im Wege. Einige Bemerkungen zur Installation des Virtual Center Management Servers und zu dem anschließenden Einbinden Ihres neuen Hosts schließen den Workshop ab. Für weitergehende Studien finden Sie die gesamte Dokumentation inkl. Kompatibilitätslisten (*Compatibility Guides*) zur unterstützten Hardware auf den VMware-Webseiten:

[www.vmware.com/support/pubs/vi\\_pubs.html](http://www.vmware.com/support/pubs/vi_pubs.html)

[www.vmware.com/pdf/vi3\\_esx\\_quickstart.pdf](http://www.vmware.com/pdf/vi3_esx_quickstart.pdf)

Sie können auch ohne eigene Hardware alle Funktionen der Virtual Infrastructure 3 ausgiebig testen. Der Schweizer Urs Stephan Alder stellt mit seiner Firma Kybernetika ein Testcenter zum Remotezugriff über das Internet bereit. Mittels RDP-Verbindung auf einen Client im Rechenzentrum können Sie tageweise eine vollständige Infrastruktur mit mehreren Servern, SAN-Speicher und Gigabit-Ethernet mieten. Nach einer Einweisung können Sie die vorinstallierten Server nutzen oder auch selbst Installationen auf der Hardware durchführen. Alle VMware Features, etwa VMotion und auch Zusatzsoftware wie esxRanger, lassen sich auf diese Weise auf einer Hardware-Ausstattung evaluieren, die nicht in jeder Testumgebung zur Verfügung stehen dürfte. Eine interessante Alternative für erste eigene Erfahrungen oder Vorbereitungen.

<http://www.kybernetika.ch>



### 9.3.1 Voraussetzungen zur Installation

Zuerst benötigen Sie eine Hardware-Basis, auf welcher der ESX Server läuft. Wenn Sie nicht bereits über einen Server mit unterstützter Hardware verfügen, können Sie sich ein erstes Evaluierungsgerät mit preiswerten Komponenten bestücken – Empfehlungen finden Sie gleich im Anschluss. Wollen Sie externen Speicher über iSCSI oder NAS anbinden, sollten Sie über eine Gigabit-Netzwerkverbindung verfügen, um nicht ungerechtfertigt einen schlechten Eindruck von der Leistung zu bekommen. Auf externen Speicher können Sie auch ganz verzichten, dann muss das Testgerät aber über einen unterstützten SCSI-Controller mit SCSI-Festplatten verfügen, und Sie können VMotion, VMware HA oder DRS nicht testen.

Bei ernsthaften Überlegungen, den ESX Server einzusetzen, sollten Sie unbedingt unterstützte Hardware einsetzen, wenn möglich bereits für Ihre ersten Tests. Ich kenne allerdings auch die Situation in Testumgebungen: Gerade in dem Moment, wenn man einmal Hardware benötigt, um etwas zu probieren, ist keines der vorhandenen Geräte abkömmlich. Mit einer Minimalkonfiguration, bestehend aus einer Intel-Ethernet-Karte, einer IDE- oder SCSI-Festplatte und externem Speicher auf iSCSI-Basis (z.B. Starwind aus dem Cluster-Workshop in Teil 2, Kapitel 8, *„Cluster mit VMs und einem iSCSI-Target als externem Speicher“*), können Sie bereits fast alle Funktionen der Virtual Infrastructure 3 testen. Lediglich Cluster über mehrere Hosts mittels *Raw Device Mapping* und Consolidated Backup verlangen eine Fibre-Channel-Anbindung. Aussagen zur Performance lassen sich mit einer solchen Testumgebung allerdings nicht treffen, und bei Problemen sollten Sie unbedingt unterstützte Hardware verwenden, bevor Sie den Fehler bei VMware suchen.

**Testumgebung  
einrichten**



In produktiven Umgebungen sollten nur von VMware unterstützte Server- und Speichersysteme zum Einsatz kommen.

Hier finden Sie Vorschläge für Ausbaustufen eines ESX Servers. Beachten Sie dabei, dass während der Installation nur kompatible Hardware vom ESX Server erkannt wird. Die Hardware-Kompatibilitätslisten können Sie auf den VMware-Seiten zur Virtual Infrastructure (siehe weiter oben) einsehen. Im Zweifelsfalle hilft ausprobieren. Um einen realistischen Eindruck von der Performance des ESX Servers zu bekommen, sollten Sie unbedingt eine höhere Ausbaustufe für den Host wählen.

### Minimales Testgerät für den ESX Server 3

Diese vorgestellte Konstellation stellt nur eine minimale Notlösung dar, um einen Blick auf den ESX Server zu werfen. Sie können aber bereits mit wenigen VMs arbeiten.

- ▶ Mindestens 2 GB RAM
- ▶ Mindestens eine CPU mit Hyperthreading (zwei logische CPUs)
- ▶ Ein bis zwei GBit-Netzwerkkarten, zur Not auch nur 100 MBit
- ▶ Eine IDE-Festplatte für die lokale Systeminstallation des Servers (SATA funktioniert nur mit IDE-Emulation, hier hilft nur ausprobieren, besser und viel schneller ist ein preiswerter SCSI-Controller mit SCSI-Platte).
- ▶ Ein zusätzlicher Rechner im LAN mit iSCSI Software Initiator (z.B. Starwind) oder ein NAS mit NFS (z.B. Linux) kann als externer Speicher dienen.

*Alternativ:*

Ein lokaler SCSI-Controller (z.B. Adaptec) mit 2 SCSI-Platten, dafür kein externer Speicher (bei Verzicht auf VMotion usw.)

### Besseres Testgerät für den ESX Server 3

- ▶ 4 GB RAM
- ▶ Zwei physische CPUs oder mindestens eine Dual Core CPU
- ▶ Mindestens zwei GBit-Netzwerkkarten zum Testen der Teaming-Funktionen
- ▶ Eine SCSI-Platte für die lokale Installation des Servers
- ▶ iSCSI- oder Fibre-Channel-HBA für externen Speicher, als Alternative bietet sich auch eine dedizierte Gigabit-Netzwerkkarte für den VMware iSCSI Software Initiator an
- ▶ Freier Speicher im vorhandenen SAN (Fibre-Channel oder iSCSI)

## **Einstiegsgerät für produktiven Einsatz**

- ▶ Nur unterstützte Hardware verwenden
- ▶ Ab 4 GB RAM
- ▶ Zwei oder mehr physische CPUs, idealerweise Dual Core CPUs (bitte erhöhte Lizenzkosten bei mehr als zwei CPU-Sockeln beachten!)
- ▶ Drei oder mehr GBit-Netzwerkkarten (empfohlen ist die Trennung von VMotion-Verkehr, Service Console und Adaptern für die Gäste, weiterhin Teaming zur Ausfallsicherheit einplanen)
- ▶ RAID1 oder RAID5 für die lokale Installation des Servers, jeweils mit zusätzlicher Hotfix-Platte zur optimalen Ausfallsicherheit
- ▶ Mindestens ein iSCSI- oder Fibre-Channel-HBA für externen Speicher (zur besseren Ausfallsicherheit unterstützt Fibre-Channel auch Multipathing bei zwei HBAs im Server)
- ▶ Freier Speicher im vorhandenen SAN, ideal (wenn auch sehr teuer) sind zwei gespiegelte redundante SAN-Geräte für beste Ausfallsicherheit
- ▶ Redundante Lüfter und Netzteile im ESX Server
- ▶ USV (unterbrechungsfreie Stromversorgung), möglichst redundant
- ▶ Optional sind eine Fernsteuerung für den Host in Form eines KVM-Switches mit Ethernet-Unterstützung oder Lösungen wie HP iLO nützlich. Damit können Sie in Notfällen den Host auch auf Bios-Ebene fernwarten.

## **Zusätzlich benötigte Geräte für die Virtual Infrastructure 3**

Zusätzlich zum Server benötigen Sie mindestens einen LAN-Client, auf dem Sie den Virtual Infrastructure Client zur Verwaltung installieren können.

Für die Installation des Virtual Center Management Servers ist ein weiterer Rechner vorzusehen, zum Testen genügt bereits ein PC oder sogar eine virtuelle Maschine, z.B. auf einem bereits vorhandenen VMware Server. Der Infrastructure Client und der Management Server können auf dem gleichen PC laufen.

Gegebenenfalls kommt für VMware Consolidated Backup ein Server mit Windows 2003 hinzu, der Zugriff auf das SAN über einen Fibre-Channel-HBA haben muss.



Wenn Sie mehrere ESX Server mit der Hochverfügbarkeitslösung VMware HA betreiben, können Sie den Virtual Center Management Server in einer VM auf der ESX Server-Farm installieren, ohne einen dedizierten physischen Rechner zu verwenden. Damit sparen Sie die Hardware und haben für das Management eine ausfallsichere Lösung. Dazu müssen Sie sich vorerst mit dem VI Client direkt auf einen ESX Server verbinden, um die erste VM einzurichten, in der dann Virtual Center installiert werden kann.

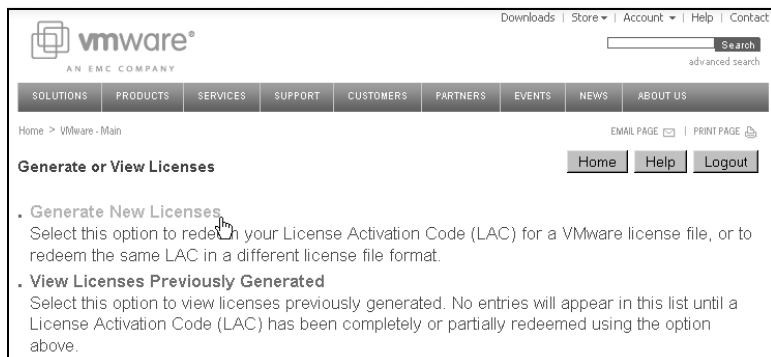
### 9.3.2 Evaluierungssoftware und Lizenzen bei VMware anfordern

Über die Webseite [www.vmware.com/download/vi/](http://www.vmware.com/download/vi/) können Sie sich über den Button EVALUATE für eine 30 Tage lauffähige Evaluierungsversion der VMware Infrastructure 3 registrieren. Sie benötigen dazu ein Nutzerkonto bei VMware, sollten Sie noch keines haben, dann lässt sich auf der Registrierungsseite über den Button REGISTER gleich ein neues Konto anlegen. Nach der Anmeldung bekommen Sie per Mail einen Link zur Download-Seite der Software und einen *License Activation Code*, der lediglich zum Aktivieren der Lizenz und zum Erzeugen einer Lizenzdatei dient.

#### Lizenzdatei über das Internet erzeugen, Host Based oder License Server Based

Ganz gleich, ob Sie eine Evaluierungsversion anfordern oder das Produkt kaufen, Sie müssen auf einer Webseite von VMware mit dem Aktivierungscode eine Lizenzdatei erzeugen. Den Link zur Aktivierungsseite erhalten Sie ebenfalls per Mail, bzw. Sie finden ihn auf der oben genannten Webseite unter REDEEM YOUR LICENSE ACTIVATION CODES. Nach erfolgter Anmeldung mit Ihrem VMware Konto und der Auswahl der einzulösenden Lizenzen können Sie mittels GENERATE NEW LICENSES eine neue Lizenzdatei erstellen (Abbildung 9.3). Bereits erzeugte Lizenzdateien lassen sich mittels VIEW LICENSES PREVIOUSLY GENERATED erneut herunterladen.

Abbildung 9.3:  
Auf der Webseite  
von VMware kann  
eine neue Lizenz-  
datei erzeugt und  
heruntergeladen  
werden



Die über GENERATE NEW LICENSES erstellte Lizenzdatei können Sie sich anschließend per E-Mail an Ihre Adresse senden, direkt herunterladen oder per Cut&Paste als Inhalt in eine leere Textdatei kopieren. Sie benötigen die erzeugte Datei später, wenn Ihr ESX Server installiert ist.

VMware unterscheidet zwei Arten von Lizenzen. *Host Based* bedeutet, die Lizenz wird direkt auf einem ESX Server installiert. Damit können Sie unkompliziert einen allein stehenden Server testen. Eine *License Server Based*-Lizenz müssen Sie auf einem eigens installierten Lizenzserver hinterlegen, der dann von allen ESX-Hosts und vom Virtual Center abgefragt wird. Dieser Lizenzserver läuft als Dienst auf einem Windows-Rechner. Sollten Sie irgendwann nach der gewünschten Art Ihrer Lizenz gefragt werden, wählen Sie am besten immer *License Server Based*, für Virtual Center benötigen Sie sowieso einen Lizenzserver. Nur wenn Sie auf lange Sicht mit einzeln stehenden Servern ohne Virtual Center arbeiten, ist die Verwaltung einer *Host Based*-Lizenz einfacher. Bei der Evaluierung werden immer *License Server Based*-Lizenzen generiert, die Option *Host Based* steht nicht zur Verfügung.



## Software für ESX 3 und Virtual Center 2 herunterladen

Ebenfalls über die Evaluierungswebseite können Sie das ISO-Image des ESX Servers 3 und eine ZIP-Datei mit dem Setup des Virtual Centers 2 herunterladen. Dazu müssen Sie über gültige registrierte Lizenzen oder über eine erteilte Evaluierungslizenz verfügen. Das ISO-Image des Servers brennen Sie nach dem Download auf eine CD.

### 9.3.3 Installation des ESX Servers

Mit der bootfähigen Setup-CD starten Sie den angehenden ESX Server. VMware stellt für die Installation wahlweise eine grafische oder eine textbasierte Oberfläche bereit (Abbildung 9.4).

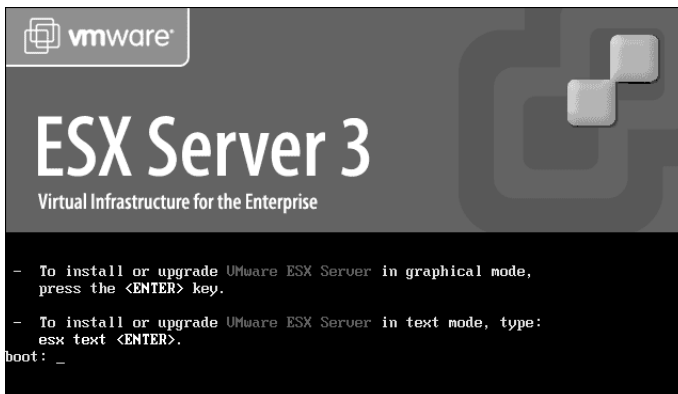


Abbildung 9.4:  
Der ESX Server kann  
mit einer grafischen  
Setup-Routine oder  
textbasiert installiert  
werden

Nach dem Bestätigen des Begrüßungsbildschirms mit  werden Sie gefragt, ob Sie Ihre Installations-CD prüfen lassen wollen. Sollten Sie Ihrer Internetanbindung und dem heruntergeladenen Image nicht trauen, dann tun Sie das. Gleich darauf beginnt die menügeführte Installation mit der Auswahl der Sprache und der Eingabegeräte wie Maus und Tastatur. Interessant wird es erst bei der Auswahl des Datenträgers, auf dem der ESX Server installiert werden soll (Abbildung 9.5).

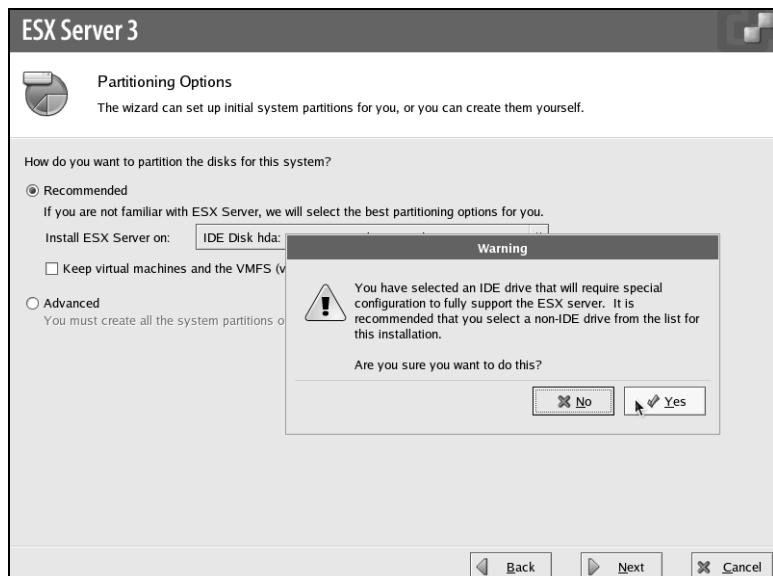


Wählen Sie eine leere unbenutzte Platte, die Daten darauf gehen verloren, wenn Sie die automatische Partitionierung verwenden!

Wenn der ESX auf Ihrem Testgerät keine Festplatten findet, dann wird Ihr Controller wahrscheinlich nicht unterstützt, und Sie müssen sich nach anderer Hardware umsehen, z.B. einem preiswerten Adaptec SCSI Controller. Schauen Sie vorher in die Hardware-Kompatibilitätsliste. Trotz immer wieder zu lesender Behauptungen – Linux-Treiber nützen Ihnen auf dem ESX Server nichts, VMware liefert eigene Treiber für den VMkernel.

Sollten Sie eine IDE-Platte verwenden, dann erscheint ein Warnhinweis, den Sie mit OK bestätigen können (Abbildung 9.5). Auf IDE-Platten lassen sich keine VMFS-Partitionen anlegen, das müssen Sie später auf einem unterstützten externen Speicher nachholen, in unserem Testbeispiel auf einem iSCSI-Target. Wenn Sie auf eine lokale SCSI-Platte installieren, auf der von früheren Installationen bereits virtuelle Maschinen auf VMFS-Partitionen liegen, können Sie diese mit dem Haken an KEEP VIRTUAL MACHINES AND THE VMFS... erhalten.

Abbildung 9.5:  
Der Systemdaten-  
träger kann zu Test-  
zwecken eine IDE-  
Platte sein, besser ist  
aber ein SCSI- oder  
RAID-Controller im  
ESX Server



VMware macht für den weiteren Vorgang bereits Vorgaben, z.B. zur Partitionierung der Festplatte (Abbildung 9.6). Es kursieren viele Vorschläge zur Optimierung der Partitionsstruktur. Wie bei Linux üblich, sollten z.B. für die Service Console `/tmp` `/var` und `/usr` in separaten Partitionen liegen, etwa um das Vollschieben der wichtigen `root`-Partition von einer überlaufenden Log-Datei zu verhindern. Sie können aber die Vorgaben von VMware übernehmen und sparen sich damit das manuelle Partitionieren.

Wenn Sie den ESX Server testweise auf einer Dual-Boot-Maschine aufsetzen, dann sollten Sie im darauf folgenden Bildschirm bei der Auswahl der Bootmethode FROM A PARTITION wählen, um den ESX später in Ihren Bootmanager einbinden zu können.

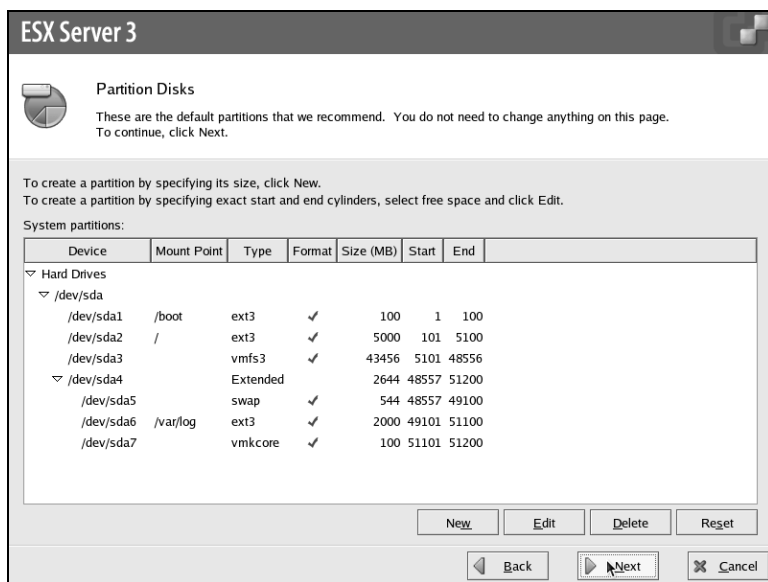


Abbildung 9.6: VMware schlägt eine Partitionierung des Systemdatenträgers bereits vor

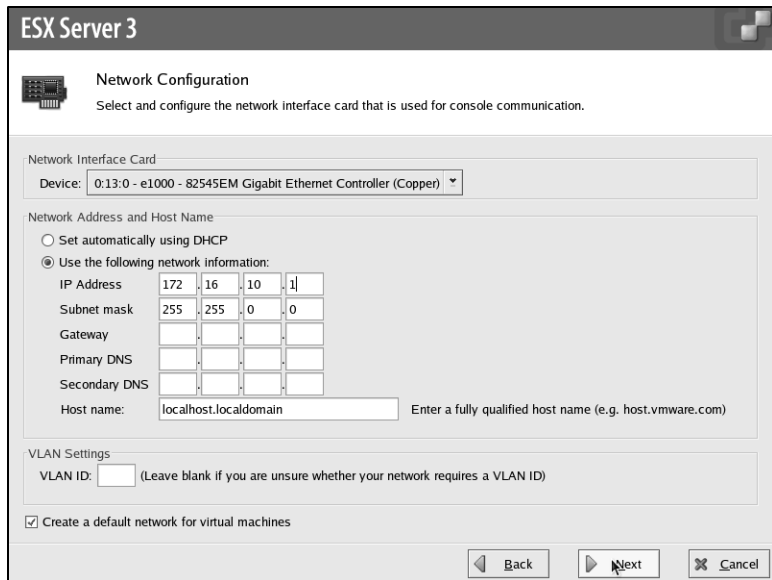
Bei der Konfiguration der Netzwerkkarte sollte eine feste IP-Adresse Verwendung finden (Abbildung 9.7), da über DHCP nicht sicher ist, dass der Host immer unter der gleichen Adresse erreichbar bleibt, es sei denn, Sie reservieren auf Ihrem DHCP-Server eine IP-Adresse für den ESX Server. Unter dieser Adresse werden Sie den Host später über das LAN verwalten. Weiterhin können Sie bei HOST NAME anstelle `localhost.localdomain` einen Namen für den ESX Server vergeben. Eine VLAN ID wird im Normalfall nicht gebraucht, GATEWAY und DNS SERVER sind ebenfalls nicht zwingend notwendig.

Nach der Auswahl der Zeitzone und dem Festlegen des Passworts für den Nutzer `root` beginnt das Kopieren der Dateien, und im Anschluss startet der Host neu. Nach dem Neustart begrüßt Sie ein schwarzer Bildschirm mit Versionsnummer und IP-Adresse Ihres neuen ESX Servers. Mit `[ALT] + [F1]` gelangen Sie zur Kommando-



zeile der Service Console, an der Sie sich als *root* anmelden können. Im weiteren Workshop arbeiten wir aber größtenteils mit dem komfortableren Virtual Infrastructure Client, welcher der Dreh- und Angelpunkt der Administration der Virtual Infrastructure 3 ist.

Abbildung 9.7:  
Für den ESX Server  
sollte eine feste  
IP-Adresse verwen-  
det werden



### 9.3.4 Den Virtual Infrastructure Client installieren

An einem LAN-Client rufen Sie in einem Browser mittels `https://mein_host` die Begrüßungsseite des neuen ESX Servers auf. Dort laden Sie mittels **DOWNLOAD THE VIRTUAL INFRASTRUCTURE CLIENT** den Client zur Bedienung des ESX Servers herunter (Abbildung 9.8) und installieren ihn lokal auf dem PC.

Abbildung 9.8:  
Über einen Browser  
kann der Virtual  
Infrastructure Cli-  
ent vom ESX Server  
heruntergeladen und  
installiert werden



Nach dem Starten des Clients können Sie sich bereits als Nutzer *root* mit dem ESX Server verbinden (Abbildung 9.9). Wer bereits Erfahrungen mit den anderen VMware-Produkten gemacht hat, dem ist zumindest die Bedienung der virtuellen Maschinen nicht fremd (Abbildung 9.2). Sie sehen aber auf den ersten Blick, dass der ESX Server eine Vielzahl weiterer Optionen bietet. Bevor Sie im VI Client Ihre ersten VMs erstellen und verwalten können, sind noch einige Handgriffe notwendig.



Abbildung 9.9:  
Als Nutzer *root*  
erhalten Sie im  
VI Client die volle  
Kontrolle über den  
ESX Server

### 9.3.5 Lizenzierung von ESX Server 3

Um überhaupt eine virtuelle Maschine starten zu können, will der ESX Server zuerst lizenziert werden. Sie haben die notwendige Lizenzdatei bereits heruntergeladen. Jetzt kommt es darauf an, welchen Lizenztyp Sie verwenden. Eine *host-based* Lizenz können Sie sofort im VI Client über CONFIGURATION/LICENSCE D FEATURES/LICENSE SOURCES/EDIT auf dem Server installieren (Abbildung 9.10).

Wenn Sie sich nicht sicher sind, welche Art von Lizenz Sie besitzen, dann probieren Sie zuerst, die Lizenzdatei als *host-based* am ESX zu registrieren. Gelingt das nicht, dann müssen Sie einen Lizenzserver einrichten. Evaluierungslizenzen sind immer *server-based*.



#### Installation des Lizenzservers auf einem Rechner im LAN

Für eine Lizenz vom Typ *server-based* benötigen Sie einen Lizenzserver, der standardmäßig bei der Installation des Virtual Center Management Servers mit eingerichtet wird. Sie können vorerst auch nur den Lizenzserver allein aufsetzen, ohne gleich Virtual Center zu installieren. Dazu befindet sich im heruntergeladenen ZIP-Archiv, oder auf der CD von Virtual Center, im Verzeichnis *bin* die Datei *VMware-lisencesserver.exe*, die Sie auf einem PC installieren. Die Installation ist simpel, das Setup fragt nur nach dem Standort Ihrer Lizenzdatei. Diese Datei sollte in einem lokalen Verzeichnis liegen, auf das der Lizenzserver permanent Zugriff hat. Kopieren Sie die Lizenzdatei vor der Installation des Lizenzservers dorthin.

Abbildung 9.10:  
Nach dem Einrichten  
des Lizenz-  
servers stehen alle  
lizenzierten Funkti-  
onen zur Verfügung



### Eintragen der Lizenzen am ESX Server

Wenn Sie sich zum Lizenzserver verbunden haben, können Sie alle Komponenten auf folgende Weise lizenzieren:

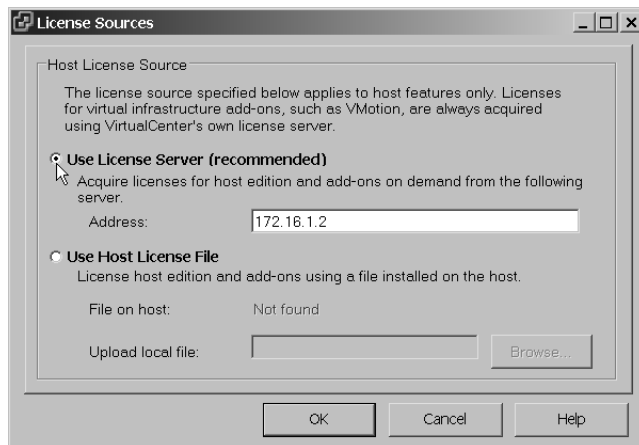
1. Tragen Sie im Virtual Infrastructure Client über CONFIGURATION/LICENSCEDED FEATURES/LICENSE SOURCES/EDIT die Adresse des Lizenzservers ein (Abbildung 9.11).
2. Wählen Sie über ESX SERVER LICENSE TYPE mittels EDIT (Abbildung 9.10) den Typ Ihrer Lizenz aus, Starter oder Standard.



Die höchste angebotene Stufe im Lizenzierungsdialog ist immer ESX Server Standard, wählen Sie diese auch dann, wenn Sie eine Enterprise Edition erworben haben. Die Komponenten der Enterprise Edition, wie VMotion, DRS und HA, können nur im Virtual Center lizenziert werden.

3. Zum Abschluss können Sie über ADD-ONS mittels EDIT (Abbildung 9.10) eventuelle Zusatzkomponenten, wie etwa Consolidated Backup, freischalten. VMotion, DRS und HA werden erst später über das Virtual Center lizenziert.

Abbildung 9.11:  
Die Verwendung  
eines Lizenzservers  
ist die empfohlene  
Methode



Bei der Starter-Edition der VMware Infrastructure 3 ist kein externer Speicher über iSCSI oder Fibre-Channel lizenziert, was bedeutet, dass Sie die Konfiguration des iSCSI Initiators in diesem Workshop nicht durchführen können. Sollten Sie vom GSX Server ein kostenloses Upgrade durchgeführt haben oder aus anderen Gründen nur über eine Starter-Edition verfügen, können Sie sich trotzdem für eine Evaluierungsversion registrieren, um alle anderen Funktionen zu testen.



### 9.3.6 Anlegen des VMFS-Dateisystems auf einem externen oder lokalen Datenträger

Wie bereits erwähnt, können die virtuellen Platten der Gäste nur auf dem Dateisystem VMFS oder auf einem externen NAS liegen. Bevor Sie Ihre erste virtuelle Maschine auf dem ESX Server erstellen, ist zuerst dieser Datenspeicher zu konfigurieren. Wir verwenden im Workshop den integrierten Software iSCSI Initiator des ESX, um auf externen Speicher zuzugreifen, weshalb zuerst einige Schritte zur Konfiguration des Initiators notwendig sind. Für die Verwendung eines NAS sollten Sie folgende Schritte für die Konfiguration des Netzwerks ebenfalls beachten.

**iSCSI Software Initiator für die Testumgebung**

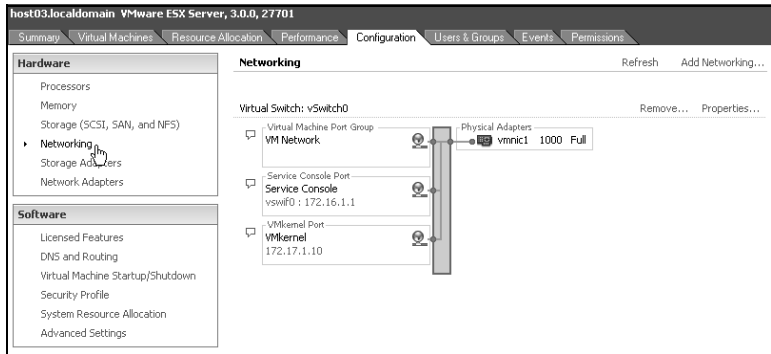
Wenn Sie nur lokalen Speicher verwenden, also SCSI-Festplatten oder ein RAID-System, bzw. wenn im Server ein Hardware-Initiator für iSCSI oder ein Fibre-Channel-HBA eingebaut ist, dann können Sie den folgenden Schritt der Netzwerkkonfiguration überspringen und gleich bei „Anlegen und Erweitern von VMFS-Datenspeichern auf lokalen oder externen Datenträgern“ weiterlesen.

**Lokalen SCSI-Speicher oder HBA verwenden**

#### Vorbereitungen für die Verwendung des iSCSI Software Initiators oder eines NAS

Der iSCSI Software Initiator des ESX Servers, der im Workshop zum Einsatz kommt, muss über eine physische Netzwerkkarte mit dem Target (z.B. ein SAN) im Netzwerk kommunizieren können. Zur gesamten Netzwerkfunktionalität des ESX Servers gehe ich weiter unten detaillierter ein, hier wird vorläufig nur der iSCSI-Zugriff realisiert. Da der Initiator als Dienst im VMkernel läuft, benötigt der Kernel dazu eine Verbindung mit einem virtuellen Switch. Über eine physische Netzwerkkarte, die diesem Switch zugeordnet ist, erfolgt dann die Kommunikation mit dem LAN (Abbildung 9.12). Auf die gleiche Art und Weise, nämlich über einen virtuellen Switch, erreichen bei allen anderen Virtualisierungsprodukten nur die Gäste das LAN (siehe *Teil 3, Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“*). Die Besonderheit beim ESX Server liegt darin, dass das Hostbetriebssystem (VMkernel) ebenfalls den Weg über virtuelle Switches zur Kommunikation verwendet.

Abbildung 9.12:  
In der einfachsten  
Variante kommunizieren alle Gäste und Dienste über eine gemeinsame Netzwerkkarte am gleichen Switch



Die Installationsroutine des ESX Servers hat bereits einen Switch mit einer physischen Netzwerkkarte angelegt, an dem die Gäste und die Service Console angeschlossen sind (Abbildung 9.12). Vorerst verwenden Sie den gleichen Switch auch für den iSCSI- bzw. NAS-Verkehr (VMkernel). Das ist für die Performance nicht optimal, aber die Netzwerkkonfiguration mit ihren vielen Optionen ist ein eigenes Kapitel wert, das weitere Möglichkeiten aufzeigt. Haben Sie in Ihrem Testserver nur eine Netzwerkkarte zur Verfügung, ist die gemeinsame Verwendung sowieso die einzige mögliche Variante. Verfügt der Host über mehrere physische Netzwerkkarten, können Sie später einen davon dediziert nur für die iSCSI-Verbindung reservieren.



Ist Ihr Speichernetzwerk für das SAN physisch vom Datennetzwerk (LAN) getrennt, dann müssen Sie schon jetzt einen separaten Switch mit eigener physischer Netzwerkkarte konfigurieren, weil der Adapter für den iSCSI-Verkehr wahrscheinlich an einen anderen physischen Switch angeschlossen wird als der Adapter für die Gäste und für die Service Console.

#### Netzwerkverbindung für VMkernel herstellen

Folgendermaßen können Sie die Netzwerkverbindung für den iSCSI Initiator oder für ein NAS einrichten:

1. Zuerst müssen Sie in der Firewall, die den ESX Server schützt, den Port für den iSCSI- bzw. NFS-Client (NAS) öffnen. Unter SECURITY PROFILE/PROPERTIES finden Sie die Einstellungen (Abbildung 9.13).
2. Jetzt können Sie mittels NETWORKING/ADD NETWORKING einen Port für den VMkernel zum Switch vSwitch0 hinzufügen oder einen neuen Switch erstellen.
3. Wählen Sie im ersten Dialog VMKERNEL, und bestätigen Sie mit NEXT.
4. Wählen Sie USE VSWITCH0, um den vorhandenen Switch mitzubenutzen, z.B. wenn Sie nur eine Netzwerkkarte zur Verfügung haben. Für ein separates Speichernetzwerk erstellen Sie dagegen mit CREATE A VIRTUAL SWITCH einen neuen Switch, um eine dedizierte Netzwerkkarte für die iSCSI-Verbindung einsetzen zu können.

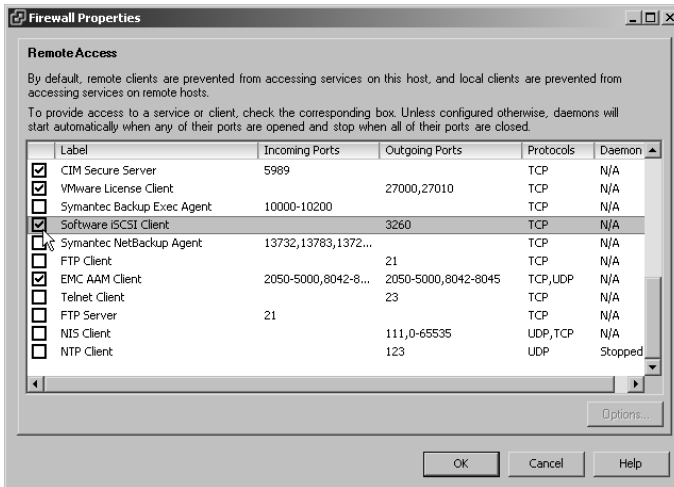


Abbildung 9.13:  
Für die Kommunikation mit dem Netzwerk müssen verschiedene Ports der Firewall geöffnet werden

- Lassen Sie als NETWORK LABEL die Vorgabe *VMkernel* stehen und vergeben Sie eine IP-Adresse mit passender Subnetzmaske, unter der die Dienste des Kernels mit dem LAN kommunizieren sollen. Im Falle des iSCSI Initiators muss das eine Adresse aus Ihrem LAN oder aus dem Speichernetz sein, unter der das iSCSI Target ansprechbar ist (Abbildung 9.14).

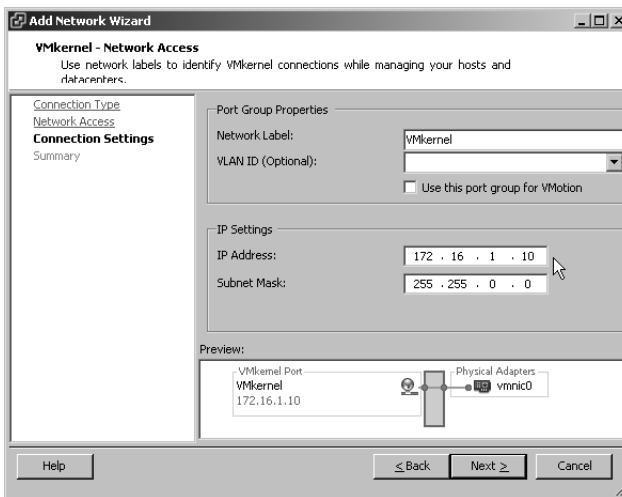


Abbildung 9.14:  
Für Dienste des Kernels, unter anderem iSCSI, muss ein eigener Port an einem Switch mit physischem Adapter angelegt werden

- Die Meldung zum fehlenden Default Gateway können Sie ignorieren, wenn sich Ihr iSCSI-Target im gleichen Netzwerk wie der physische Adapter befindet. Wenn nicht, dann müssen Sie die Adresse des Routers angeben, über den der Verkehr ins Speichernetz gelangt. Das dürfte nur in Testumgebungen relevant sein.

Wenn Sie den schon vorhandenen Switch VSWITCH0 der Service Console mitverwenden, ist die Netzwerkkonfiguration damit bereits beendet (Abbildung 9.12). Haben Sie einen neuen Switch erstellt, dann sind noch zwei weitere Schritte notwendig:

1. Wählen Sie am neuen Switch *VSwitch1* **PROPERTIES/NETWORK ADAPTERS**, und weisen Sie eine freie physische Netzwerkkarte zu, die dann ausschließlich für den iSCSI-Verkehr reserviert ist.



Verwenden Sie auf keinen Fall den Adapter, der bereits dem Switch der Service Console zugewiesen ist, sonst können Sie nicht mehr mit dem Server über das LAN kommunizieren!

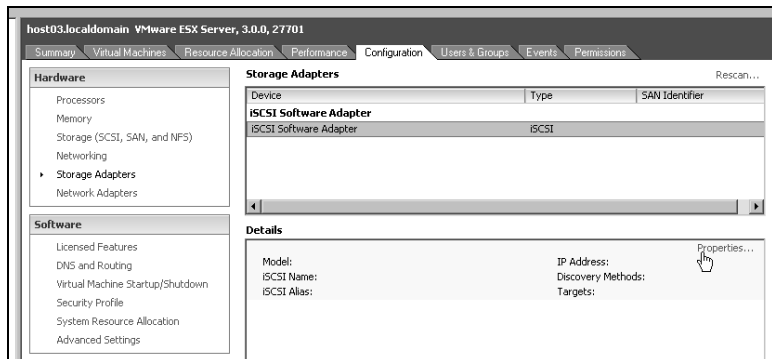
2. Der neue Switch benötigt weiterhin eine zusätzliche Verbindung zur Service Console, da iSCSI auch eine Komponente in der Konsole verwendet. Fügen Sie dazu unter **PROPERTIES/ADD** dem neuen Switch *VSwitch1* einen weiteren Port für die Service Console hinzu, die Service Console kann gleichzeitig mit mehreren Switches verbunden sein. Geben Sie diesem neuen Port der Service Console eine freie Adresse aus dem Bereich des Speichernetzwerks (nicht aus dem Bereich Ihres LAN).

Damit ist das Netzwerk vorbereitet, Sie können die Verbindung zum iSCSI-Target oder auch zu einem NAS konfigurieren.

### Konfiguration des iSCSI Initiators oder eines HBA zum Zugriff auf das SAN

Um auf externen Speicher zugreifen zu können, ist es notwendig, den entsprechenden Adapter im Server zu konfigurieren. Ich zeige Ihnen das am Beispiel des iSCSI Initiators, grundsätzlich ist die Vorgehensweise auch bei einem Hardware-Initiator oder bei einem Fibre-Channel HBA ähnlich.

Abbildung 9.15:  
Ohne lokale SCSI-  
Platte oder HBA  
erscheint nur der  
iSCSI Software  
Initiator des ESX  
Servers in der  
Auswahl



Unter STORAGE ADAPTERS sehen Sie alle erkannten physischen SCSI-, iSCSI- sowie Fibre-Channel-Adapter und auch den Software iSCSI Initiator, jedoch keine IDE Platten (Abbildung 9.15). Wenn ein Gerät nicht in der Liste auftaucht, können Sie den Server mittels RESCAN neu suchen lassen. Die Konfiguration erfolgt beim iSCSI Software Initiator folgendermaßen:

1. Klicken Sie auf den Initiator in der Liste.
2. Wählen Sie im unteren Fenster PROPERTIES.
3. Wählen Sie GENERAL/CONFIGURE, setzen Sie den Haken bei ENABLED, und bestätigen Sie mit OK.
4. Wechseln Sie zum Reiter DYNAMIC DISCOVERY/ADD, und tragen Sie hier die Adresse und den Port Ihres Targets ein, auf dem Sie freien Platz zur Verfügung haben. Der vorgegebene Standard-Port ist in den meisten Fällen richtig 3260 (Abbildung 9.16).

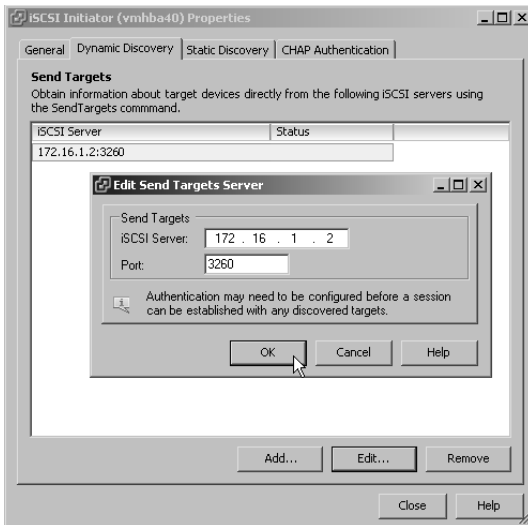


Abbildung 9.16:  
Der Initiator muss mit einem bestimmten Target kommunizieren können, um später die LUNs zu sehen

5. Gegebenfalls müssen Sie unter dem Reiter CHAP AUTHENTICATION die Anmeldedaten für Ihr Target hinterlegen.
6. Sie können die Konfiguration mit CLOSE verlassen.
7. Nach einem erneuten RESCAN und einem Klick auf den Adapter werden die verfügbaren LUNs des Targets im unteren Teil des Fensters angezeigt. Voraussetzung ist, das Target verfügt über freigegebene LUNs. Verwenden Sie zum Testen beispielsweise Starwind, müssen Sie dort vorher Freigaben konfigurieren (Vorgehensweise siehe Cluster-Workshop in Teil 2, Kapitel 8, „Cluster mit VMs und einem iSCSI-Target als externem Speicher“).





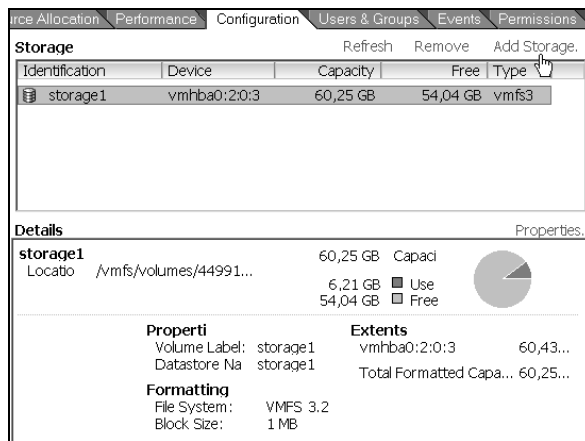
Nach dem Hinzufügen von LUNs in einem SAN müssen Sie an dieser Stelle erst ein RESCAN durchführen, damit die neuen LUNs vom ESX Server erkannt werden. Sollte ein RESCAN nicht genügen, hilft es oft, nochmals auf PROPERTIES/DYNAMIC DISCOVERY zu gehen und den Dialog ohne Änderung einfach zu bestätigen. Dann sollte die neue LUN in der Liste zum Speicheradapter auftauchen.

Ihr externer Speicher steht jetzt zur Verfügung und erscheint auf dem Host wie eine lokal eingebaute Festplatte. Sie können zum Menüpunkt STORAGE (SCSI, SAN, NFS) wechseln und den freien Platz mit dem VMFS-Dateisystem formatieren (Abbildung 9.17).

### Anlegen und Erweitern von VMFS-Datenspeichern auf lokalen oder externen Datenträgern

Unter dem Reiter CONFIGURATION finden Sie das Menü STORAGE (SCSI, SAN, NFS). HIER werden die vorhandenen VMFS-Datenträger, so genannte *Datastores*, angezeigt (Abbildung 9.17). Haben Sie den ESX Server auf eine lokale SCSI-Festplatte installiert, dann wurde der vom System nicht benötigte Plattenplatz bereits automatisch als *storage1* eingerichtet. Über ADD STORAGE führt ein Wizard durch die Erstellung weiterer Datenspeicher, z.B. auf weiteren unbelegten Platten oder neuen LUNs. Der Vorgang unterscheidet sich bei lokalen Festplatten oder externem Speicher nicht.

Abbildung 9.17:  
Freier Datenträger-  
platz kann als eigen-  
er Datastore forma-  
tiert oder einem  
vorhandenen Data-  
store hinzugefügt  
werden



1. Klicken Sie auf ADD STORAGE, und wählen Sie DISK/LUN, um ein VMFS-Volume auf lokalem SCSI-Speicher oder auf einem SAN zu erstellen.
2. VMware zeigt Ihnen alle unbenutzten LUNs und Plattenbereiche an, auf denen ein VMFS-Dateisystem erstellt werden kann. Bleibt diese Liste leer, dann haben Sie entweder keine freien SCSI-Platten

im System oder keine freie LUN im SAN. Sollten freie vorhandene LUNs nicht erscheinen, versuchen Sie nochmals ein RESCAN auf dem Adapter.

Wenn Sie Festplatten mit anderen Partitionen, z.B. NTFS, im Host eingebaut haben, etwa bei Dual-Boot-Maschinen, dann achten Sie unbedingt darauf, keine bereits belegten Platten zu überschreiben. Mit Fremdpartitionen belegte Datenträger erscheinen gemeinsam mit leeren Festplatten und LUNs in der Auswahlliste und könnten komplett mit VMFS formatiert werden!



3. Wenn Sie einen Eintrag auswählen und NEXT anklicken, können Sie einen neuen Datastore erstellen. Vergeben Sie einen passenden Namen, und wählen Sie eine gewünschte Größe. Der Datastore kann auch nachträglich jederzeit erweitert werden, sobald freier Platz vorhanden ist. Bei der Wahl der Blockgröße folgen Sie am besten den VMware-Vorgaben.

Anstelle mit ADD STORAGE ein völlig neues VMFS-Volume zu erstellen, können Sie mittels rechter Maustaste auf einen vorhandene Datastore über PROPERTIES/ADD EXTEND diesem den freien Platz hinzufügen. Ein VMFS-Datastore kann sich über mehrere Datenträger erstrecken.



### Auf den Inhalt von VMFS-Datenträgern zugreifen

Wenn Sie einen Datastore mit der rechten Maustaste anklicken und BROWSE DATASTORE wählen, können Sie den Inhalt des Datenspeichers anzeigen. Allerdings gibt es nur die Option, Dateien und Verzeichnisse zu löschen bzw. vorhandene VMs ins Inventory aufzunehmen. Vollständigen Zugriff zum Kopieren, Ordneranlegen oder Verschieben erhalten Sie entweder an der Kommandozeile der Service Console oder über einen sFTP-Client wie WinSCP (siehe auch Abschnitt 9.4, „Einige Tipps zum Umgang mit dem ESX Server 3“).

Sie können virtuelle Platten von anderen Rechner zwar direkt auf ein VMFS-Volumen kopieren, z.B. mittels WinSCP, danach sind diese allerdings in den meisten Fällen unbrauchbar. Virtuelle Platten müssen importiert oder exportiert werden, mehr dazu unter Abschnitt 9.3.8, „Eine virtuelle Maschine von VMware Server oder Workstation auf den ESX Server übernehmen“.



Alle Datastores sind im Linux-Dateisystem der Service Console im Verzeichnis `/vmfs/volumes` eingebunden, alle Datenträger unter `/vmfs/devices/disks`.

Folgender Befehl zeigt alle Datastores an:

```
ls -l /vmfs/volumes
```

Folgender Befehl zeigt alle physischen Datenträger an:

```
ls -l /vmfs/devices/disks
```

Und mit diesem Kommando sehen Sie die vorhandenen Partitionen:

```
fdisk -l /vmfs/devices/disks/vmhbaA:B:C:D
```

Die Schreibweise, die der ESX Server für die Datenträger verwendet, lautet *vmhbaA:B:C:D* (z.B. *vmhba0:2:0:3*) und setzt sich folgendermaßen zusammen:

- ▶ *A* – (HBA) – physischer Controller, z.B. ein SCSI-/RAID-Controller oder ein Host-Bus-Adapter
- ▶ *B* – (Target) – beispielsweise die Nummer eines RAID-Arrays oder einer SCSI-Platte an einem Controller
- ▶ *C* – (LUN) – die Nummer einer LUN
- ▶ *D* – (Partition) – die Nummer der Partition (z.B. mit NTFS, ext3 oder VMFS) auf dem Datenträger

### 9.3.7 Die erste virtuelle Maschine erstellen und einen Resource Pool anlegen

Jetzt verfügen Sie bereits über eine gute Basis – Sie haben Ihren Server lizenziert, externen Speicher angebunden und einen Ablageplatz für die Gäste mit VMFS formatiert. Sie können über den Reiter SUMMARY mittels NEW VIRTUAL MACHINE Ihre erste VM erstellen. Die Konfiguration und Bedienung eines Gastes unterscheidet sich nur wenig von den Hosted-Produkten, so dass ich hier nicht detailliert darauf eingehen werde. Wer bis hierher vorgedrungen ist, dürfte keine Probleme damit haben. Alle zu VM gehörenden Dateien legt VMware in einem Ordner auf einem VMFS-Datenträger ab, dieser Ordner hat den gleichen Namen, wie Sie beim Anlegen unter VIRTUAL MACHINE NAME für den Gast festlegen.



Der ESX Server kennt keine Zuwachsplatten, er legt virtuelle Platten immer in vollständiger Größe an. Sie benötigen also genügend freien Platz und sollten virtuelle Platten nicht allzu großzügig konfigurieren. Es werden nur virtuelle SCSI-Platten unterstützt.

Wechseln Sie nach dem Erstellen der virtuellen Maschine nochmals zum Menü CONFIGURATION/STORAGE (SCSI, SAN, NFS), dann können Sie mit einem Rechtsklick und der Auswahl BROWSE den Inhalt des Datastores anzeigen. Sie sehen dort Ihre virtuelle Maschine mit allen zugehörigen Dateien in einem separaten Verzeichnis. Hierüber können Sie auch VMs ins Inventory aufnehmen, z.B. nach manuellen Importvorgängen. Es genügt ein rechter Mausklick auf die *vmx*-Datei und ADD TO INVENTORY.

Den Bildschirm eines laufenden Gastes sehen Sie unter dem Reiter CONSOLE, zusätzlich können Sie, mittels rechter Maustaste auf den Inventory-Eintrag der VM, über den Menüpunkt OPEN CONSOLE ein separates Konsolenfenster öffnen. Dieses Fenster lässt sich dann auch skalieren. Einen Vollbildmodus bietet nur die Webkonsole, die Sie über die URL [https://mein\\_host/ui](https://mein_host/ui) erreichen. Sie ermöglicht die Steuerung der Gäste auch ohne VI Client.

Bei installierten VMware Tools funktioniert der gleitende Übergang der Maus in den Gast und zurück, wie Sie es von den Hosts-Produkten gewohnt sind. Einige erweiterte Funktionen der VMware Tools kommen hinzu, z.B. zum kurzzeitigen Einfrieren des Dateisystems NTFS für Consolidated Backup oder zur Speicherverwaltung des Gastes. Sie erkennen die zusätzlichen Optionen bei einer Installation der Tools im Custom-Modus.

Erwähnenswert ist u.a. die Möglichkeit multipler Snapshots, die schon von der VMware Workstation bekannt sind, oder auch die Leistungsauswertung des Gastes über den Reiter PERFORMANCE.

### Mit Resource Pools Leistung an die Gäste verteilen und begrenzen

Eine sehr interessante Funktion des ESX Servers sind sicherlich die Möglichkeiten zur Ressourcenverwaltung für die Gäste. Stellen Sie sich vor, Sie wollen in Ihrer Testumgebung einige Maschinen laufen lassen, um im Pilotversuch eine Migration vorzubereiten. Dabei sollen auf dem gleichen Host laufende produktive Maschinen in ihrer Leistung nicht beeinträchtigt werden. Sie könnten jetzt für jede VM über EDIT SETTINGS/RESOURCES festlegen, wie viel CPU-, RAM- und I/O-Performance einer bestimmten Maschine minimal und maximal zusteht und wie viel von den vorhandenen Ressourcen der Gast prozentual im Verhältnis zu anderen Gästen abfordern darf (*Shares*). Das ist mit mehreren Maschinen aber sehr umständlich.

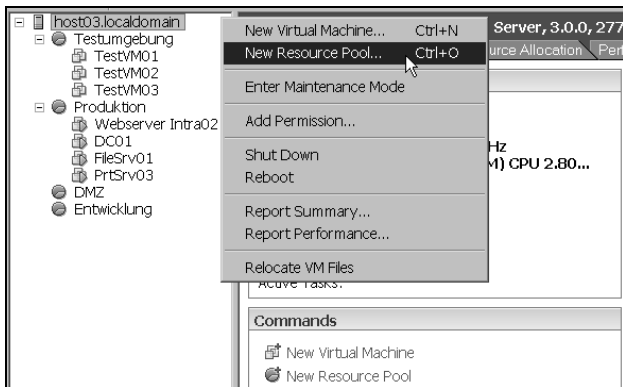


Abbildung 9.18:  
Mit Resource Pools  
können Gruppen  
von VMs in ihrer  
Leistung bevorzugt  
oder begrenzt  
werden

Aus diesem Grunde gibt es das Konzept der Resource Pools. Alle Maschinen in einem solchen Pool erben automatisch die übergreifend definierten Werte. Damit können Sie einen Pool für die Testumgebung erstellen und einen Pool für die Produktionsmaschinen (Abbildung 9.18). Die Maschinen lassen sich flexibel zwischen den Pools verschieben, und die Performancezuweisung erfolgt global für die jeweilige Gruppe. Beispielsweise können Sie in der Testumgebung die CPU-Leistung mit Maximalwerten begrenzen und einen geringeren Wert für die Shares festlegen als für den Produktionspool. Durch höhere Shares haben die Produktionsmaschinen immer Vorrang, wenn die verfügbaren Ressourcen knapp werden, und die Maximalwerte beschränken die Testumgebung grundsätzlich auf eine bestimmte CPU-Leistung. Sie können das praktisch nachvollziehen, indem Sie den Pool der Testumgebung auf maximal 75 MHz CPU-Leistung begrenzen und darin eine virtuelle Maschine mit einem aktuellen Betriebssystem, etwa Windows XP, ausführen.

### 9.3.8 Eine virtuelle Maschine von VMware Server oder Workstation auf den ESX Server übernehmen

Eine neue virtuelle Maschine zu erstellen ist nur die eine Seite der Medaille. Wenn Sie bereits einige Gäste auf anderen VMware-Produkten laufen haben, dann wollen Sie diese sicherlich gleich auf dem ESX Server einsetzen. Wie lassen sich vorhandene VMs auf den ESX Host kopieren und dort ausführen?

- ▶ Beachten Sie grundsätzlich die Hinweise zum Zugriff und zu Kopiervorgängen auf den ESX Server unter *Abschnitt 9.4, „Einige Tipps zum Umgang mit dem ESX Server 3“*.
- ▶ Der ESX Server unterstützt nur virtuelle SCSI-Platten, keine IDE-Platten. Die Platten und die Treiber in den Gästen müssen gegebenenfalls angepasst werden (siehe Platten-Workshop in *Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“*).
- ▶ Der ESX Server legt virtuelle Platten immer in der vollen Größe an. Eine virtuelle Platte von 50 GB belegt auch 50 GB, Zuwachsplatten kennt der ESX Server nicht.
- ▶ Manche Kopiervorgänge auf den ESX Server scheitern an einer Begrenzung der maximalen Dateigröße einiger Protokolle oder Clients, z.B. können Sie von einer SMB-Freigabe und mit manchen FTP-Clients nur Dateien von maximal 2 GB übertragen. Eine sichere Übertragung ermöglicht beispielsweise das Programm WinSCP.
- ▶ Nach dem Übertragen sollten Sie in den Gästen auf dem ESX Server die aktuellsten VMware Tools installieren.

## Der herkömmliche Weg des Importvorganges auf den ESX Server

Virtuelle Maschinen von einem Hosted-Produkt können Sie nicht einfach auf einen VMFS-Datenträger kopieren, etwa mittels WinSCP, weil die virtuellen Platten des Gastes konvertiert werden müssen. In der Vorgängerversion, dem ESX Server 2, war es dazu notwendig, die virtuellen Platten zuerst per FTP oder sFTP auf den ESX Server in eine Linux *ext3*-Partition zu kopieren bzw. auf einer gemounteten SMB-Freigabe im LAN bereitzustellen. Danach wurden die Platten mit dem Kommando `vmkfstools -i` auf der Kommandozeile der Service Console oder über das Web-Interface des ESX Servers 2 auf ein VMFS-Volumen importiert. Im Anschluss konnte eine neue VM mit der importierten Platte erstellt werden. Diesen etwas umständlichen Weg über Kopieren und nachträgliches Importieren der Platten können Sie auch beim ESX Server 3 weiterhin mit dem Kommando `vmkfstools` durchführen, über das Web-Interface ist dagegen kein Import mehr möglich. Die Methode eignet sich vor allem dann, wenn eine große Anzahl virtueller Platten zu übernehmen ist, für Einsteiger ist das sehr umständlich.

Am einfachsten können Sie mit dem *VMware Virtual Machine Importer 2* komplette VMs beliebiger Produkte auf den ESX Server übertragen. Für Ihre ersten Schritte mit dem ESX Server sollten Sie auf den Importer zurückgreifen. Eine weitere Möglichkeit, VMs zwischen den Produkten zu migrieren, wäre VMware Virtual Center.

## Der VMware Virtual Machine Importer 2 vereinfacht den Import-/Exportvorgang von VMs

Der *VMware Virtual Machine Importer 2* vereinfacht den Transfer virtueller Maschinen zwischen den verschiedenen Produkten wesentlich. Zur Drucklegung des Buches befand er sich noch in der Version 2.0 Beta 3, bei Erscheinen der Final sollten Sie im Link den Ordner */beta* weglassen, um zum Download zu gelangen:

[www.vmware.com/products/beta/vmimporter](http://www.vmware.com/products/beta/vmimporter)

Denken Sie beim Import einer VM auf den ESX Server daran, dass die virtuellen Platten auf dem ESX Server immer in voller Größe angelegt werden. Das kann bei allzu großzügig angelegten Zuwachsplatten vom VMware Server oder von VMware Workstation zum Problem werden. Bei Platzproblemen können Sie vor dem Importieren der virtuellen Platte den Inhalt mittels eines Imaging Tools auf eine kleinere virtuelle Platte übertragen und dabei auch gleich die Partition des Gastes verkleinern (siehe Platten-Workshop Teil 3, Kapitel 3).



Zum Übertragen einer virtuellen Maschine vom VMware Server oder von VMware Workstation auf den ESX Server gehen Sie folgendermaßen vor:

1. Starten Sie den Virtual Machine Importer, und wählen Sie **IMPORT A STANDALONE VIRTUAL MACHINE**.
2. Geben Sie die Konfigurationsdatei der Quell-VM an.
3. Wählen Sie als Ziel (*Destination*) **VMWARE ESX SERVER VIRTUAL MACHINE**.
4. Geben Sie den Zielnamen der VM auf dem ESX Server an, und melden Sie sich am Server als *root* an.
5. Wählen Sie einen Datastore auf dem ESX, wo die VM erstellt werden soll, existiert nur einer, wählt ihn der Importer automatisch. Als Ordner für alle Dateien des Gastes wird der Name der Ziel-VM verwendet. Ist dieser Name auf dem ESX Server schon vorhanden, bricht der Importer ab.
6. Für den ESX Server steht nur die Auswahl **CREATE A FULL CLONE** zur Verfügung, nach dem Bestätigen beginnt der Import.
7. Die übertragene VM erscheint im Inventory des ESX Servers und sollte nachträglich noch in einen Resource Pool verschoben werden.



Beim Übertragen übernimmt der Importer auch die Umwandlung der virtuellen Festplatten in SCSI-Platten. Dabei ersetzt der Importer in Windows-Gastsysteme auch die richtigen Treiber für den virtuellen SCSI-Controller, darum müssten Sie sich beim manuellen Kopieren und Importieren selbst kümmern (siehe Platten-Workshop in Teil 3, Kapitel 3).

### Die Geheimnisse des Import-/Exportvorganges auf VMFS-Datenträgern

Warum müssen virtuelle Platten auf VMFS-Datenträgern überhaupt importiert bzw. exportiert werden? Ein Grund liegt darin, dass der ESX Server keine Zuwachsplatten und auch keine segmentierten Platten in 2-GB-Streifen unterstützt. Das sind aber die häufigsten Formate, in denen virtuelle Platten der Hosted-Produkte angelegt werden. Das ganze Geheimnis des Importvorganges liegt darin, die virtuellen Platten in eine monolithische Platte ohne Segmente (auch als *Monolithic Flat* bezeichnet) umzuwandeln und für den ESX Server 3 zusätzlich eine passende Kopfdatei mit den Geometriedaten der Platte zu erstellen (siehe auch Platten-Workshop in Teil 3, Kapitel 3).

Umgekehrt ist es nicht möglich, eine virtuelle Platte des ESX Servers einfach auf ein Hosted-Produkt zu kopieren. Beim ESX Server 2 fehlt die Kopfdatei (das sog. *Header File*), aus dem sich die Hosted-Produkte die Geometriedaten und den Controllertyp einer virtuellen Platte im Format *Monolithic Flat* entnehmen. Der ESX Server 2 benutzt die virtu-

ellen Platten immer ohne Kopfdateien, der Kernel kennt die benötigten Geometriedaten. Der ESX Server 3 erstellt zwar eine Kopfdatei für jede virtuelle Platte, aber mit Parametern, welche die Hosted-Produkte nicht akzeptieren. Der Exportvorgang einer virtuelle Platte vom ESX Server muss also die passende Kopfdatei mit den richtigen Parametern erstellen. Zusätzlich wird die monolithische Platte in 2-GB-Streifen umgewandelt, um sie einfacher vom ESX Server wegzukopieren.

### Direktes Kopieren virtueller Platten vom ESX Server ohne Exportfunktion

Der interne Aufbau der Behälterdateien im Format *Monolithic Flat* ist zwischen VMware Server, Workstation und ESX Server untereinander kompatibel. Virtuelle Platten gehen also beim direkten Kopieren von einem VMFS-Volumen über das Netzwerk nicht „kaputt“, wie das in vielen Diskussionen zu hören ist. Sie können durchaus virtuelle Platten direkt vom ESX Server kopieren und mit dem VMware Server oder der Workstation verwenden. Umgekehrt können Sie eine Platte, die unter VMware Server oder Workstation mittels (*allocate all disk space now*) als monolithische Platte in voller Größe angelegt wurde, ohne Importvorgang direkt zum ESX Server 3 auf eine VMFS-Partition kopieren, z.B. mit WinSCP.

Dazu sind nur einige Parameter in der Kopfdatei der virtuellen Platte mit einem Texteditor anzupassen, die Behälterdatei bleibt unangetastet. Der ESX Server 2 verwendet keine Kopfdatei, Sie müssen erst eine erstellen, beim ESX Server 3 können Sie die vorhandene Datei einfach anpassen. Die Kopfdatei ist immer die kleinere der beiden *vmdk*-Dateien ohne die Erweiterung *-flat.vmdk* (siehe dazu auch den Platten-Workshop in Teil 3, Kapitel 3):

- Beispielparameter für den ESX Server 3:

```
createType="vmfs"
Extent description
RW 4194304 VMFS "meinePlatte-flat.vmdk"
```

- Beispielparameter für VMware Server/Workstation/Player:

```
createType="monolithicFlat"
Extent description
RW 4194304 FLAT "meinePlatte-flat.vmdk" 0
```

## 9.3.9 Konfiguration des Netzwerks auf dem ESX Server 3

Sie haben bereits bei der Vorbereitung der iSCSI-Verbindung einen Blick auf die Netzwerkkonfiguration geworfen. Grundsätzlich verfolgt der ESX Server das gleiche Prinzip der Verwendung virtueller Switches wie alle Hosted-Produkte. Den Unterschied machen die erweiterten Möglichkeiten optimierter Treiber und der direkten Kon-



trolle über die Netzwerkhardware, durch die der ESX Server Funktionen wie Teaming oder VLAN-Verwaltung direkt und ohne Zusatzkomponenten bereitstellen kann.

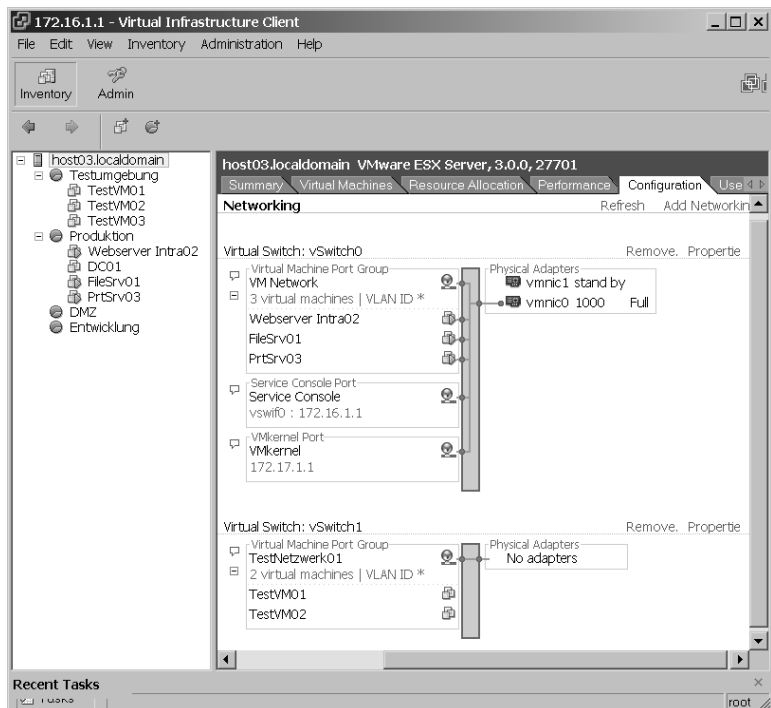


Sollten Sie den Begriff *virtueller Switch* noch nicht kennen, dann lesen Sie bitte als Einführung die ersten Seiten des Teil 3, Kapitel 2, „*Virtuelle Netzwerke Teil 2 – die ganze Wahrheit*“. Dort sind alle Grundlagen zu virtuellen Netzwerken erklärt, sie gelten zum großen Teil auch für den ESX Server.

### Virtuelle Switches und Netzwerkkarten, Portgruppen und physische Adapter

Im Reiter CONFIGURATION finden Sie unter NETWORK ADAPTERS alle erkannten physischen Netzwerkkarten auf dem Host, sie werden hier nur angezeigt und lassen sich nicht bearbeiten. Diese Adapter können Sie im Menüpunkt NETWORKING virtuellen Switches zuweisen. Der VI Client stellt den Aufbau des virtuellen Netzwerks übersichtlich grafisch dar (Abbildung 9.19).

Abbildung 9.19:  
VMs, Service Console und Kernel hängen an virtuellen Switches, denen physische Adapter zugewiesen werden können



Wie Sie gleich nach der Installation sehen, hat VMware bereits einen virtuellen Switch *vSwitch0* erstellt und diesem eine physische Netzwerkkarte *vmnic0* zugeordnet. Darüber kommuniziert der Anschluss *vswwf0* der Service Console mit dem LAN. Ohne diese beim Setup

automatisch erfolgte Konfiguration hätten Sie sich gar nicht erst mit dem VI Client auf den Server verbinden können, weil die Service Console keinen LAN-Zugang hätte. Je nach verfügbaren Netzwerkkarten kommunizieren auch die Gäste, dargestellt durch eine Portgruppe namens *VM Network*, über diesen Switch. Welche Gäste der entsprechenden Portgruppe zugeordnet sind, wird ebenfalls dargestellt. Sie können an dieser Stelle weitere Switches und Portgruppen erstellen oder bestimmten Switches physische Netzwerkkarten zuweisen.

Bei der Vorbereitung für den iSCSI-Initiator haben Sie der vorhandenen Konfiguration einen Port für den *VMkernel* am Switch *vSwitch0* hinzugefügt und damit die Kommunikation von Diensten des Kernels mit dem LAN ermöglicht.

### Funktion der virtuellen Switches und Portgruppen beim ESX Server 3

Die Funktion der virtuellen Switches des ESX Servers unterscheidet sich grundsätzlich kaum vom Netzwerk-Workshop für die Hosted-Produkte, einige Funktionen kommen hinzu:

- ▶ Gäste sind mit virtuellen Adaptern an virtuellen Switches angeschlossen. Beim ESX Server ist ein Switch zusätzlich in Portgruppen untergliedert, die es z.B. ermöglichen, VLANs zu definieren oder spezielle Teaming-Profile zu konfigurieren. Genau genommen ist der virtuelle Adapter eines Gastes an eine bestimmte Portgruppe eines virtuellen Switches angeschlossen.
- ▶ Nur Gäste am gleichen Switch bilden ein Netzwerk und können miteinander kommunizieren. Sind über bestimmte Portgruppen VLANs definiert, können sich nur die Gäste im gleichen VLAN sehen. Netzwerke über unterschiedliche Switches hinweg lassen sich nur durch virtuelle Maschinen mit zwei virtuellen Adaptern als Router verbinden.
- ▶ Den virtuellen Switches sind wiederum physische Netzwerkkarten zugeordnet, die einen *Uplink* (*kaskadierende Verbindung zwischen Switches*) zu einem physischen Switch im LAN bilden können. Über diese Verbindung kommunizieren alle angeschlossenen Gäste und Dienste mit dem physischen Netzwerk. Unter dem ESX Server 3 können einem virtuellen Switch mehrere physische Netzwerkkarten zugeordnet werden, wodurch Teaming zur Ausfallsicherheit oder Bandbreitenkopplung möglich ist.
- ▶ Switches ohne zugewiesene physische Adapter bilden interne abgeschottete Netzwerke, ohne direkten Kontakt zur Außenwelt, z.B. für ein Testnetzwerk oder eine DMZ (im Bild *vSwitch1*).



Beim ESX Server 3 sind zusätzlich zu den Portgruppen für die Gäste (*VM Network*) auch Ports der Service Console (*Service Console*) und Dienste des Kernels (*VMkernel*) an virtuelle Switches angeschlossen. Dadurch kommuniziert auch das Host-System, also der ESX Server, über virtuelle Netzwerke mit dem physischen LAN. Das ist eine konsequente Umsetzung der Virtualisierung – was für die Gäste gilt, gilt auch für den Wirt.

Eine Verbindung der Service Console ist zur Verwaltung des Hosts und der Gäste über das LAN unbedingt notwendig. Der Kernel muss für die Kommunikation mit einem NAS bzw. für die Verbindung mit einem Target über den Software iSCSI Initiator oder für die Verwendung von VMotion das physische Netzwerk erreichen können.

### Weitere Switches einrichten und Teaming konfigurieren

Sie sehen bereits an diesem einfachen Beispiel, wie flexibel die Netzwerkkonfiguration unter dem ESX Server ist. Alle Dienste des Hosts und alle Gäste können den gleichen physischen Adapter verwenden, oder jede Gruppe hat ihr eigenes Netzwerk mit Switch und physischer Netzwerkkarte zur Verfügung. Mittels *ADD NETWORKING* können Sie weitere Switches erstellen und physische Netzwerkkarten zuweisen. Switches ohne Netzwerkkarten können interne Testnetzwerke bilden. Mittels *PROPERTIES* lassen sich die Einstellungen eines Switches ändern. Hier können Sie z.B. auch festlegen, ob ein virtueller Switch für VMotion verwendet werden darf oder nicht. VMware empfiehlt eine eigene physische Netzwerkkarte für den VMotion-Verkehr.



Achten Sie bei Ihren Experimenten immer darauf, dass die Service Console eine Verbindung zu einem Switch hat, der wiederum über eine physische Netzwerkkarte verfügt. Sonst sägen Sie sich sozusagen den Ast ab, auf dem Sie sitzen, und können nur durch umständliche Kommandozeilenarbeit direkt an der Server Console wieder eine Verbindung zum ESX Server herstellen (siehe *Abschnitt 9.4, „Einige Tipps zum Umgang mit dem ESX Server 3“*).

Das Besondere am ESX Server sind die zusätzlichen Optionen, die erst durch die eigenen Netzwerkkartentreiber und die direkte Verwaltung der Hardware möglich werden. Z.B. können Sie einem virtuellen Switch mehrere physische Adapter zuweisen und damit mehrere redundante Uplinks zum physischen Netzwerk bereitstellen, was einem Teaming entspricht (*vmnic1* in Abbildung 9.19). Es lässt sich genau festlegen, ob beide Adapter aktiv sein sollen (Bündelung der Bandbreite) oder ob ein Adapter nur als Stand-by-Gerät für den Notfall dienen soll (Ausfallsicherheit).

Wenn Sie beispielsweise zwei Adapter dem virtuellen Switch zuweisen, über den die Service Console kommuniziert, können Sie einen davon als Stand-by-Adapter definieren. Wenn beide Adapter an dem physischen LAN-Switch Ihres Netzwerks angesteckt sind, wird der Stand-by-Adapter automatisch aktiviert, sobald Sie vom ersten Adapter das Kabel abziehen, also einen Ausfall simulieren. Die Konsole, bzw. alle VMs an diesem Switch, bemerken keine Unterbrechung.

**Teaming zur  
Ausfallsicherheit  
der Konsole**

Der Nachteil an diesem Beispiel besteht darin, dass der Stand-by-Adapter im Normalfall ständig ungenutzt ist, das ist eine Verschwendung von Hardware. Dabei macht der ESX Server 3 viel flexiblere Konstellationen möglich. Z.B. können Sie für jede Portgruppe eines Switches, etwa für die Gäste und die Service Console, jeweils eine dedizierte Netzwerkkarte zuweisen. Damit hat jeder Dienst für optimale Performance einen eigenen Adapter zur Verfügung. Über Teaming-Regeln legen Sie fest, dass beim Ausfall eines Adapters die zugehörige Portgruppe automatisch über den Adapter der anderen Portgruppe mitkommunizieren darf. Dadurch ist im Störfall zwar keine optimale Leistung mehr gegeben, aber alle Dienste bleiben weiterhin erreichbar. Vor allem benötigen Sie nicht unbedingt zusätzliche Stand-by-Adapter, die nur bei einem Ausfall zum Zuge kommen und sonst im Leerlauf bleiben.

Folgendermaßen erstellen Sie eine Stand-by-Konfiguration für die Portgruppe *VM Network* und für den Service Console Port an *vSwitch0*:

1. Wählen Sie **PROPERTIES** für den *vSwitch0*, und öffnen Sie die Eigenschaften von *vSwitch* mittels **EDIT**.
2. Unter dem Reiter **NIC-TEAMING** definieren Sie bei **FAILOVER ORDER** die globale Teaming-Regel für den gesamten Switch.
3. Ordnen Sie mittels **MOVE UP/MOVE DOWN** die Netzwerkkarte *vmnic0* den **ACTIVE ADAPTERS** zu und *vmnic1* den **STANDBY ADAPTERS**. Das bedeutet, alle Portgruppen am Switch verwenden nur den Adapter *vmnic0* – solange dieser nicht ausfällt, bleibt *vmnic1* inaktiv. Das ist zwar schon redundant, aber die Hardware ist nicht optimal ausgenutzt.

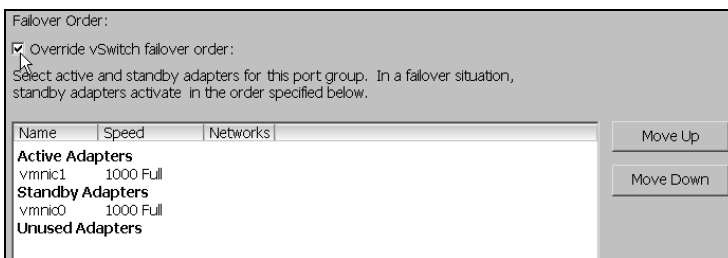


Abbildung 9.20:  
Aktive und Stand-  
by-Adapter können  
für jede Portgruppe  
separat zugewiesen  
werden

4. Wählen Sie die Portgruppe *VMkernel*. Unter **NIC-TEAMING** können Sie dort eine vom Switch abweichende **FAILOVER ORDER** einstellen, indem Sie den Haken bei **OVERRIDE vSWITCH FAILOVER**

ORDER setzen (Abbildung 9.20). Vertauschen Sie die Adapter, dass für diese Portgruppe *vmnic0* stand-by und *vmnic1* aktiv ist. Jetzt kommuniziert nur der Port VMkernel, und damit z.B. der iSCSI-Initiator oder VMotion, über den physischen Adapter *vmnic1*. Bei Ausfall von *vmnic1* kann der Kernel über *vmnic0* weiterkommunizieren.

5. Die Service Console und die Gäste verwenden weiterhin ausschließlich *vmnic0*, können aber bei einem Ausfall auf *vmnic1* abweichen.

Das Beispiel funktioniert allerdings nicht, wenn das physische Speichernetz völlig abgeschottet vom LAN läuft, weil dann die Service Console bei einem Ausfall ihres Adapters nur noch im Speichernetz kommunizieren könnte bzw. der Kernel im LAN. Das Beispiel verdeutlicht trotzdem die Möglichkeiten der Teaming-Regeln. In größeren Umgebungen können auf diese Weise den Portgruppen verschiedener Gäste dedizierte physische Adapter zugewiesen werden, um die Last zu verteilen. Im Notfall können alle Gäste automatisch über den gleichen Adapter kommunizieren.

Ein kleiner Schönheitsfehler dieser Methode ist die fehlende Anzeige in der grafischen Netzwerkübersicht. Dort wird immer die übergreifende Regel für den Switch dargestellt. Dass der vermeintliche Stand-by-Adapter in Abbildung 9.19 eigentlich in unserer Konstellation von der Portgruppe *VMkernel* aktiv verwendet wird, geht aus der Anzeige in Abbildung 9.19 nicht hervor. Erst in den Einstellungen der Portgruppe unter *PROPERTIES* ist die wirksame Konfiguration sichtbar.



Für Produktionsumgebungen mit höheren Anforderungen an die Ausfallsicherheit und mit getrennten Netzwerken für Daten, Verwaltung und Speicher sollten Sie mehrere virtuelle Switches mit dedizierten Netzwerkadaptern erstellen. Ein Netzwerkadapter kann dabei immer nur einem bestimmten Switch zugewiesen werden, für Teaming und Ausfallsicherheit benötigen Sie also mehrere Adapter pro virtuellem Switch.

Es lohnt sich durchaus, an dieser Stelle etwas zu experimentieren und alle Optionen der Netzwerkkonfiguration zu erforschen, z.B. die Konfiguration einer VLAN-ID oder die Verwendung interner Switches mit Routing-VMs. Auch das praktische Beispiel der virtuellen DMZ aus *Teil 2, Kapitel 3, „Virtuelle DMZ mit Firewall und Webserver im Internet“* kann problemlos auf dem ESX Server umgesetzt werden.



Erstellen Sie bei Ihren Experimenten mittels Teaming auch eine Ausfallsicherung für die Service Console, das spart Ihnen den Gang zur Kommandozeile bei Fehlkonfigurationen.

## 9.4 Einige Tipps zum Umgang mit dem ESX Server 3

An dieser Stelle werde ich Ihnen noch einige Fragen beantworten, auf die Sie früher oder später stoßen werden. Hinweise für eine tiefgreifendere Bedienung des ESX Servers finden Sie in den Produkthandbüchern.

### 9.4.1 Benutzer für die tägliche Verwaltung und Probleme mit eingeschränkten Rechten

Für die tägliche Verwaltung kann es gefährlich sein, immer mit vollen Root-Rechten zu agieren. Aus diesem Grunde sollten Sie Nutzer mit abgestuften Berechtigungen auf dem ESX Server anlegen. Zumindest benötigen Sie einen Nutzer, mit dem Sie administrative Aufgaben erledigen können, da Sie sich standardmäßig mit dem Nutzer *root* nicht über das Netzwerk auf die Kommandozeile verbinden können (siehe „Eingeschränkte Rechte bei Remote-Anmeldungen an der Konsole mittels SSH und sFTP“).

Nutzer auf dem ESX Host lassen sich nur direkt am Server, nicht über Virtual Center anlegen!



Gehen Sie folgendermaßen vor, um einen Nutzer mit Administratorrechten anzulegen:

1. Wechseln Sie zum Reiter **USERS & GROUPS**, und wählen Sie **USERS**.
2. Klicken Sie mit der rechten Maustaste ins Fenster, und wählen Sie **ADD**.
3. Legen Sie einen Nutzer an, und nehmen Sie ihn gleich in die Gruppe *root* auf. Dazu müssen Sie *root* manuell in das Gruppenfeld schreiben und den Button **ADD** anklicken. Setzen Sie dabei den Haken an **GRANT SHELL ACCESS**, um eine Anmeldung an der Kommandozeile zu ermöglichen. Die **UID** kann leer bleiben.

Sie können anstelle der *root*-Mitgliedschaft unter **GROUPS** auch eine eigene Gruppe anlegen und den Nutzer dort aufnehmen. Unter dem Reiter **PERMISSIONS** können Sie dieser Gruppe eine Zugriffsrolle (*Role*) zuweisen, z.B. die vordefinierten Rollen *Administrator* oder *read only*. Weitere Rollen lassen sich über den Button **ADMIN** (neben **INVENTORY** ganz oben links im VI Client) erzeugen.

## Eingeschränkte Rechte bei Remote-Anmeldungen an der Konsole mittels SSH und sFTP

Der ESX Server 3 ist mit sehr restriktiven Sicherheitsregeln ausgestattet, wodurch es nicht möglich ist, sich mit dem Benutzer *root* über eine Remote-Session an der Konsole anzumelden, z.B. um mittels *SSH* (*Secure Shell*) die Kommandozeile zu bedienen oder um über *sFTP* (*SSH File Transfer Protocol*) auf das Dateisystem zuzugreifen. Standardmäßig gelingt die *root*-Anmeldung nur direkt am Server. Sie haben zwei Möglichkeiten, diese Einschränkung zu umgehen:

### Das Kommando *su* für Root-Rechte

Sie können einen neuen Nutzer anlegen und diesem Konto Zugriff auf die Shell erlauben. Damit ist eine Anmeldung über das Netzwerk per *SSH* (z.B. *putty*) möglich. Allerdings hat selbst in der höchsten Berechtigungsstufe ein Nutzer niemals alle Rechte, auch nicht bei Mitgliedschaft in der Gruppe *root*. Beispielsweise sind die wichtigen Ordner der Service Console nur für den Nutzer *root*, nicht aber für die Gruppe *root* mit Schreibrechten ausgestattet. Sie können beispielsweise keine Ordner in der Wurzel anlegen oder die Datei *FSTAB* editieren. Um trotzdem den vollen Zugriff zu erlangen, verwenden Sie in einer Konsolen-Sitzung das Kommando *su*. Sie werden nach dem *root*-Passwort gefragt und verfügen danach über alle Rechte.

### Root Remote-zugriff erlauben

Die zweite Möglichkeit ist das Editieren der Datei */etc/ssh/sshd\_config*, um dem Nutzer *root* eine Remote-Anmeldung an der Console zu erlauben. Eigentlich benötigen Sie das nicht, weil Sie sich bereits mit dem Kommando *su* die notwendigen Rechte bei Bedarf verschaffen können. Nur für den Fall, dass Sie mit einem Programm wie *WinSCP* auf das Dateisystem der Service Console zugreifen wollen und dabei alle Rechte benötigen, etwa um Ordner im Wurzelverzeichnis anzulegen, sollten Sie auf diese Methode zurückgreifen. Gehen Sie folgendermaßen vor:

1. Melden Sie sich an der Server Console als *root* an, oder verschaffen Sie sich mittels *su* *root*-Rechte.
2. Editieren Sie die Datei *sshd\_config* mit folgendem Befehl:  

```
vi /etc/ssh/sshd_config
```
3. Drücken Sie die Taste **[i]** (für *Insert*), um den Inhalt der Datei zu editieren und um Zeichen einzufügen.
4. Suchen Sie die Zeile `PermitRootLogin no`, und kommentieren Sie diese mit einem `#` davor aus.
5. Drücken Sie die Taste **[Esc]**, um den Einfügemodus wieder zu verlassen.
6. Schreiben Sie folgende Zeichenfolge, um die Änderungen zu speichern und den Editor zu verlassen (den führenden Doppelpunkt mitschreiben!):  

```
:wq
```
7. Starten Sie mit dem Befehl `/etc/init.d/sshd restart` den Dienst neu.

Jetzt können Sie sich auch mit dem Benutzer *root* an einer Remote-Session oder mit einem sFTP-Client wie WinSCP anmelden.

Denken Sie daran, dass das ein Sicherheitsrisiko für Ihren Server darstellt. Versehen Sie das *root*-Konto mit einem sicheren Passwort!



### 9.4.2 Zugriff auf das Dateisystem des ESX Servers von einem Client aus zum Kopieren und Verwalten

Eine häufige Frage von ESX-Einsteigern ist immer wieder: Wie kopiere ich Dateien auf den ESX Server, z.B. ein ISO-Image? Der komfortabelste Weg ist über sFTP mit einem Programm wie WinSCP. Damit können Sie sich mit dem Server verbinden und auf das Dateisystem zugreifen. Unter */vmfs/volumes* finden Sie z.B. Ihre VMFS-Speicher, wo Sie in einem Unterordner ISO-Images ablegen können. ISO-Images können ohne besondere Behandlung kopiert werden, denken Sie aber daran, dass virtuelle Platten importiert bzw. exportiert werden müssen, kopieren genügt nicht.

[www.winscp.net](http://www.winscp.net)

Eine Alternative zum bekannten, aber oft als langsam beklagten WinSCP finden Sie hier:

<http://www.bitvise.com/tunnelier.html>

Das unsichere, aber schnelle FTP wird vom ESX 3 nicht mehr unterstützt. Es ist kein FTP-Server mehr in der Service Console installiert.



#### Kopieren mit WinSCP ist viel zu langsam

Die Geschwindigkeit bei Kopiervorgängen über sFTP bzw. SCP ist durch Verschlüsselungsvorgänge weitaus langsamer als mit dem einfachen FTP. Ein wenig mildern können Sie den Umstand durch die Verwendung einer anderen Verschlüsselung als das standardmäßig gewählte *AES (Advanced Encryption Standard)*. Dazu müssen Sie unter WinSCP den Haken an *EXPERTENMODUS* setzen und im Menü unter *SSH* das Protokoll *blowfish* ganz nach oben schieben. Da ab dem ESX Server 3 standardmäßig nur noch AES als Verschlüsselung akzeptiert wird, müssen Sie zusätzlich in der Datei */etc/ssh/sshd\_config* auf dem Server folgende Zeile suchen und mit *#* auskommentieren; gehen Sie zum Editieren vor wie weiter oben bereits beschrieben:

```
Ciphers aes256-cbc,aes128-cbc
```



### Das Kopieren von ISO-Images und anderen Dateien mit WinSCP bricht am Ende des Vorganges ab

WinSCP kann die temporär angelegten Dateien, die einen Wiederanlauf bei abgebrochener Kopieraktion ermöglichen sollen, am Ende des erfolgreichen Kopiervorganges auf dem ESX Server nicht in den endgültigen Namen umbenennen. Um diesen Fehler zu umgehen, schalten Sie die Funktion zum Fortsetzen der Übertragung unter WinSCP ab. Sie finden die Einstellung bei laufender Session im Menü EINSTELLUNGEN/ÜBERTRAGUNG/FORTSETZEN, wählen Sie AUSSCHALTEN.

#### 9.4.3 Fernbedienung der Service Console von einem Client aus

Um auf die Kommandozeile der Service Console für Verwaltungsaufgaben über das Netzwerk zugreifen zu können, ist es möglich, dass Sie sich per SSH zum Server verbinden. Dazu kann das kostenlose Tool *Putty* dienen. Beachten Sie die Bemerkungen unter „Eingeschränkte Rechte bei Remote-Anmeldungen an der Konsole mittels SSH und sFTP“.

[www.putty.nl/](http://www.putty.nl/)

#### 9.4.4 SMB-Freigaben eines Windows Servers am ESX Server mounten

Um Gästen auf dem ESX Server die Benutzung einer ISO-Sammlung eines Windows-Servers zu ermöglichen, oder zum einfache Dateiaustausch, kann es praktisch sein, eine SMB-Freigabe (normale Verzeichnisfreigabe eines Windows-Servers oder einer Workstation) gleich am ESX Server zu verbinden. Damit entfällt der Umweg des Kopierens über WinSCP. Die verbundene Netzwerkfreigabe ist dann in der Service Console als Verzeichniseintrag im Dateisystem zu sehen.

1. Zuerst müssen Sie in der Firewall auf dem ESX Server die Ports für den SMB-Client zulassen (Vorgehensweise siehe bei „Vorbereitungen für die Verwendung des iSCSI Software Initiators oder eines NAS“).
2. An der Service Console geben Sie mit Root-Rechten folgenden Befehl ein, um ein Verzeichnis als Mountpoints für die zu verbindende Dateifreigabe anzulegen:

```
mkdir /mountpoint
```

3. Jetzt können Sie die Freigabe verbinden, der Inhalt erscheint im Verzeichnis des Mountpoints:

```
smbmount //windows_server_ip/freigabe /mountpoint
-o username=nutzername
```

4. Einfacher geht das Mounten, wenn Sie folgende Zeile in die Datei */etc/fstab* aufnehmen:

```
//server01/freigabe /mountpoint smbfs
ip=ipadresse,username=nutzername,workgroup=domainn
ame,password=passwort,noauto 0 0
```

Es genügt dann an der Kommandozeile der Befehl:

```
mount /mountpoint
```

Auf dem Windows Server darf nicht das so genannte *SMB Signing* aktiviert sein. Sie finden die Einstellung in den Gruppenrichtlinien unter:

Computer Verwaltung/Windows Einstellungen/lokale  
Sicherheitseinstellungen/lokale Richtlinien/  
Sicherheits Optionen/Microsoft Netzwerk Server.

Hier sollte *Kommunikation digital signieren (immer)* deaktiviert sein. Wurde diese Funktion vom Administrator aktiviert, verletzen Sie mit dem Deaktivieren eventuell die Sicherheitsrichtlinien in Ihrem Netzwerk!

Über eine SMB-Verbindung lassen auf dem ESX Server keine Dateien kopieren, die größer als 2 GB sind!



### **Zugriff von Gästen auf ISO-Images, die auf einem Windows Server im Netzwerk liegen**

Eigentlich müssen sich ISO-Images auf einem VMFS-Volumen befinden, um sie einem Gast zuzuordnen. Ein kleiner Trick hilft dabei, den oben angelegten SMB-Mount gleich direkt als Quelle von ISO-Images zu verwenden und dieses Image dadurch über das LAN als virtuelle CD in den Gästen einzubinden. Damit spart man sich das redundante Kopieren bereits vorhandener ISO-Sammlungen auf den ESX Server.

Legen Sie einfach auf einem VMFS-Datenträger einen symbolischen Link auf den Mountpoint Ihrer verbundenen SMB-Freigabe an. Verwenden Sie dazu in der Service Console folgenden Befehl:

```
ln -s /mountpoint /vmfs/volumes/datastore01/iso_images
```

In diesem Beispiel ist */datastore01* ein vorhandenes VMFS-Volumen, auf dem der Link angelegt werden soll, und *iso\_images* ist der Name des symbolischen Links. Der Link zeigt auf das Verzeichnis */mountpoint*, unter dem die Netzwerkfreigabe mittels *smb-mount* verbunden ist. Wenn Sie jetzt im VI Client einem Gast ein ISO-Image als CD zuweisen wollen, können Sie im Dialog den Namen des Links auf dem VMFS-Datenträger wie ein Verzeichnis öffnen. Unter diesem Verzeichnis wird der Inhalt der Netzwerkfreigabe angezeigt. Sie können ein dort liegendes ISO-Image auswählen und im Gast als CD benutzen.

### 9.4.5 Verbindung zur Service Console verloren?

Sollte es trotz aller Vorsicht doch passieren und Sie entziehen der Service Console die Verbindung zum LAN, dann können Sie diese Verbindung nur direkt am Server an der Kommandozeile wiederherstellen. Melden Sie sich dazu als Benutzer *root* an, und versuchen Sie, mit folgenden Befehlen dem Switch für die Service Console wieder eine physische Netzwerkkarte zuzuweisen:

- ▶ `esxcfg-nics -l` listet alle physischen Adapter auf in der Form *vmnic0*, *vmnic1*. Sie sehen auch den Linkstatus und können durch Abziehen des Kabels testen, welche die richtige Karte für die Service Console ist.
- ▶ `esxcfg-vswitch -l` listet alle Portgruppen und Switches auf. Ein Switch nennt sich z.B. *vSwitch0*. Mit folgendem Befehl verbinden Sie die physische Karte *vmnic1* wieder mit dem Switch *vSwitch0*, an dem standardmäßig die Service Console hängt:

```
esxcfg-vswitch -L vmnic1 vSwitch0
```

- ▶ `esxcfg-vswif` erstellt einen neuen Port (*vswif*) für die Service Console oder schließt sie wieder an den richtigen Port an. Dabei ist die IP-Konfiguration auch anzugeben.

### 9.4.6 An der Kommandozeile einen Snapshot für ein Hot-Backup setzen

Eine Stärke des ESX Servers ist seine Snapshot-Funktion. Außer in der GUI des Clients können Sie einen Snapshot auch per Kommandozeile setzen und damit die virtuelle Platte mit einem Redo-Log versehen. Ähnlich arbeitet z.B. auch VMware Consolidated Backup. Dieser Tipp dient als kleines Beispiel für die Macht der Kommandozeile.

1. Dieser Befehl listet alle registrierten (sich im Inventory befindlichen) VMs auf und gibt im Pfad den Datastore als ID an. Diese Pfadangabe mit der ID benötigen Sie für die weiteren Kommandos:

```
vmware-cmd -l
```

2. Mit diesem Befehl erhalten Sie den Status der VM als Test, ob der Pfad korrekt ist und die VM existiert. Die lange Zahlenfolge ist die vorher angezeigte ID des Datastores:

```
vmware-cmd /vmfs/volumes/449913d9-ddda40a9-ccfe-0007e909b5d0/test99/test99.vmx getstate
```

```
getstate() = on
```

3. Mit diesem Befehl setzen Sie einen Snapshot, die 1 bei den letzten Ziffern besagt, dass das Dateisystem in einen konsistenten Zustand gebracht werden soll (*Quiescing*), die 0 verhindert, dass der RAM-Inhalt mitgesichert wird:

```
vmware-cmd /vmfs/volumes/449913d9-ddda40a9-ccfe-0007e909b5d0/test99/test99.vmx createsnapshot
"snap1" "vor Hotbackup" 1 0
```

4. In der VM erscheinen im Ereignisprotokoll folgende Meldungen (auszugsweise), die das automatische Synchronisieren (*Quiescing*) des Dateisystems vor dem Snapshot anzeigen, wenn die VMware Tools installiert sind:

```
LGTO_Sync:
Sync Stop done
Flush Completed
```

5. Nachdem Sie beispielsweise die virtuelle Platte für eine Sicherung wegkopiert haben, können alle Snapshots wieder entfernt werden, aufgelaufene Transaktionen werden automatisch mit der zugrunde liegenden virtuellen Platte zusammengeführt (commit):

```
vmware-cmd /vmfs/volumes/449913d9-ddda40a9-ccfe-0007e909b5d0/test99/test99.vmx removesnapshots
```

## 9.5 Installation von Virtual Center 2 mit Einbinden der ESX Hosts und der VMs

Mit dem Crashkurs zum ESX Server 3 haben Sie die Grundlagen für den Umgang mit dem Herzstück Ihrer virtuellen Infrastruktur gelegt. Ein ESX Server bietet schon für sich allein sehr interessante Funktionen, die erweiterten Möglichkeiten wie VMotion, Hochverfügbarkeit (HA) oder Ressourcenverwaltung mit Load Balancing (DRS) werden erst mit der zentralen Verwaltungsplattform Virtual Center möglich.

Die Installation des Virtual Center Management Servers kann zusammen mit dem Lizenzserver und dem Virtual Infrastructure Client auf einem PC im Netzwerk erfolgen. Ist der Lizenzserver noch nicht eingerichtet, geschieht das während des Setups. Folgende Hauptkomponenten sind im Installationspaket enthalten:

- ▶ *Lizenzserver* – Sie haben den Lizenzserver bei der Installation des ESX Servers bereits kennen gelernt. Der gleiche Dienst verwaltet auch die Lizenzen für Virtual Center.
- ▶ *Virtual Center Management Server* – Der Management Server ist die zentrale Komponente von Virtual Center. Er verwaltet alle eingebundenen Hosts und die VMs in einer Datenbank. VMware kann eine vorhandene Datenbank verwenden oder auf dem Rechner eine Instanz der *Microsoft SQL Server Desktop Engine (MSDE)* installieren.

- ▶ *Virtual Infrastructure Client* – Das ist der gleiche Client, den Sie bereits für die Verwaltung Ihres ESX Servers verwendet haben. Sie können ihn auf einem PC im LAN oder auf dem Management Server installieren und mit ihm sowohl auf einen einzelnen ESX Server als auch auf einen Management Server zugreifen.
- ▶ *Virtual Infrastructure Web Access* – Über diesen Dienst können Sie, ähnlich wie beim allein stehenden ESX Server, alle VMs der Infrastruktur in einem Browser verwalten. Dazu installiert VMware auf dem Management-Rechner Apache Tomcat als Webserver.

### 9.5.1 Installation des Virtual Center Management Servers

Zur Installation des Virtual Center Management Servers gehen Sie folgendermaßen vor:

1. Sollte Ihre CD nicht automatisch starten, dann öffnen Sie die *autorun.exe*, und wählen Sie VIRTUAL CENTER MANAGEMENT SERVER (Abbildung 9.21). Sie finden alle Komponenten auch einzeln im Verzeichnis */bin* der Installations-CD.

Abbildung 9.21:  
Der Virtual Center  
Management Server  
setzt einen Lizenz-  
server voraus, der  
automatisch mitins-  
talliert werden kann



2. Wenn Sie auf den Zugriff auf Gäste über einen Browser (*Web Access*) und den damit verbundenen Webserver verzichten wollen, dann können Sie mit einer Custom-Installation diese Komponente abwählen.
3. Wählen Sie die Art Ihrer Datenbank. Wenn Sie keine vorhandene Datenbank verwenden, dann installiert VMware eine Microsoft SQL Server Desktop Engine (MSDE) auf dem Verwaltungsrechner.
4. Sollten Sie noch keinen Lizenzserver eingerichtet haben, übernimmt VMware die Installation. Ansonsten wählen Sie Ihren vorhandenen Lizenzserver aus. Standardmäßig verwendet der Lizenzserver den Port 27000. Wenn er auf dem gleichen Rechner installiert ist, dann lautet die Adresse *27000@localhost*, anderenfalls ersetzen Sie *localhost* mit der IP-Adresse oder dem Namen Ihres Lizenzservers.

- Die vorgeschlagenen Ports für die Virtual Center-Komponenten können Sie übernehmen. Sollte bereits ein anderer Webserver auf dem Verwaltungsrechner laufen, dann sind die Ports 80 und 443 des VMware Web Service abzuändern.
- Konfigurieren Sie, ob Apache Tomcat automatisch als Dienst starten soll und auf welchem Port er erreichbar ist, standardmäßig verwendet er 8086. Dieser Port hat nichts mit dem Virtual Center zu tun, es ist die Verwaltungswebseite des Apache Tomcat Servers.

Damit ist das Setup bereits beendet. Auf der Begrüßungswebseite des Management Servers, zu erreichen mittels [https://mein\\_vc/](https://mein_vc/), sind wieder der VI Client und der Link zum VMware Web Access verfügbar. Mit dem VI Client, den Sie bereits weiter oben im Workshop vom ESX Server installiert haben, können Sie sich sofort zum Virtual Center Management Server verbinden, es ist die gleiche Software wie der Client des Management Servers.

Die Anmeldung am Virtual Center Management Server mit dem VI Client erfolgt mit einem Windows-Benutzer des Verwaltungsservers und nicht mit einem Nutzer eines ESX Servers.

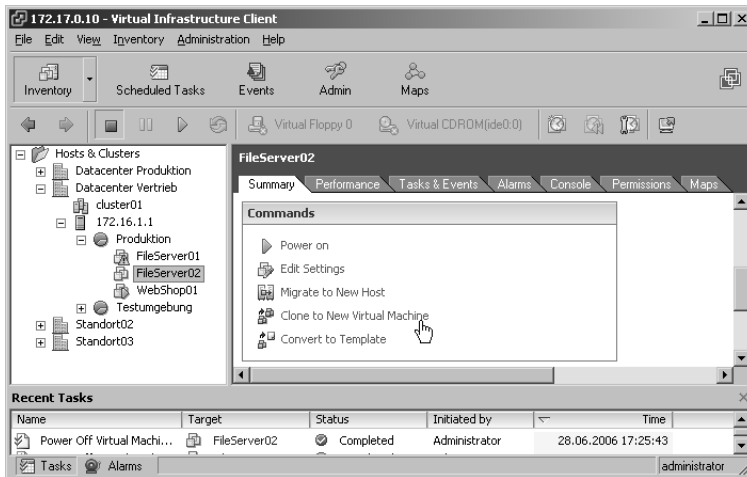


Abbildung 9.22:  
Templates und Klone  
von VMs sowie Migra-  
tionen von Gästen  
zwischen den Hosts  
sind nur einige Funk-  
tionen von Virtual  
Center

### 9.5.2 Erste Schritte im Virtual Center 2

Die Oberfläche von Virtual Center ähnelt der des ESX Servers. Neben den speziellen Einstellungen der zentralen Verwaltungsplattform finden Sie zu jedem Host und zu jeder VM die bereits bekannten Menüpunkte und Karteikartenreiter. Die angezeigten Reiter sind spezifisch für den jeweiligen aktiven Eintrag in der linken Baumstruktur, je nachdem, ob Sie ein DATACENTER, einen HOST oder eine VM auswählen.

Die gesamte Infrastruktur wird in so genannte *Datacenter* organisiert, in jedem Datacenter können einzelne Hosts oder *Cluster* aus Hosts existieren, und Resource Pools fassen die Gäste in Gruppen zusammen.

So integrieren Sie Ihren Host ins Virtual Center:

1. Im VI Client legen Sie mittels rechter Maustaste auf HOSTS & CLUSTER und NEW DATACENTER zuerst ein neues Datacenter an.
2. Mittels ADD HOST wird Ihr bereits installierter ESX Server ins neue Datacenter importiert, dazu benötigen Sie seine IP-Adresse und einen Anmeldenamen. Ab jetzt können Sie alle Funktionen, bis auf die lokale Benutzerverwaltung des ESX Servers, über Virtual Center erreichen.
3. Die Gäste können Sie in Resource Pools des Virtual Centers aufnehmen.
4. Mehrere Hosts können Sie zu einem Cluster zusammenfassen, um VMware HA zu konfigurieren.

#### Lizenzierung der Komponenten wie VMware HA oder DRS

Im Virtual Center erfolgt auch die Lizenzierung der Funktionen VMotion, VMware HA und VMware DRS (Abbildung 9.23). Die Agenten für die ESX Server Hosts sind seit ESX Server 3 bereits mit enthalten und müssen nicht separat erworben werden. Zum Menü LICENSED FEATURES gelangen Sie mit einem Klick auf einen bestimmten Hostnamen und dann über den Reiter CONFIGURATION.

Abbildung 9.23:  
Komponenten wie  
VMotion, VMware  
DRS und VMware  
HA können nur  
über Virtual Center  
lizenziert werden

| Summary Virtual Machines Resource Allocation Performance Configuration Tasks & Events Alerts                                                                                                                                    |                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Hardware</b>                                                                                                                                                                                                                 |                    |
| Processors                                                                                                                                                                                                                      |                    |
| Memory                                                                                                                                                                                                                          |                    |
| Storage (SCSI, SAN, and NFS)                                                                                                                                                                                                    |                    |
| Networking                                                                                                                                                                                                                      |                    |
| Storage Adapters                                                                                                                                                                                                                |                    |
| Network Adapters                                                                                                                                                                                                                |                    |
| <b>Software</b>                                                                                                                                                                                                                 |                    |
| <ul style="list-style-type: none"> <li>Licensed Features</li> <li>DNS and Routing</li> <li>Virtual Machine Startup/Shutdown</li> <li>Security Profile</li> <li>System Resource Allocation</li> <li>Advanced Settings</li> </ul> |                    |
| <b>Licensed Features</b>                                                                                                                                                                                                        |                    |
| <b>License Sources</b>                                                                                                                                                                                                          |                    |
| License Server:                                                                                                                                                                                                                 | 172.17.0.10        |
| Host License File:                                                                                                                                                                                                              | None               |
| <b>ESX Server License Type</b>                                                                                                                                                                                                  |                    |
| ESX Server Standard                                                                                                                                                                                                             | Licensed for 2 CPU |
| ISCSI Usage                                                                                                                                                                                                                     |                    |
| SAN Usage                                                                                                                                                                                                                       |                    |
| Up to 4-way virtual SMP                                                                                                                                                                                                         |                    |
| NAS Usage                                                                                                                                                                                                                       |                    |
| <b>Add-Ons</b>                                                                                                                                                                                                                  |                    |
| VMotion                                                                                                                                                                                                                         | Licensed for 2 CPU |
| VMware DRS                                                                                                                                                                                                                      | Not Used           |
| VMware HA                                                                                                                                                                                                                       | Not Used           |
| VMware Consolidated Backup                                                                                                                                                                                                      | Licensed for 2 CPU |
| VirtualCenter Agent for ESX Server                                                                                                                                                                                              | Licensed for 2 CPU |



Um VMotion verwenden zu können, müssen Sie einen virtuellen Switch bestimmen, über den der Verkehr der VMotion-Vorganges laufen soll (hauptsächlich Kopieren des RAM-Inhaltes des zu verschiebenden Gastes). Sie finden die Einstellung unter CONFIGURATION/NETWORKING/PROPERTIES. Wählen Sie dort einen Port für VMkernel (oder erstellen Sie einen neuen Switch mit einem VMkernel-Port), und setzen Sie den Haken an VMOTION ENABLED. VMware empfiehlt eine separate physische Netzwerkkarte nur für VMotion, um ein möglichst schnelles Verschieben der VMs zu gewährleisten, ohne Störung des produktiven Netzwerks durch das teilweise hohe Datenaufkommen.

Auf jedem an VMotion beteiligten Host müssen die gleichen Switches und Portgruppen existieren, an denen die zu verschiebenden Gäste angeschlossen sind. Sonst kann VMware auf dem neuen Host die virtuellen Adapter nicht wieder zuordnen, und der verschobene Gast hat keine Netzwerkverbindung.

Eine interessante Funktionen von Virtual Center 2 sind z.B. die so genannten *Maps*, zu finden unter dem gleichnamigen Reiter. Diese grafische Anzeige stellt in größeren Umgebungen sehr übersichtlich die Zusammenhänge von Gästen, Datenspeicher, Netzwerken und Hosts dar. In Installationen mit mehreren Hosts und Dutzenden virtueller Maschinen kann dieser Überblick hilfreich sein.

Weiterhin können unter Virtual Center Warnmeldungen (*Alarms*) für verschiedenste Bedingungen konfiguriert werden, und nicht zuletzt ist es bei mehreren Hosts möglich, die Gäste mittels rechter Maustaste und MIGRATE flexibel zwischen den Hosts zu verschieben. Ist die VM dabei eingeschaltet, erfolgt die Migration mittels VMotion im laufenden Betrieb der VM.

Alle diese Funktionen sind vielleicht einmal Thema eines ausführlichen Werkes zur Virtual Infrastructure 3. Den Umfang und das Anliegen dieses Buches, Sie in den Umgang mit virtuellen Maschinen anhand nachvollziehbarer Projekte und Workshops einzuführen, würden sie bei weitem sprengen.

## 9.6 Ausblick

Es gibt viele Aspekte, die hier aus Platzgründen nicht behandelt werden konnten. Aber mit etwas Forschergeist können Sie auf Basis der Testinstallation aus diesem Crashkurs schon tiefer in die Funktionen der Virtual Infrastructure 3 eindringen, die größten Stolpersteine und Fragen sind aus dem Weg geräumt. Eventuell haben Sie an dieser Stelle bemerkt, dass der kostenlose VMware Server Ihren Anforderungen bereits genügt. Auch dann hat sich der Ausflug zum Virtualisierungsjumbo ESX Server 3 gelohnt.





# Teil 3

## Konzepte und Technik im Detail

In den Praxis-Workshops von Teil 2 sind für Sie wichtige Fragen offen geblieben? Sie wollen mehr über die Funktionen zum Netzwerk, zu den virtuellen Platten oder zu multiplen Snapshots erfahren, bzw. Sie interessieren sich für Konzepte wie Datensicherung und Ausfallsicherheit?

**Erweiterte Erklärungen**

*Dann folgen Sie den Workshops in Teil 3 in die Tiefe!*

### Was lernen Sie im dritten Teil?

Der dritte Teil dieses Buches dient als Ergänzung zu den Praxis-Workshops, kann aber auch separat für die Lösung von speziellen Problemen verwendet werden. Zu den wichtigsten Funktionen virtueller Maschinen finden Sie hier eigene Kapitel, welche die Grundlagen sehr detailliert erklären. Besonderen Platz habe ich beispielsweise dem Netzwerk und den virtuellen Platten eingeräumt, da diese das Rückgrat einer VM bilden und auch die meisten beeinflussbaren Optionen haben.

**Technik im Detail**

Weiterhin stellt Teil 3 wichtige Konzepte vor, die Sie bei der täglichen Arbeit benötigen, z.B.:

**Wichtige Konzepte**

- ▶ Wie sichert man die Daten auf dem Host oder im Gast?
- ▶ Wie können Sie virtuelle Platten vor versehentlichem Löschen schützen, ohne die Lauffähigkeit der Maschine zu stören?
- ▶ Wie lassen sich physischen Server ohne Neuinstallation in eine VM übernehmen?
- ▶ Wie nutzen Sie die multiplen Snapshots der VMware Workstation effektiv für Ihre Testumgebungen?



# 1 Virtuelle Netzwerke – Schnellstart

Sie möchten mit Ihrer VM ohne viel Aufwand im Internet surfen oder mit anderen physischen Rechnern im LAN kommunizieren. Vielleicht benötigen Sie auch ein internes abgeschottetes Testnetz, um das Firmennetzwerk nicht zu gefährden. Das alles wollen Sie schnell und unkompliziert einrichten, ohne sich vorher durch alle Interna zu lesen? Dann sind Sie in diesem Schnelleinstieg richtig! Ich zeige Ihnen die wichtigsten Grundlagen virtueller Netze unter VMware sowie Microsoft.

**Schnell ins Internet oder ins LAN**

Für viele Einsatzzwecke und für die ersten Schritte mit virtuellen Netzwerken genügt bereits dieses Kapitel. Tiefere Einblicke in alle Netzwerkfunktionen liefert *Teil 3, Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“*.

Zusätzlich gibt Ihnen der Workshop *Teil 2, Kapitel 3, „Virtuelle DMZ mit Firewall und Webserver im Internet“*, einen sehr ausführlichen praktischen Einstieg in das Thema.

Wenn Sie folgenden Workshop mit VMs nachvollziehen, in denen Windows XP oder Windows 2003 läuft, dann schalten Sie für Ihre Tests die Windows-Firewall in den Gästen ab. Sonst können Ihre VMs nicht miteinander kommunizieren, obwohl Sie eigentlich alles richtig konfiguriert haben. Auf einen *Ping*-Befehl erhalten Sie dann beispielsweise keine Antwort, weil er von der Firewall des Zielgastes geblockt wird. Die Einstellungen erreichen Sie über SYSTEMSTEUERUNG/WINDOWS-FIREWALL. Auch aktuelle Linux-Distributionen installieren automatisch eine Firewall.

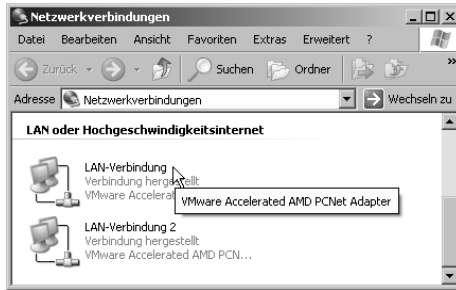


## 1.1 Die emulierten Netzwerkkarten in virtuellen Maschinen

Jeder VM können Sie bis zu vier virtuelle Netzwerkkarten zuweisen. Die Netzwerkfunktionalität einer VM ist dabei grundsätzlich unabhängig von den physischen Karten im Host. Die VM kann im LAN uneingeschränkt erreichbar sein oder komplett abgeschottet in einem internen Netzwerk laufen. Das geht so weit, dass im Host überhaupt keine physische Netzwerkkarte notwendig ist, wenn die VMs nur untereinander kommunizieren. Der Datenverkehr erfolgt dann ausschließlich in virtuellen Netzwerken, was in Testumgebungen oder auf mobilen Laptops nützlich ist.

**Bis zu vier virtuelle Netzwerkkarten**

Abbildung 1.1:  
In den Gästen  
erscheinen die virtu-  
ellen Adapter wie  
normale Netzwerk-  
karten, teilweise  
werden optimierte  
Treiber verwendet



Sobald Sie einen virtuellen Adapter konfiguriert haben, wird dieser in der VM emuliert. Das Gastsystem ist davon überzeugt, mit echter Hardware zu arbeiten. In der Netzwerkumgebung des Gastsystems erscheinen ein oder mehrere Einträge vom Typ *AMD-PCNet* unter VMware (Abbildung 1.1) bzw. *Intel PCI-Fast Ethernet* bei Microsoft-Maschinen. VMware kennt noch weitere Typen wie den *VMware PCI Ethernet Adapter* oder einen *Intel PRO/1000 Gigabit Adapter*. Sie benötigen diese Adapter vorerst nicht. Auf den Unterschied gehe ich im ausführlicheren Netzwerk-Workshop ein (Teil 3, Kapitel 2).

Dank funktionierender Plug&Play-Unterstützung erkennen die meisten Betriebssysteme die Netzwerkkarten in den Gästen automatisch und installieren die passenden Treiber, Sie müssen sich nicht darum kümmern. Die erkannten Netzwerkkarten funktionieren innerhalb der virtuellen Maschine wie echte Adapter. Es lassen sich alle Protokolle verwenden, die vom Gastbetriebssystem unterstützt werden; neben TCP/IP also beispielsweise auch IPX/SPX oder NetBUI. Sie können den Adaptern feste IP-Adressen zuweisen oder die Adressen von einem DHCP-Server beziehen lassen. Auch Routing zwischen mehreren virtuellen Netzwerken lässt sich konfigurieren. Damit ist es möglich, komplexe Testnetze aufzubauen, ohne ein einziges Kabel zu verlegen.

## 1.2 Produktübergreifende Anschlussarten der virtuellen Adapter

Im realen LAN  
oder abge-  
schottet

Ob der erzeugte Netzwerkverkehr aus einer VM die physische Welt erreicht oder ob diese Pakete nur im virtuellen Netzwerk bleiben, hängt maßgeblich von der Konfiguration des emulierten Adapters ab. Es stehen für jeden Virtualisierer, ob VMware oder Microsoft, verschiedene Anschlussarten zur Verfügung, die Sie einfach in den Einstellungen zu den Netzwerkkarten auswählen können. Die Funktionen der Adapter sind unter den einzelnen Produkten sehr ähnlich und unterschiedlich nur in Details. Ich beschreibe die Funktionalität hier global und gehe bei den einzelnen Produkten weiter unten nur noch auf die speziellen Einstellungen ein.

### 1.2.1 Extern (Bridged) – direkt verbunden mit einer physischen Netzwerkkarte

Ein als *Bridged* (VMware) oder auch als *Extern* (Microsoft) konfigurierter Adapter ist über eine physische Netzwerkkarte des Hosts mit dem LAN verbunden, wodurch der Gast dort als ein vollwertiger Rechner auftritt (Abbildung 1.2). Er hat vollen Zugriff auf das Netzwerk und ist uneingeschränkt zu erreichen. Er benötigt eine freie IP-Adresse aus dem LAN oder kann sich diese von einem DHCP-Server besorgen. Mehrere VMs und der Host können unabhängig und parallel über die gleiche physische Netzwerkkarte kommunizieren. Dabei treten sie im LAN auf wie separate physische Maschinen mit eigenen Anschlüssen.

**Direkt ins LAN**

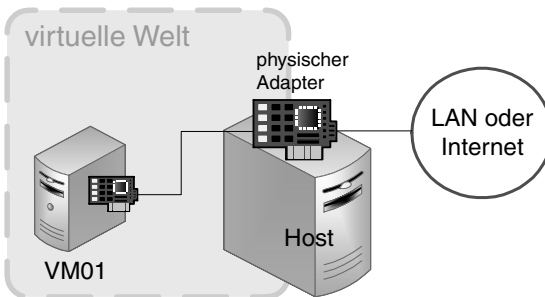


Abbildung 1.2:  
Als Bridged oder extern konfigurierte Adapter haben über eine physische Netzwerkkarte direkten Zugriff auf das LAN

### 1.2.2 Intern (Custom) – abgeschottete Netze für virtuelle Maschinen

Alle Virtualisierer beherrschen einen Modus, in dem sich virtuelle Maschinen nur intern sehen und ein abgeschottetes Netzwerk bilden. Mehrere VMs können in diesem virtuellen Netz ungestört miteinander kommunizieren, ohne dass ein einziges Paket nach draußen gelangt (Abbildung 1.3). Ideal ist diese Konfiguration für Testumgebungen, aber auch für separate abgeschottete Netzwerksegmente wie eine DMZ. Es stehen bei fast allen Produkten mehrere unabhängige isolierte Netze zur Verfügung, die wie separate Switches wirken. Virtual PC kennt nur ein einziges internes Netzwerk.

**Vollkommen abgeschottet**

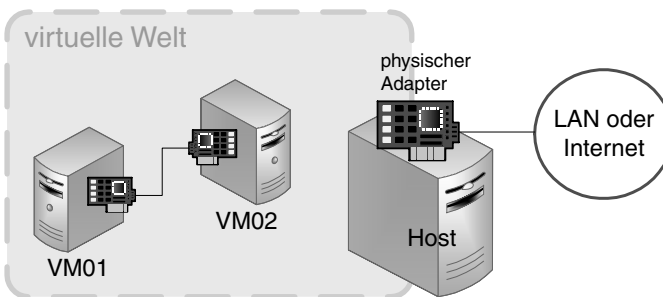


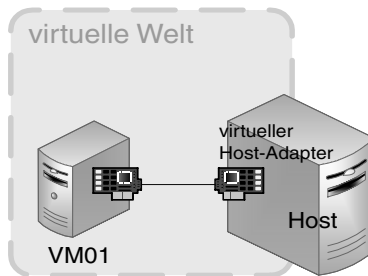
Abbildung 1.3:  
Interne virtuelle Netzwerke bleiben isoliert und ermöglichen abgeschottete Testumgebungen

### 1.2.3 Host-only – direkte Verbindung einer VM mit dem Host

#### Host und VM in einem eigenen Netz

Eine virtuelle Netzwerkkarte im Modus *Host-only* ermöglicht die uneingeschränkte Kommunikation der VM mit dem Host und umgekehrt, selbst wenn gar keine physische Netzwerkkarte vorhanden ist (Abbildung 1.4). Dazu dient ein virtueller Adapter auf dem Host selbst, der die Verbindung zu den internen Netzen herstellt. Dieser Host-Adapter ist mit einem virtuellen Netzwerk verbunden, an dem auch die Gäste angeschlossen sind. Ein häufiger Einsatzzweck ist die Verwendung auf einem mobilen Laptop, wenn z.B. ein Entwickler im Zug auf seine virtuelle Testumgebung zugreifen möchte, obwohl sein physischer LAN-Adapter nicht aktiv ist.

Abbildung 1.4:  
Adapter im Modus  
*Host-only* kommunizieren mit einem virtuellen Adapter auf dem Host auch ohne physische Netzwerkkarte



VMware installiert für diesen Anschlussstyp automatisch den virtuellen Adapter *VMware Network Adapter VMnet1* auf dem Host. Unter Virtual PC/Server existiert der Konfigurationstyp *Host-only* dagegen nicht, er kann aber mit dem so genannten *Microsoft Loopbackadapter* nachgebildet werden (siehe Abschnitt 1.4, „Die Konfiguration virtueller Adapter unter Microsoft Virtual Server und Virtual PC“).

### 1.2.4 NAT – ins LAN unter der Identität des Host-PC



NAT ist die Abkürzung für *Network Address Translation* (Netzwerk-Adressenübersetzung). Es wird heute sehr häufig in Routern verwendet, um ganze Netzwerke über eine einzige öffentliche IP-Adresse an das Internet anzubinden. Ein NAT-Router ersetzt in allen gesendeten Paketen der Clients die internen Absenderadressen mit seiner eigenen öffentlichen IP-Adresse. Die Pakete gelangen dann unter dieser IP nach draußen ins LAN oder ins Internet. In den Antwortpaketen setzt der NAT-Router die Adressen wieder um und schickt die Pakete zurück zum richtigen Client im internen Netz. Alle Rechner im LAN oder im Internet „meinen“, mit dem NAT-Router selbst zu kommunizieren. Die Clients dahinter bleiben verborgen und können daher nicht direkt erreicht werden. **Wichtig: NAT funktioniert nur mit TCP/IP!**

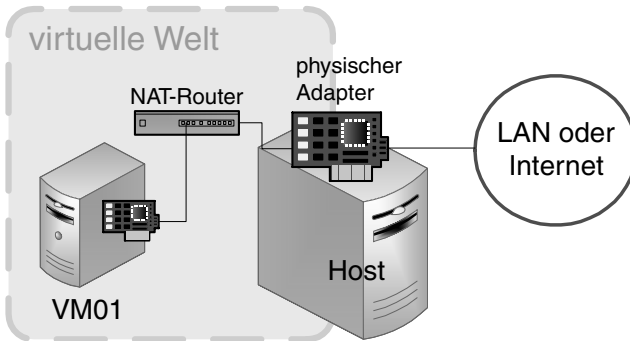


Abbildung 1.5:  
Im Modus NAT  
erreichen die VMs  
das LAN über einen  
internen NAT-Rou-  
ter, der die VMs vor  
dem LAN versteckt

Eine virtuelle Netzwerkkarte, die mit NAT als Anschlussart konfiguriert wurde, borgt sich sozusagen die Identität des Host-PC. Dazu läuft bei VMware und Microsoft Virtual PC ein NAT-Dienst, der den Netzwerkverkehr der Gäste über den Host ins LAN leitet (Abbildung 1.5). Im LAN bleiben die VMs unsichtbar. Alle LAN-Clients „meinen“, der Host-PC sendet die Pakete. Mit einem NAT-Adapter müssen Sie weder eine freie IP-Adresse im LAN kennen, noch müssen Sie sich um Routing-Einträge oder DNS-Einstellungen kümmern. NAT-Adapter sind z.B. sehr nützlich, um aus virtuellen Maschinen heraus die funktionierende Modem-, ISDN- oder UMTS-Verbindung des Host-PC mit zu benutzen, obwohl eine VM gar keine entsprechende Hardware unterstützt.

**Unter falscher  
Flagge**

Wie bei NAT üblich, ist es allerdings nicht möglich, die Gäste vom LAN aus direkt anzusprechen, da die Adressen hinter dem NAT-Router verborgen bleiben. Nur VMware bietet dazu auch *Portforwarding* (*Portweiterleitung*). Damit lassen sich Anfragen auf bestimmten Ports über den NAT-Router zur dahinter liegenden VM weiterleiten. Virtual Server hat keine eingebaute NAT-Funktion, kann aber mit der Internet-Verbindungsfreigabe auf dem Host arbeiten. Solche erweiterten Funktionen benötigen Sie nicht sofort, ich beschreibe sie in *Teil 3, Kapitel 2*.

**Portforwarding**

### 1.2.5 Anschlussart der virtuellen Netzwerkkarten im laufenden Betrieb ändern

Die Anschlussart jeder virtuellen Netzwerkkarte können Sie im laufenden Betrieb einfach umschalten, wobei der Gast meint, ein Patchkabel wurde umgesteckt. So kann eine Maschine schnell zum Testen ans LAN angeschlossen werden und lässt sich bei Problemen mit einem Mausklick sofort wieder isolieren.

### 1.2.6 DHCP-Server in den virtuellen Netzwerken

Um Ihnen die Arbeit mit den virtuellen Netzwerken möglichst einfach zu machen, bieten alle Produkte interne DHCP-Dienste an. Diese virtuellen DHCP-Server verteilen in den virtuellen Netzwerken IP-Adressen aus konfigurierbaren Bereichen und liefern auch die

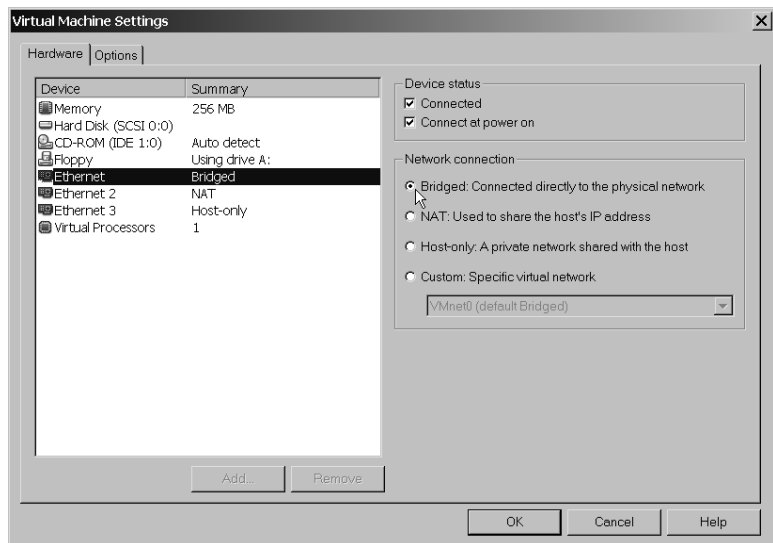


richtigen Einstellungen für das Default-Gateway und den DNS-Server gleich mit. Dadurch ist es nicht unbedingt notwendig, dass Sie in den Gästen IP-Einstellungen konfigurieren, um schnell eine Verbindung herzustellen. Die meisten Gastbetriebssysteme stellen eine neue Netzwerkkarte automatisch so ein, dass diese versucht, ihre IP-Einstellungen von einem DHCP-Server zu beziehen. Ich gehe nach dem Überblick über alle Funktionen weiter unten noch detaillierter auf das Thema ein, wie Gäste ihre IP-Einstellungen beziehen können.

### 1.3 Die Konfiguration virtueller Netzwerkkarten unter VMware

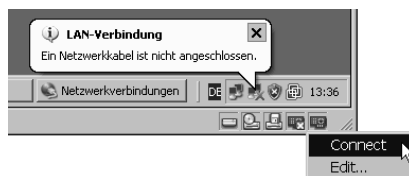
Unter VMware können Sie virtuelle Netzwerkkarten zu jedem Gast über VM/SETTINGS/HARDWARE hinzufügen und konfigurieren (Abbildung 1.6).

Abbildung 1.6:  
Jede Netzwerkkarte  
kann mit unter-  
schiedlichen  
Anschlusstypen  
konfiguriert  
werden



Einstellungen für eine spezielle Netzwerkkarte lassen sich jederzeit im laufenden Betrieb ändern, am einfachsten über das kleine Symbol unten rechts in der Statusleiste jeder VM (Abbildung 1.7). Das funktioniert über die Remote-Konsole beim VMware Server genauso wie bei VMware Workstation.

Abbildung 1.7:  
Ein kleines Symbol  
in der Statusleiste  
ermöglicht den  
schnellen Zugriff  
auf die Einstellun-  
gen der Geräte



Folgende Einstellungen stehen für jeden Adapter unter VMware zur Verfügung (Abbildung 1.6):

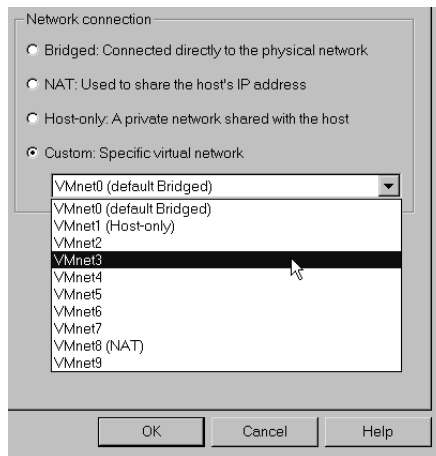
- ▶ *Connected/Not Connected* – Der virtuelle Adapter kann jederzeit angeschlossen oder abgehängt werden. Wenn der Haken am Eintrag *Connected* nicht gesetzt ist, wirkt das für den Gast, als wäre das Kabel von der virtuellen Netzwerkkarte abgezogen. Mit *Connect at power on* bestimmen Sie, ob die Netzwerkkarte beim Einschalten der VM automatisch verbunden wird oder nicht.
- ▶ *Bridged* – Standardmäßig setzt VMware jede neue virtuelle Netzwerkkarte auf den Typ *Bridged*. Dieser Adapter kommuniziert über eine physische Netzwerkkarte des Host-PC mit dem LAN. Sind mehrere physische Netzwerkkarten vorhanden, wählt VMware eine davon automatisch aus. Explizit zuweisen lassen sich bestimmte physische Netzwerkkarten über die erweiterten Optionen von EDIT/VIRTUAL NETWORK SETTINGS (siehe *Teil 3, Kapitel 2*).
- ▶ *NAT* – Eine virtuelle Netzwerkkarte vom Typ *NAT* kann unter der Identität des Host-PC unerkannt das Internet oder das LAN erreichen. NAT-Adapter können die gesamte IP-Konfiguration automatisch über den internen DHCP-Dienst von VMware beziehen. Für einen virtuellen Server, z.B. einen Webserver in einem Gast, ist die Verwendung eines NAT-Adapters allerdings umständlich, da der Gast vom LAN aus nur mittels Portweiterleitung (*Portforwarding*) erreicht werden kann. Diese Weiterleitung muss separat konfiguriert werden (siehe *Teil 3, Kapitel 2*). Meist ist für virtuelle Server ein Bridged-Adapter die bessere Wahl und wesentlich unkomplizierter.
- ▶ *Host-only* – Eine Karte im Modus *Host-only* ermöglicht die uneingeschränkte Kommunikation der VM mit dem Host auch ohne physische Netzwerkkarte. Dazu installiert VMware auf dem Host automatisch den virtuellen Adapter *VMware Network Adapter VMnet1*. Dieser ist am gleichen internen Netz angeschlossen wie alle anderen VMs mit *Host-only-Adapter*, wodurch diese VMs und der Host untereinander kommunizieren können. Auch in diesem Netz verteilt VMware per DHCP automatisch IP-Adressen, wodurch die Kommunikation mit dem Host auf Anhieb funktionieren sollte.

Ist eine VM bereits mit einem Bridged-Adapter ausgestattet, so kann sie zusätzlich zum LAN auch mit dem eigenen Host kommunizieren, ein zusätzlicher Host-only-Adapter ist nicht notwendig. Wird allerdings das LAN-Kabel vom physischen Adapter des Host-Rechners abgezogen, so deaktivieren einige Betriebssysteme die Netzwerkkarte. Dadurch können die Gäste nicht mehr über den Bridged-Adapter mit dem Host kommunizieren. In diesem Falle können Sie als Ausweg einfach den Anschlusstyp von Bridged auf Host-only umstellen.



- VMnet0–VMnet9** ► *Custom* – Die flexibelste Konfiguration ermöglicht unter VMware ein Adapter im Modus *Custom*. Dazu stehen intern zehn virtuelle VMnet-Switches bereit (VMnet0–VMnet9), an die Sie die Custom-Adapter beliebig anschließen können (Abbildung 1.8). Ein virtueller Switch bildet dabei ein internes Netzwerk, nur VMs am gleichen Switch sehen sich direkt. Hauptsächlich werden Sie am Anfang mit diesem Adaptertyp völlig abgeschottete Testnetzwerke aufbauen. Mehrere VMs können am gleichen virtuellen VMnet-Switch ungestört miteinander kommunizieren, ohne dass ein einziges Packet nach draußen gelangt. Wählen Sie dazu ein unbelegtes VMnet, z.B. VMnet3.

Abbildung 1.8:  
Es stehen zehn  
virtuelle Netzwerke  
zur Verfügung, um  
komplexe Netz-  
werke aufzubauen



Der Typ *Custom* ist eigentlich die grundlegende Konfiguration unter VMware. Die separaten Konfigurationstypen *Bridged*, *NAT* und *Host-Only* existieren nur für eine intuitivere Bedienung. Sie lassen sich allesamt genauso im Modus *Custom* abbilden. Ein Adapter an VMnet0 ist beispielsweise genau das Gleiche wie ein *Bridged*-Adapter. Zu diesen tiefgreifenderen Konfigurationen lesen Sie mehr in Teil 3, Kapitel 2.

### 1.3.1 Ausblick auf die erweiterte Netzwerkkonfiguration unter VMware

Im Menüpunkt **EDIT/VIRTUAL NETWORK SETTINGS** in der Workstation bzw. **HOST/VIRTUAL NETWORK SETTINGS** in der Remote-Konsole des Servers finden Sie schon einen Ausblick auf die volle Funktionalität der Netzwerkkonfiguration von VMware (Abbildung 1.9). Dieser Menüpunkt existiert nicht auf einem Linux-Host!

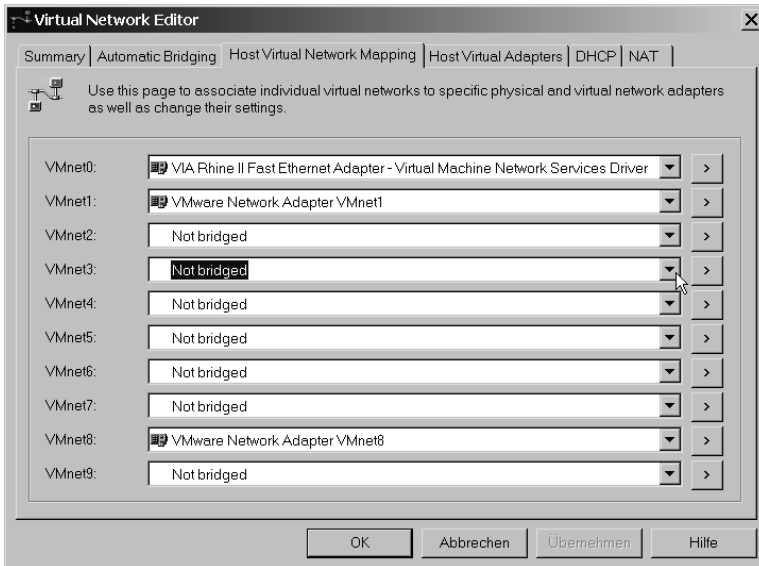


Abbildung 1.9:  
Die erweiterten  
Möglichkeiten der  
virtuellen Netz-  
werke werden für  
einfache Umgebun-  
gen nicht sofort  
benötigt

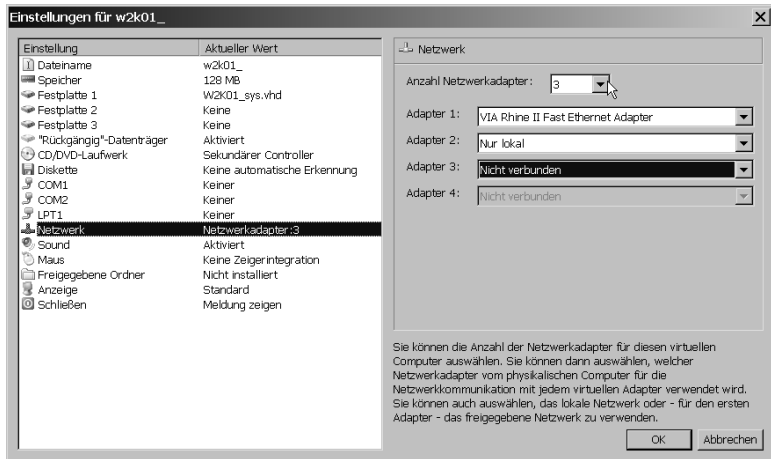
Hier ist es möglich, für einen NAT-Adapter Portforwarding zu konfigurieren, der DHCP-Bereich für jedes interne Netz kann geändert werden, und bei mehreren physischen Netzwerkkarten im Host lässt sich genau festlegen, über welche die Gäste mit dem LAN kommunizieren. Sie benötigen all diese Einstellungen für den Anfang noch nicht. Um schnell und unkompliziert einige VMs als Testumgebung zu vernetzen oder um einem Gast LAN-Zugriff zu gewähren, genügen die eben besprochenen vorkonfigurierten Einstellungen *Bridged*, *NAT* und *Host-only*. Sie finden eine ausführliche Diskussion in *Teil 3, Kapitel 2*.

## 1.4 Die Konfiguration virtueller Adapter unter Microsoft Virtual Server und Virtual PC

Auch Microsoft unterstützt die oben beschriebenen Konfigurationen. Die Einstellungen von Virtual PC und Virtual Server haben teilweise leicht unterschiedliche Bezeichnungen. Unter Virtual PC finden Sie die Einstellungen zu den einzelnen Netzwerkkarten einer VM in der Virtual PC-Konsole unter *EINSTELLUNGEN* oder im Menü der laufenden VM unter *BEARBEITEN/EINSTELLUNGEN* (Abbildung 1.10).

**Virtual PC**

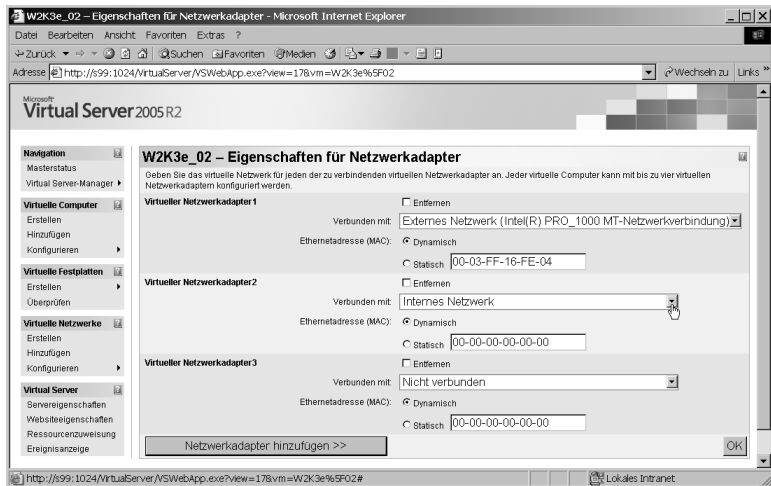
Abbildung 1.10:  
Virtual PC kann  
jeder VM vier Netz-  
werkarten mit  
unterschiedlichen  
Anschlussstypen  
zuweisen



### Virtual Server

Beim Virtual Server erfolgt die Konfiguration in der Verwaltungswebseite (Web-Interface) über das Menü VIRTUELLE COMPUTER/KONFIGURIEREN/NAME DER VM. Unter NETZWERKADAPTER finden Sie dann die Einstellungen (Abbildung 1.11). Beim Virtual Server stehen nur die ersten drei der unten aufgeführten Anschlussstypen zur Auswahl, kein NAT.

Abbildung 1.11:  
Beim Virtual Server  
konfiguriert man die  
virtuellen Adapter  
und Anschluss-  
typen über die  
Verwaltungsweb-  
seite



Folgende Anschlussstypen stehen für Gäste unter Microsoft zur Verfügung (Abbildung 1.10 und Abbildung 1.11):

- *Nicht verbunden* – Die Einstellung *Nicht verbunden* wirkt, als wäre das Kabel von der virtuellen Netzwerkkarte abgezogen worden. Es ist keinerlei Datenverkehr aus dem Gast möglich, obwohl der virtuelle Adapter in der VM weiterhin vorhanden ist.
- *Externes Netzwerk (Name einer physischen Host-Netzwerkkarte)* – Aus der Liste zu jedem virtuellen Adapter können Sie eine physische

Host-Netzwerkkarte auswählen. Der virtuelle Adapter kommuniziert über diese Netzwerkkarte des Host-PC mit dem LAN. Unter Virtual PC gibt es keinen eigenen Namen für diesen Anschlusstypen, Sie wählen einfach eine physische Netzwerkkarte aus der Liste. Beim Virtual Server wählen Sie ein *externes Netzwerk*, das standardmäßig den Namen der zugehörigen physischen Host-Netzwerkkarte trägt. Die Zuweisung der physischen Adapter an die externen Netzwerke hat Virtual Server bei der Installation automatisch vorgenommen.

- ▶ *Internes Netzwerk (Nur lokal)* – Alle VMs mit diesem Adaptertyp können nur intern miteinander kommunizieren, ohne jeden Kontakt zur Außenwelt. Virtual PC verfügt nur über ein einziges internes Netzwerk. Virtual Server bietet zwar standardmäßig ebenfalls nur ein internes Netz an, Sie können aber nachträglich weitere interne Netzwerke im Web-Interface über VIRTUELLE NETZWERKE/ERSTELLEN hinzufügen, um komplexere Umgebungen abzubilden. Für den Anfang genügt ein internes Netzwerk.
- ▶ *Gemeinsames Netzwerk (NAT)* – Der Typ NAT existiert nur bei Virtual PC. Im Gegensatz zu VMware können die mit NAT konfigurierten VMs intern nicht miteinander kommunizieren, sondern sie können nur das Internet oder das LAN aus dem internen Netzwerk erreichen. Dabei bleiben die Gäste voneinander isoliert und bilden kein internes gemeinsames Netzwerk.

**NAT-Adapter sind voneinander isoliert**

Sollten Sie eine NAT-Verbindung auch unter Microsoft Virtual Server benötigen, weil Sie z.B. keine freien IP-Adressen im LAN für die VMs haben, dann können Sie NAT etwas umständlich mit einem *Microsoft Loopbackadapter* und der *Internet-Verbindungsfreigabe* auf dem Host realisieren – lesen Sie dazu *Teil 3, Kapitel 2*.



### 1.4.1 Kommunikation mit dem Host (Host-only) über den Microsoft Loopbackadapter

Eine Einstellung *Host-only*, wie bei VMware, gibt es weder unter Virtual PC noch unter Virtual Server. Dadurch ist eigentlich keine Kommunikation der Gäste mit dem Host möglich, wenn keine physische Netzwerkkarte vorhanden ist bzw. wenn die Verbindung vom Host zur VM nur intern erfolgen soll. Um trotzdem eine Kommunikation der VMs mit dem Host ohne physische Netzwerkkarte zu ermöglichen, können Sie den schon erwähnten *Microsoft Loopbackadapter* verwenden. Dieser Adapter hat mit virtuellen Maschinen eigentlich nichts zu tun, er gehört bereits zum Lieferumfang von Windows mit dazu. Sie können ihn ganz einfach über SYSTEMSTEUERUNG/HARDWARE als neue Hardware vom Typ NETZWERKADAPTER installieren (eine detaillierte Anleitung finden Sie wieder in *Teil 3, Kapitel 2*). Der Microsoft Loopbackadapter stellt sich auf dem Host wie eine physi-

sche Netzwerkkarte dar, obwohl dazu keine Hardware existiert, und kann unter Virtual PC/Server als ein physischer Adapter ausgewählt werden. Darüber kommunizieren die Gäste mit dem Host auch ohne LAN-Verbindung (siehe auch Abbildung 1.4).

## 1.5 Anwendungsbeispiele für den Einsatz aller Anschlusstypen der Produkte

### Einsatzzweck und Beispiele

So viel zur Theorie. Sie haben jetzt einen Überblick über die Möglichkeiten virtueller Adapter in den Gästen. Vielleicht fragen Sie sich, wozu man diese Vielzahl von Optionen benötigt? Am einfachsten zu verstehen ist der Sinn anhand konkreter Einsatzfälle. Sie haben ein bestimmtes Problem zu lösen – hier ist der richtige Anschlusstyp! Die Einsatzszenarien sind unabhängig vom Produkt – vor dem Schrägstrich finden Sie die VMware-Bezeichnungen, dahinter die von Microsoft.

### 1.5.1 Einsatzbeispiele für extern angeschlossene Adapter (Bridged/externes Netzwerk)

Verwendung und Eigenschaften auf einen Blick:

- ▶ Virtuelle Server direkt im LAN bereitstellen.
- ▶ Virtuelle Clients vollwertig ins LAN integrieren.
- ▶ Transparenter Zugriff auf Ethernet-Geräte, z.B. DSL-Modems.
- ▶ Gäste sind von außen uneingeschränkt erreichbar.
- ▶ Gäste treten im LAN auf wie physische PCs.
- ▶ Gäste benötigen freie IP-Adressen aus dem LAN.

### Server im LAN bereitstellen

Bridged-Adapter werden immer dann verwendet, wenn eine VM uneingeschränkt direkt im physischen LAN erscheinen soll. Das ist in Produktionsumgebungen der Fall, wenn die VM im Netzwerk als Server auftritt, aber auch im Heimbereich, wenn die VM direkt über einen DSL-Router mitsurfen soll. So können Sie einen Webserver, einen Terminalserver oder einen Fileserver im LAN bereitstellen. Mehrere VMs und auch der Host können gleichzeitig dieselbe physische Netzwerkkarte verwenden und treten dabei als separate Rechner im LAN auf. Gäste lassen sich aber auch auf unterschiedliche physische Adapter aufteilen, z.B. aus Performancegründen oder wegen unterschiedlicher LAN-Segmente im physischen Netzwerk.

Ein weiterer Einsatzzweck für Bridged-Adapter kann die direkte Anbindung eines DSL-Modems über PPPoE an eine VM sein. Mit einem Adapter in diesem Modus ist es möglich, völlig transparent auf angeschlossene Ethernet-Geräte zuzugreifen. In *Teil 2, Kapitel 3, „Virtuelle DMZ mit Firewall und Webserver im Internet“*, wird damit eine Firewall betrieben.

**DSL-Modem  
über PPPoE**

### 1.5.2 Einsatzbeispiele für intern angeschlossene Adapter (Custom/lokal/internes Netzwerk)

Verwendung und Eigenschaften auf einen Blick:

- ▶ Interne abgeschottete Testnetzwerke zwischen Gästen aufbauen.
- ▶ Aufbau einer virtuellen DMZ.
- ▶ Verwendung als Heartbeat-Netzwerk eines virtuellen Clusters auf dem gleichen Host.
- ▶ Die VMs können nur untereinander kommunizieren, das LAN wird nicht gestört.
- ▶ Es ist keine physische Netzwerkkarte im Host notwendig.

Wenn Sie ein Netzwerk benötigen, in dem mehrere virtuelle Maschinen untereinander kommunizieren sollen, ohne Pakete ins reale LAN zu entlassen, dann können Sie solche internen Adapter verwenden. So kann z.B. eine Kopie der realen Produktionsserver samt Clients als Pilotumgebung in einer eigenen abgeschotteten virtuellen Welt existieren, ohne dass die Doubles im LAN für Chaos sorgen. Durch die Möglichkeit, mehrere VMs an unterschiedliche virtuelle Netze anzuschließen (nicht bei Virtual PC), können komplexe interne Netze mit VMs als Router aufgebaut werden. Unter VMware hat der Custom-Modus viele weitere Funktionen (siehe *Teil 3, Kapitel 2*).

**Abgeschottete  
Testumgebung  
oder DMZ**

### 1.5.3 Einsatzbeispiele für Host-only/ Microsoft Loopbackadapter

Verwendung und Eigenschaften auf einen Blick:

- ▶ Unterwegs im Zug, im Hotel oder beim Kunden auf dem Laptop die eigene virtuelle Testumgebung erreichen.
- ▶ Uneingeschränkte Kommunikation der Gäste nur mit dem Host ermöglichen.
- ▶ Virtuelle LAN-Segmente mit eigenem IP-Adressbereich über den Host ins LAN routen.
- ▶ Es ist keine physische Netzwerkkarte im Host notwendig.

Das Host-only-Netz ist für eine Verbindung der VMs mit dem Host vorgesehen, etwa zum Datenaustausch, aber auch für Entwickler, die Ihren eigenen Webserver oder SQL-Server usw. gleich „im Bauch“ Ihres Laptops laufen lassen wollen, z.B. unterwegs oder beim Kunden.

**Entwicklungs-  
umgebung auf  
dem Laptop**



Ein Host-only-Adapter kann auch als weitere Netzwerkkarte zusätzlich zu einem Bridged-Adapter verwendet werden, um bestimmte Testszenarien aufzubauen. Wir benutzen diese Kombination z.B. im Workshop in Teil 2, Kapitel 3, „*Virtuelle DMZ mit Firewall und Webserver im Internet*“, um den Host abgeschottet vom LAN auf die DMZ zugreifen zu lassen.

### 1.5.4 Einsatzbeispiele für NAT-Adapter

Verwendung und Eigenschaften auf einen Blick:

- ▶ Aus einem Gast die bestehende UMTS-, Modem- oder ISDN-Verbindung des Hosts mitbenutzen.
- ▶ Gäste vor dem LAN verstecken.
- ▶ Der Gast erreicht uneingeschränkt das LAN oder das Internet, ist aber von außen nicht erreichbar und bleibt im LAN unsichtbar.
- ▶ Der Gast benötigt nur eine interne IP-Adresse aus einem virtuellen Netzwerk. Der Aufbau des physischen LAN muss nicht bekannt sein.
- ▶ Durch einen internen DHCP-Server ist die Gastkonfiguration sehr einfach.
- ▶ NAT funktioniert nur, wenn der Host eine funktionierende LAN- oder Internet-Verbindung hat.

**Internet-Zugang  
mitbenutzen bei  
LAN, ISDN oder  
UMTS**

Eine NAT-Verbindung wird in der Praxis eher seltener eingesetzt, meist kann dafür eine flexiblere externe Verbindung (bridged/externes Netzwerk) verwendet werden, um Gäste ins LAN oder ins Internet zu bringen. Immer dann, wenn man entweder keine freie IP-Adresse aus dem LAN zur Verfügung hat bzw. wenn die VM nur als heimlicher Zaungast am Netzwerkverkehr teilnehmen soll, können Sie einen Adapter im Modus NAT verwenden. Vorausgesetzt der Host hat bereits eine Verbindung zum LAN oder ins Internet, so haben Sie sich in der VM um nichts weiter zu kümmern. Vor allem den ISDN-, Modem- oder UMTS-Zugang des Hosts kann der Gast auf diese Weise ganz einfach mitbenutzen, obwohl spezielle ISDN- oder UMTS-Hardware in einer VM gar nicht unterstützt wird. Großer Nachteil von NAT: Die VM ist nicht von außen zu erreichen, um z.B. Dienste wie VNC oder Remotedesktop in den Gästen anzusprechen. Nur VMware bietet dazu Portforwarding an.

## 1.6 Die Netzwerkkonfiguration und die IP-Adressen in den Gastsystemen

Über die Optionen der Virtualisierer haben Sie nun einen Überblick, aber auch im Gastbetriebssystem der VM müssen Einstellungen getroffen werden. Wo bekommt der Gast seine IP-Adresse her, über welches Gateway kommt er ins Internet, welchen DNS-Server kann er zur Namensauflösung verwenden? Die Treiber der virtuellen Netzwerkkarten werden unter VMware und unter Microsoft von fast allen Betriebssystemen automatisch erkannt und installiert. Die Konfiguration der IP-Adressen und der sonstigen Einstellungen hängt dann aber von Ihrem Ermessen ab.

**Treiber und IP-Adressen**

### 1.6.1 Automatische IP-Konfiguration in den Gästen mittels DHCP

Die virtuellen Adapter können ihre Adressen automatisch beziehen. Nach einer neuen Betriebssysteminstallation ist das praktischerweise immer die Standardeinstellung aller erkannten Netzwerkkarten in den Gästen (Abbildung 1.12).

**IP-Adressen automatisch zuweisen**

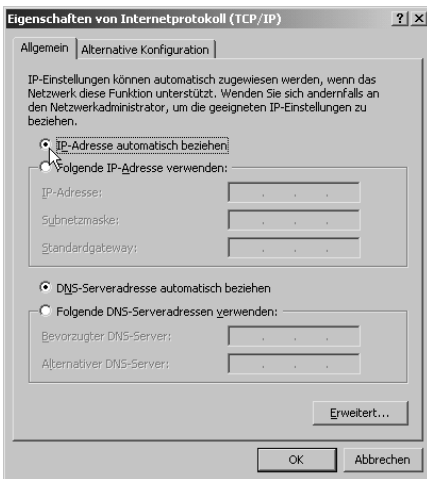


Abbildung 1.12:  
Am einfachsten  
bezieht ein Gast seine  
IP-Konfiguration  
von einem DHCP-  
Server. Adressen las-  
sen sich auch manu-  
ell festlegen

### Externe DHCP-Server im LAN

Soll ein extern angeschlossener Adapter (bridged/externes Netzwerk) die IP-Einstellungen automatisch beziehen, dann sollte im LAN ein DHCP-Server existieren. Im Firmennetz ist das obligatorisch, im Heimbereich verteilen die meisten DSL-Router Adress-einstellungen automatisch.

## Interne DHCP-Dienste in den virtuellen Netzwerken

In den internen virtuellen Netzwerken von VMware und Microsoft laufen DHCP-Dienste, welche die richtigen IP-Adressen samt Default-Gateway und DNS-Einstellungen für die Gäste verteilen. Ich beschränke mich in diesem Schnellstart auf die notwendigsten Funktionen, die für die meisten Anwendungsfälle ausreichend sind – tiefere Einblicke liefert Ihnen bei Interesse das *Teil 3, Kapitel 2*.

### DHCP unter VMware

Unter VMware sind die DHCP-Dienste schon für die vorkonfigurierten Netzwerke Host-only und NAT funktionsfähig installiert. Sie werden eher selten Änderungen an den Einstellungen vornehmen müssen und können dadurch DHCP in den Gästen unter VMware sofort benutzen, wenn Sie keine IP-Adressen manuell vergeben wollen. So funktioniert z.B. der NAT-Zugriff aus einem Gast über den Host ins Internet auf Anhieb. VMware verteilt Adressen aus automatisch ausgewählten freien Class-C-Netzwerken, z.B. 192.168.72.x.

### DHCP unter Virtual Server

Unter Virtual Server muss der DHCP-Server eines internen Netzwerks unter VIRTUELLE NETZWERKE / KONFIGURIEREN / INTERNES NETZWERK / DHCP-SERVER erst eingeschaltet werden (Abbildung 1.13). Sie können die Vorgaben von Virtual Server der Einfachheit halber gleich übernehmen oder auch einen eigenen Adressbereich festlegen.

Abbildung 1.13:  
Der DHCP-Server  
muss unter Virtual  
Server auch für die  
internen Netze erst  
aktiviert werden

| Internes Netzwerk – Eigenschaften von DHCP-Server |                                               |
|---------------------------------------------------|-----------------------------------------------|
| <b>Virtueller DHCP-Server</b>                     | <input checked="" type="checkbox"/> Aktiviert |
| Netzwerkadresse:                                  | 10.237.0.0                                    |
| Netzwerkmaske:                                    | 255.255.0.0                                   |
| IP-Startadresse:                                  | 10.237.0.16                                   |
| IP-Endadresse:                                    | 10.237.255.254                                |
| Adresse des virtuellen DHCP-Servers:              | 10.237.0.1                                    |
| Standardgatewayadresse:                           |                                               |
| DNS-Server:                                       |                                               |
| WINS-Server:                                      |                                               |
| IP-Adressen-Leasezeitraum:                        | 36 Stunden                                    |
| Lease-Erneuerungszeitraum:                        | 18 Stunden                                    |
| Lease-Neueinbindungszeitraum:                     | 27 Stunden                                    |
| OK                                                |                                               |



Wenn Sie einen virtuellen DHCP-Server an einem Bridged- bzw. externen Netzwerk freischalten, verteilt dieser auch IP-Adressen im LAN. Das kann den Betrieb Ihres Netzwerks stören, wenn sich dadurch physische Clients IP-Adressen aus dem falschen Netzwerkbereich abholen oder wenn die Bereiche sogar kollidieren. Aktivieren Sie DHCP-Server also möglichst nur in den internen Netzwerken.

Virtual PC bietet nur für NAT-Adapter einen internen DHCP-Dienst, dieser liefert nur Adresse aus dem festen voreingestellten Bereich 192.168.131.x.

### 1.6.2 Manuelle IP-Konfiguration in den Gästen

Sie können die IP-Einstellungen aller Adapter in den Gästen auch manuell vornehmen. Das ist z.B. bei virtuellen Servern sinnvoll, um diese über eine unveränderliche IP-Adresse ansprechen zu können. Für extern angeschlossene Adapter (bridged/externes Netzwerk) benötigen Sie dazu eine freie IP-Adresse aus dem Netzwerkbereich Ihres LAN. Gegebenenfalls sollten Sie zusätzlich die richtigen Adressen für das Default-Gateway und für den DNS-Server kennen, wenn Sie das Internet oder andere Standortnetze aus dem Gast heraus erreichen wollen.

Für die internen virtuellen Netzwerke können Sie Ihre Adressen selbst verwalten und beliebige Adressbereiche verwenden. Sie sollten aber darauf achten, einen anderen Netzwerkbereich als Ihr physisches LAN zu benutzen, für den Fall, dass doch einmal eine VM in den Modus bridged/extern umgeschaltet wird, wodurch dann im LAN doppelte IP-Adressen auftauchen könnten. Weiterhin kann Routing zwischen IP-Netzwerken nur funktionieren, wenn alle beteiligten Netzwerke eindeutige Adressbereiche verwenden.

**IP-Adressen  
manuell ver-  
geben**

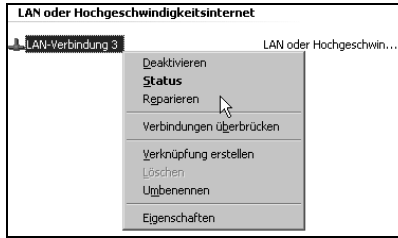
Für die Verwendung von virtuellen Netzwerken benötigen Sie ein minimales Grundwissen über das Protokoll TCP/IP. Sie erhalten in *Teil 3, Kapitel 2*, einen Überblick, wie eine IP-Adresse aufgebaut ist, sollten Sie bisher noch nicht mit Netzwerken gearbeitet haben.



### 1.6.3 Anpassung der Gast-IP nach einem Wechsel des Anschlusstyps im laufenden Betrieb

Wie Sie bereits erfahren haben, kann der Modus der virtuellen Netzwerkkarte im laufenden Betrieb von *Bridged* auf *NAT*, von *Lokal* auf *Nicht angeschlossen* usw. gewechselt werden. Die VM meint, das Anschlusskabel wurde umgesteckt oder abgezogen. Dabei muss das Gastbetriebssystem an die neuen Gegebenheiten angepasst werden. Der Wechsel von Bridged auf NAT bedeutet schließlich einen Wechsel des Netzwerks und damit des Adressbereiches. Ein Wechsel des Typs kann z.B. notwendig sein, wenn Sie eine VM aus dem virtuellen Netzwerk ins physische LAN bringen wollen, um vorbereitete Funktionen zu testen, oder wenn Sie diese VM wieder isolieren möchten.

Abbildung 1.14:  
In Windows-Gästen  
kann die Erneue-  
rung der IP-Konfi-  
guration über die  
Netzwerkumge-  
bung erfolgen



#### DHCP neu abfragen

Bei manueller Konfiguration der IP-Adressen müssen Sie die Einstellungen der Adapter selbst ändern und neue Adressen sowie Gateway-Einstellungen eintragen. Dagegen muss bei Adaptern, die ihre Adresse per DHCP beziehen, in der VM nur die IP-Konfiguration neu abgefragt werden. Das erfolgt unter Windows mit dem DEAKTIVIEREN und erneutem AKTIVIEREN des Adapters in der Netzwerkumgebung über die rechte Maustaste bzw. über den Punkt REPARIEREN (Abbildung 1.14). Am sichersten funktioniert das Neuabfragen der IP-Einstellungen manuell in einer DOS-Box mit folgenden Befehlen:

```
ipconfig /release
ipconfig /renew
```

Unter Linux funktioniert es bei den meisten Distributionen an der Kommandozeile mit folgenden Befehlen:

```
ifdown eth0
ifup eth0

oder:

ifconfig eth0 down
ifconfig eth0 up
```

## 1.7 Ausblick und Erweiterungen zur Netzwerkkonfiguration

#### MAC-Adressen und mehrere Netzwerkkarten

Im Prinzip wissen Sie jetzt schon alles, was Sie benötigen, um virtuelle Maschinen schnell zu vernetzen. Wollen Sie spezielle Problemstellungen lösen oder einfach weiter hinter die Kulissen schauen, dann können Sie das in *Teil 3, Kapitel 2*. Dort sind u.a. die Verwaltung mehrerer physischer Netzwerkkarten, Portforwarding, MAC-Adressen und Performancefragen Themen.

#### Und Linux?

In *Teil 3, Kapitel 2*, erfahren Sie auch, wie das Netzwerk auf einem Linux-Host unter VMware individuell angepasst werden kann.

# 2 Virtuelle Netzwerke – die ganze Wahrheit

Einen Überblick über die Verwendung virtueller Netzwerke haben Sie bereits im Schnelleinstieg von *Teil 3, Kapitel 1, „Virtuelle Netzwerke Teil 1 – Schnellstart“*, bekommen. Mit den dort erläuterten Standardmethoden gelangen Sie schnell zum Ziel, ohne genau wissen zu müssen, wie es intern funktioniert. In diesem Kapitel werden wir dagegen tiefer in die Materie eindringen und uns nicht mehr mit den vorkonfigurierten Typen wie *NAT* oder *Host-only* zufrieden geben.

Nochmals der Hinweis: Wenn Sie folgenden Workshop nachvollziehen, dann schalten Sie bitte Firewalls in den Gastbetriebssystemen ab. Sonst kann es sein, dass Ihre Test-VMs nicht miteinander kommunizieren können, obwohl Sie alles richtig konfiguriert haben.



## 2.1 Allgemeine Netzwerkgrundlagen als Vorbereitung

Gleich zu Beginn werden wir einen kurzen Ausflug zu den allgemeinen Funktionen eines Netzwerks unternehmen. Ich beschränke mich dabei auf die notwendigsten Begriffe. Sie werden feststellen, dass viele Komponenten eines physischen Netzwerks auch in der virtuellen Welt auftauchen. Wenn Sie bereits sicher mit Begriffen wie *Switch*, *Router* oder *DHCP* umgehen, dann lesen Sie bitte gleich unter *Abschnitt 2.1.4, „Die Komponenten virtueller Netzwerke“*, weiter.

**Reale Netzwerke sind das Vorbild**

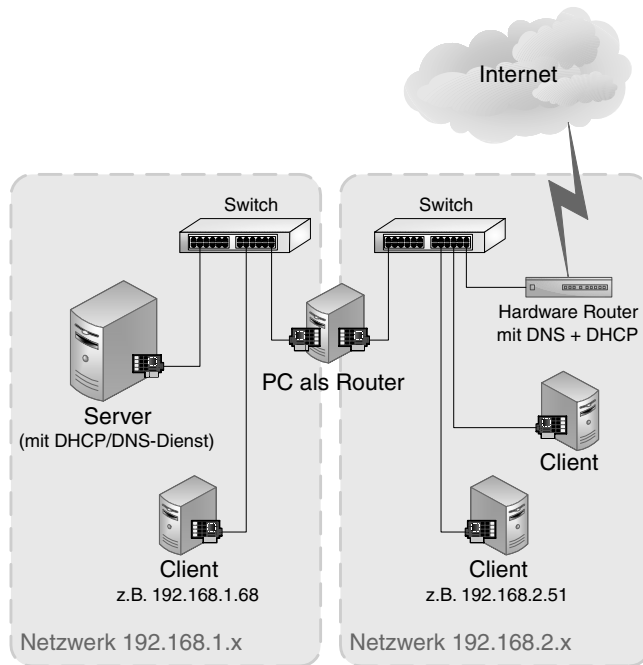
### 2.1.1 Einige grundlegende Komponenten eines Netzwerks

Vereinfacht betrachtet besteht ein Netzwerk unter anderem aus folgenden Komponenten (Abbildung 2.1):

- ▶ Geräte (Netzwerkclients), wie PCs oder Server, mit eingebauten Netzwerkkarten.
- ▶ Switches oder Hubs, an denen die Netzwerkkarten der Geräte angeschlossen sind.
- ▶ Komponenten und Dienste wie DHCP-Server, DNS-Server oder Router.
- ▶ Medien, wie Kabel oder Funkkanäle, die das Ganze verbinden.

Auf dieser Infrastruktur setzen die Protokolle auf, mit denen Netzwerkpakete zwischen den Teilnehmern (z.B. PC und Server) versendet werden. Die Pakete enthalten die eigentlichen Nutzdaten. Das derzeit am häufigsten verwendete Protokoll ist TCP/IP. Die Kommunikation erfolgt dort über IP-Adressen in der Form 192.168.1.1 oder 172.16.0.1. Weitere, nur noch wenig verwendete Protokolle sind IPX/SPX oder NetBEUI.

Abbildung 2.1:  
Der grundlegende  
Aufbau eines Netz-  
werks besteht aus  
Rechnern mit Netz-  
karten, Switches,  
Routern und Dienst-  
en wie DHCP



### 2.1.2 Kurze Einführung zum Aufbau einer IP-Adresse

Wenn Sie erfolgreich Testumgebungen mit mehreren virtuellen Adaptern in unterschiedlichen Netzwerken aufbauen wollen, benötigen Sie ein minimales Grundwissen über das Protokoll TCP/IP. Sie erhalten hier einen stark vereinfachten Überblick, wie eine IP-Adresse aufgebaut ist. Für tief greifendere Informationen sollten Sie zusätzliche Literatur konsultieren.

#### Netzwerkteil und Geräteteil

Eine IP-Adresse gliedert sich in den so genannten *Netzwerkteil* und den *Geräteteil*, auch Hostteil genannt. Der Netzwerkteil wird vom vorderen Abschnitt der IP-Adresse gebildet und bleibt im selben Netzwerk immer gleich. Zwischen verschiedenen Netzwerken muss der Netzwerkteil dagegen unterschiedlich und eindeutig sein. In jedem Netzwerk werden die einzelnen Clients mit dem hinteren Teil der IP-Adresse, dem Geräteteil, eindeutig adressiert.

Bei einer Beispieladresse 192.168.1.68 aus Abbildung 2.1 wird das Netzwerk eindeutig durch 192.168.1 dargestellt. Innerhalb dieses Netzwerks ist die 68 die eindeutige Adresse für den Adapter eines Gerätes, beispielsweise für einen LAN-Client. Jede Stelle einer IP-Adresse kann einen Wert von 0–255 annehmen, das hängt damit zusammen, dass die Werte intern binär mit 8 Bit (1 Byte) dargestellt werden. Es können damit im Beispiel theoretisch maximal 256 (0–255) Geräte pro Netzwerk adressiert werden. In der Praxis sind die Adressen 0 und 255 eines jeden Netzwerks allerdings reserviert und dürfen keinem Adapter zugewiesen werden, so dass nur 254 Geräte adressiert werden können.

Welcher Teil der IP-Adresse der Netzwerkteil ist und welcher Teil der Geräteteil, wird durch die so genannte *Subnetzmaske* (*Subnetmask*) bestimmt. In unserem Beispiel wäre die richtige Maske die 255.255.255.0, alle Stellen mit einer 255 entsprechen dem Netzwerkteil. Man nennt das auch ein Class-C-Netzwerk. Ein anderes Beispiel wäre eine Adresse aus einem so genannten Class-B-Netzwerk, etwa 172.16.25.31. Hier ist die Subnetzmaske die 255.255.0.0, was bedeutet, dass nur die ersten beiden Stellen das Netzwerk spezifizieren und dadurch zwei Bytes für die Adressierung der Geräte im Netzwerk übrig bleiben. Im Beispiel wäre das Netzwerk die 172.16 und der Client die 25.31. Class-B-Netzwerke kommen z.B. zum Einsatz, wenn mehr als 254 Clients adressiert werden müssen, in den Beispielen im Buch arbeiten wir immer mit Class-C-Netzwerken, also z.B. 192.168.1.68. Diese Beschreibung der Subnetzmaske ist sehr vereinfacht, genügt aber für die Beispiele im Buch.

#### Subnetzmaske

Alle Adapter an gleichen Netzwerken benötigen Adressen aus dem jeweils gleichen Netzwerkbereich mit der Angabe der passenden Subnetzmaske, um miteinander kommunizieren zu können. Verwendete Adressbereiche dürfen nicht mehrfach in unterschiedlichen Netzwerken benutzt werden, sie müssen immer eindeutig bleiben. Ansonsten können sich Konflikte ergeben, wenn z.B. ein internes Netzwerk plötzlich mit dem physischen LAN verbunden wird und dadurch doppelte IP-Adressen auftauchen. Auch wenn mehrere Netzwerke über Router verbunden werden sollen, funktioniert das nur, wenn alle beteiligten Netzwerke eindeutige Adressbereiche verwenden, in Abbildung 2.1 also die 192.168.1.x und 192.168.2.x. Darin unterscheidet sich ein virtuelles Netzwerk nicht von der realen Welt.

### 2.1.3 Das Zusammenspiel der Komponenten eines Netzwerks

Um später das Zusammenspiel der Netzwerkkomponenten virtueller Maschinen besser zu verstehen, sollten Sie einen groben Überblick über die Funktionen eines Netzwerks haben. Ich gebe Ihnen deshalb hier eine kurze Erklärung zu den Komponenten.



### Netzwerkkarten kommunizieren mittels IP-Adresse

Wenn ein PC Daten an einen anderen Rechner versenden will, dann werden die Daten in Pakete verpackt und mit einem bestimmten Protokoll (z.B. TCP/IP) über eine Netzwerkkarte versendet. Das Ziel ist meist ebenfalls ein Rechner mit einer Netzwerkkarte, welche die Pakete empfängt. Damit die Kommunikation zwischen den Teilnehmern im Netzwerk funktioniert, benötigt jeder teilnehmende Rechner (Client) für seine Adapter eindeutige IP-Adressen, z.B. 192.168.1.68.

### Ein Switch verbindet die Clients eines Netzwerks

Sollen die versendeten Netzwerkpakete eine Zieladresse erreichen, dann müssen beide Netzwerkkarten miteinander kommunizieren können. *Quellrechner und Zielrechner müssen am gleichen Netzwerk angeschlossen sein.* Meist werden dazu alle beteiligten Rechner über ein Kabel mit einem Switch oder Hub verbunden. Solche Geräte leiten die Pakete der angeschlossenen Clients intern weiter und verbinden die Teilnehmer. Alle Rechner am gleichen Switch bilden ein Netzwerk.



In der Praxis sind oft mehrere Switches direkt miteinander verbunden (*Uplink* oder *Stacking*), weil sonst die Anzahl der Anschlüsse (*Ports*) nicht ausreichen würde. Aber auch solch ein Verband kann als ein einziger großer Switch betrachtet werden.

### Router vermitteln Pakete aus unterschiedlichen Netzwerken

PCs an unterschiedlichen Switches sehen sich normalerweise nicht. Nur ein Router kann diese getrennten Netze verbinden. Oftmals ist das ein spezielles Gerät, ein Hardware-Router, der z.B. den Internet-Zugang bereitstellt. Auch ein PC mit zwei Netzwerkkarten an unterschiedlichen Netzwerken kann als Router dienen (Abbildung 2.1). Die Protokollsoftware des PC kann Pakete aus dem einen Netz ins andere übertragen, was auch als *Routing* bezeichnet wird. Welcher Router in einem Netzwerk zuständig für die Weiterleitung in ein anderes Netzwerk ist, das weiß jeder Client anhand einer Tabelle, der so genannten *Routing-Tabelle*. Dort schaut die Protokollsoftware nach, an welchen Router die Pakete zu senden sind, die ein bestimmtes Netzwerk erreichen sollen.

### Das Default-Gateway ist der zentrale Router eines Netzwerks

Wurde in der Routing-Tabelle für ein bestimmtes gesuchtes Zielnetz keine Route hinterlegt, dann werden die Pakete an jene IP-Adresse übermittelt, die als das so genannte *Default-Gateway* eingetragen ist. Das Gerät, das als Default-Gateway im Netzwerk dient, ist dann dafür zuständig, die Pakete weiter zu vermitteln und ins richtige Netzwerk oder an den nächsten Router zu senden. Z.B. kann ein Hardware-Router, der den Zugang ins Internet bereitstellt, das Default-Gateway für

ein LAN sein. Über ihn werden alle Pakete, die nicht in dieses LAN gehören, zu weiteren Routern im Internet übermittelt, die ihrerseits dafür sorgen müssen, dass die Pakete irgendwann ihr Ziel erreichen, z.B. einen bestimmten Webserver.

### **Mit DHCP werden IP-Adressen automatisch zugewiesen**

Jeder Client im Netzwerk benötigt eine eindeutige IP-Adresse, damit eine Kommunikation überhaupt erst möglich wird. Damit nicht alle PCs manuell konfiguriert werden müssen, können sie sich die Konfiguration automatisch von einem DHCP-Dienst abholen. Dieser Dienst verteilt IP-Adressen aus einem definierten Bereich, vermerkt sich ausgeteilte Adressen in einer Datenbank und liefert auch Einstellungen wie Default-Gateway und DNS-Server für das Netzwerk mit. DHCP läuft auf einem Gerät, das ebenfalls am gleichen Switch steckt, z.B. auf einem Server oder Hardware-Router.

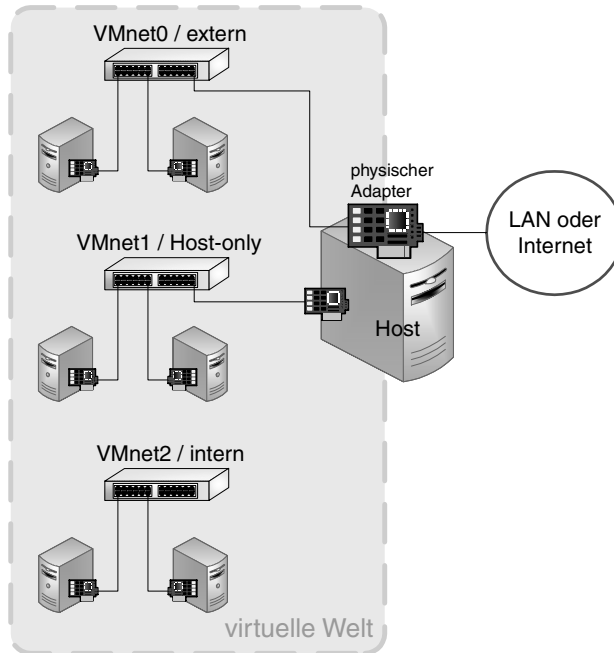
### **DNS löst Rechnernamen in die richtigen IP-Adressen auf**

Weil die Arbeit mit IP-Adressen für den Menschen sehr umständlich ist (oder wissen Sie, dass man die Webseite von VMware unter der Adresse 66.35.226.138 erreicht?), werden üblicherweise Rechnernamen verwendet, wie *www.vmware.com* oder einfach *mein\_pc01*. Die richtigen IP-Adressen zu diesen Namen stellt ein DNS-Server auf Anfrage einem Client zur Verfügung. Neben den IP-Adressen können manche DNS-Server auch Informationen zu wichtigen Diensten und Funktionen im Netzwerk liefern. z.B. spielt in einem Windows-Netzwerk mit Active Directory DNS eine zentrale Rolle.

## **2.1.4 Die Komponenten virtueller Netzwerke**

Jetzt kommen wir zur Sache – auch ein virtuelles Netz verfügt über die gleichen Komponenten wie ein physisches LAN. Die Gäste haben virtuelle Netzwerkkarten, die an virtuellen Switches angeschlossen sind (Abbildung 2.2). So bilden die VMs auf einem Host intern unterschiedliche virtuelle Netzwerke, allerdings ohne ein einziges Kabel. In diesen Netzwerken laufen Dienste, wie DHCP und DNS, ebenso können Router zwischen virtuellen Netzwerken Pakete weiterleiten. Zusätzlich existieren Schnittstellen zur Anbindung der VMs an die physische Welt, damit die Gäste auch mit dem LAN oder mit VMs auf anderen Hosts kommunizieren können. Diese Komponenten finden Sie bei allen Virtualisierungsprodukten, auch wenn sich die Bezeichnungen unterscheiden.

Abbildung 2.2:  
Der Anschluss an  
ein bestimmtes  
virtuelles Netzwerk  
entscheidet, ob die  
VM mit dem LAN  
kommunizieren  
kann



### Virtuelle Netzwerkkarten in den VMs

#### Virtuelle Patchkabel

VMware oder Microsoft emulieren bis zu vier Netzwerkkarten in einer VM. Unabhängig von der Hardware im Host findet das Gastbetriebssystem immer das gleiche emulierte Adaptermodell. Dazu muss nicht einmal eine physische Netzwerkkarte existieren, wenn sich die Gäste nur innerhalb der virtuellen Netzwerke unterhalten wollen (VMnet2 in Abbildung 2.2). Das kann sehr praktisch in Testumgebungen sein. Das Gastsystem „meint“, immer mit einem echten Adapter zu arbeiten, und kann keinen Unterschied feststellen. Im Gegensatz zu realen Adapters verfügen virtuelle Netzwerkkarten jedoch nicht über eine Buchse mit Kabel zu einem physischen Switch, sondern sie sind an virtuelle Switches (Netzwerke) gebunden.

### Virtuelle Netzwerkkarten auf dem Host

Ein Sonderfall der virtuellen Netzwerkkarten sind spezielle Netzwerkkartentreiber, die auf dem Host selbst installiert werden, ohne dass eine physische Netzwerkkarte dazugehört. Über diese Adapter ist der Host ebenfalls an die internen virtuellen Netzwerke angeschlossen, obwohl er gar keine VM ist (VMnet1 in Abbildung 2.2). Diese Host-Netzwerkkarten haben also ebenfalls keine physische Buchse nach draußen, sondern nur ein virtuelles Kabel nach drinnen in die emulierte Welt. Unter Microsoft ist das der *MS Loopbackadapter*, und unter VMware sind es die beiden Adapter *VMware Network Adapter VMnet1* und *8*, zu sehen in der Netzwerkkonfiguration des Host-PC. Ich komme später darauf zurück.

## Die virtuellen Switches

Es ist in der virtuellen Welt wie in jedem anderen LAN, unsere emulierten Netzwerkkarten sind intern an die Switches der Virtualisierer angeschlossen, um miteinander kommunizieren zu können. Ein virtueller Switch ist ein logisches Netzwerk, das alle angeschlossenen Gäste verbindet. Im konkreten Falle sind das *VMnet0* bis *VMnet9* unter VMware bzw. unter Microsoft ein *internes* oder *externes Netzwerk*. Wie schon erwähnt, kann auch der Host an diesen virtuellen Switches mit speziellen Host-Adaptern angeschlossen sein. Sogar physische Netzwerke des Wirts lassen sich einem virtuellen Switch zuweisen, wodurch eine Brücke ins LAN entsteht (siehe „Bridge-Protokoll – die vollwertige Verbindung zur realen Welt“).

## Der DHCP-Dienst in den virtuellen Netzwerken

DHCP-Server sind ebenfalls am gleichen virtuellen Switch (und damit Netzwerk) angeschlossen und verteilen IP-Adressen an die VMs. VMware und Microsoft lassen dazu eigene Dienste laufen. Theoretisch könnte aber auch eine VM mit installiertem DHCP-Dienst, z.B. ein Windows-Server, diese Arbeit in einem virtuellen Netzwerk übernehmen.

## Router zwischen virtuellen Netzwerken

Genauso wie physische Rechner in unterschiedlichen Netzwerken sich nicht sehen können, so sind auch VMs an unterschiedlichen virtuellen Switches voneinander isoliert. Nur Router können Pakete weiterleiten und die getrennten virtuellen Netzwerke verbinden. Routen kann z.B. ein Gast mit zwei virtuellen Adaptionern an verschiedenen virtuellen Switches. Damit können komplexe Testnetze entstehen.

Zusätzlich stellen einige Produkte, außer der VMware ESX Server und Microsoft Virtual Server, einen NAT-Dienst bereit, der als spezieller Router in die reale Welt fungiert und die so genannte *Netzwerk-Adressumsetzung* (NAT) beherrscht. Damit kann ein Gast z.B. mit dem LAN oder mit dem Internet kommunizieren, ohne selbst im physischen Netzwerk sichtbar zu werden.

**NAT-Router**

## Bridge-Protokoll – die vollwertige Verbindung zur realen Welt

In der virtuellen Umgebung funktioniert alles wie in einem richtigen Netzwerk, nur dass die Pakete ausschließlich innerhalb unserer Spiegelwelt bleiben. Wie gelangt der Verkehr eines Gastes aber ohne Einschränkungen ins physische LAN? Denn ein produktiver Server muss ja von den Clients auch erreicht werden können.

### Verbindung zur realen Welt

Sie wissen bereits, dass die VMs virtuelle Netzwerkkarten haben, die an virtuellen Switches angeschlossen sind. Zusätzlich zu den virtuellen Adaptern der Gäste kann jedem dieser Switches eine physische Netzwerkkarte des Hosts zugewiesen werden. Der virtuelle Switch ist dadurch mit einer Art *Uplink* mit einem physischen Switch verbunden, und es wird eine Kommunikation mit dem LAN möglich (VMnet0 in Abbildung 2.2). Das Bindeglied ist ein spezielles Protokoll auf dem Host, unter VMware das so genannte *VMware Bridge Protocol*, unter Microsoft die *Virtual Machine Network Services*. Über dieses Protokoll zapfen die Virtualisierer den Datenverkehr der physischen Netzwerkkarte an und leiten Pakete, die an Adressen virtueller Adapter gerichtet sind, ins virtuelle Netzwerk weiter. Umgekehrt tunnelt das Protokoll Pakete aus den VMs direkt auf die Hardware und damit ins LAN.



Die Bridge-Protokolle versetzen die physischen Netzwerkkarten in den so genannten *Promiscuous Mode*. In diesem Modus empfängt ein LAN-Adapter auch Pakete, die eigentlich nicht für seine physische MAC-Adresse (*MAC – Media Access Control*) bestimmt sind. Die MAC-Adresse einer Netzwerkkarte ist eine eindeutige Hardware-Nummer, über die auf der untersten Ebene die Kommunikation im Netzwerk abläuft. Auch IP-Adressen werden letztendlich bestimmten MAC-Adressen zugeordnet. Das Bridge-Protokoll kann dank *Promiscuous Mode* den LAN-Verkehr ins virtuelle Netzwerk übermitteln, und die Gäste empfangen die Pakete, die für ihre virtuellen Adapter bestimmt sind. Ohne diesen Trick würde der physische Adapter des Hosts nur solche Pakete entgegennehmen, die an ihn adressiert sind, und die VMs gingen leer aus.

### 2.1.5 Spezielles zu den virtuellen Netzwerken der unterschiedlichen Produkte

Ab hier scheiden sich die Geister, oder besser gesagt, die Produkte von VMware und Microsoft. Die grundlegende Logik der Netzwerkfunktionen ist zwar beinahe gleich, aber die Begriffsbezeichnungen und die Bedienung sind verschieden. Da es unübersichtlich ist, im laufenden Text immer beide Varianten zu beschreiben, vor allem beim komplexen Thema Netzwerke, habe ich die Hersteller getrennt. So müssen Sie nur das Kapitel für Ihr Produkt durcharbeiten. Die Kapitel zusammen bieten allerdings einen ausführlichen Überblick und Vergleich der Netzwerkfähigkeiten.

## 2.2 Virtuelle Netzwerke unter VMware

Für das tiefere Verständnis der Netzwerkfunktionalität von VMware lassen wir die Konfigurationstypen *Host-only*, *NAT* und *Bridged* links liegen und konzentrieren uns auf das Wesentliche, den *Custom*-Modus mit seinen virtuellen Switches *VMnet0-VMnet9* (Abbildung 2.3). Dieser Modus bietet die grundlegenden Netzwerkfunktionen unter VMware. Alle anderen Modi, die Sie schon aus *Teil 3, Kapitel 1*, kennen, sind nur voreingestellte Synonyme für eine einfache Bedienung. Sie werden gleich merken, dass ein Custom-Adapter an VMnet0 genau das Gleiche ist wie ein Bridged-Adapter. Ein Adapter an VMnet1 hat dieselbe Funktion wie Host-only, und einer an VMnet8 funktioniert, als wäre er mit NAT konfiguriert.

**Der Custom-Modus liefert alle Funktionen**

### 2.2.1 Unterschiede in der Netzwerkkonfiguration von VMware Workstation, Server und ESX

Die Grundlagen der Netzwerke sind bei VMware Workstation und VMware Server gleich. Sie unterscheiden sich hauptsächlich durch die Menüposition von VIRTUAL NETWORK SETTINGS. Unter der Workstation finden Sie den Punkt unter EDIT, in der Remote-Konsole vom Server dagegen unter HOST.

Auf einem Linux-Host fehlt das Menü VIRTUAL NETWORK SETTINGS vollständig. Die Konfiguration virtueller Netzwerke erfolgt dort über das Konfigurationsskript *vmware-config.pl*. Hinweise zur Linux-Konfiguration finden Sie in einem eigenen Abschnitt weiter unten.

**Linux-Host**

Der ESX Server unterscheidet sich stärker in der Bedienung, auch wenn die internen Netze und die Zuweisung von Netzwerkkarten von der Logik grundsätzlich gleich sind. Es gibt allerdings kein NAT und keine virtuellen Host-Adapter, und auch die Konfiguration erfolgt anders. Beachten Sie dazu den ESX-Workshop in *Teil 2, Kapitel 9*, „VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2“.

**ESX Server**

### 2.2.2 Virtuelle Netzwerkkarten unter VMware

Unter VMware können Sie den Gästen bis zu vier virtuelle Adapter zuweisen. Zusätzlich existieren auch auf dem Wirt selbst zwei virtuelle Netzwerkkarten, die den Host ebenfalls mit der emulierten Welt verbinden.

### Konfiguration der virtuellen Adapter in Gästen unter VMware

VMware Server bietet für jede VM maximal vier virtuelle Netzwerkkarten, die VMware Workstation unterstützt offiziell nur drei. Wenn Sie wirklich einmal vier Netzwerkkarten in einer VM unter VMware Workstation benötigen sollten, lässt sich das mittels Editieren der Konfigurationsdatei `*.vmx` realisieren. Fügen Sie einfach folgende Einträge hinzu:

```
Ethernet3.present = "TRUE"
ethernet3.connectionType = "hostonly" | "bridged" |
"nat"
```

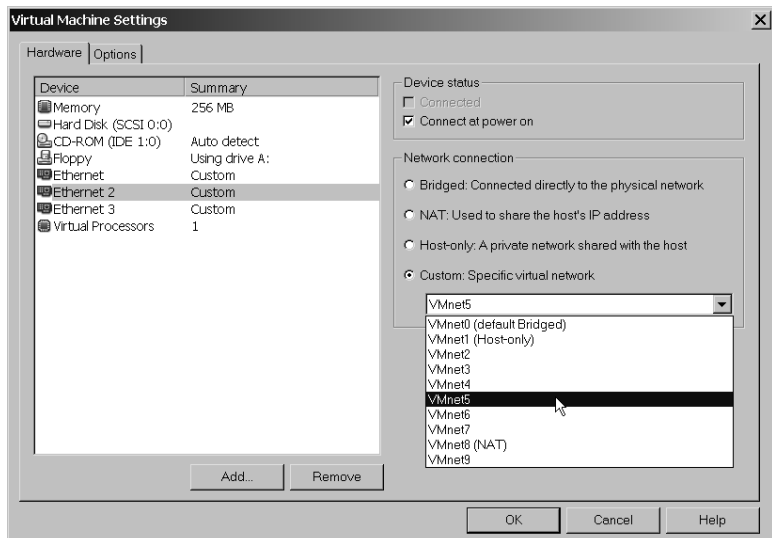
#### Konfiguration der Netzwerkkarten

Die Netzwerkkarten eines Gastes lassen sich über VM/SETTINGS/HARDWARE konfigurieren (Abbildung 2.3). Sehr praktisch ist auch das kleine Netzwerkkartensymbol unten rechts in der Statusleiste einer laufenden VM, worüber sich mit einem Doppelklick die Einstellungen jederzeit aufrufen lassen. Alle Einstellungen der Adapter können Sie auch im laufenden Betrieb ändern. Damit lässt sich ein Gast z.B. an ein anderes Netzwerk anschließen oder offline schalten. Für diesen erweiterten Workshop ist nur die Einstellung *Custom* relevant. Mit dem Modus *Custom* und der Auswahl eines VMnet stecken Sie das Patchkabel sozusagen an einen bestimmten virtuellen Switch und schließen den Gast damit an dieses Netzwerk an. Mit dem Haken an *Connected* können Sie das virtuelle Patchkabel jederzeit abziehen oder anstecken und so die Verbindung herstellen oder unterbrechen.



Denken Sie daran: Nur VMs mit virtuellen Netzwerkkarten am gleichen Switch (VMnet) können miteinander kommunizieren. Und auch nur dann, wenn diese Gäste IP-Adressen aus dem gleichen Netzwerkbereich haben.

Abbildung 2.3:  
Ein Custom-Adapter kann an zehn virtuelle Switches angeschlossen werden



## Die Adaptermodelle *vlan*ce, *vmxnet* und *e1000* in den Gästen

Standardmäßig emuliert VMware einen Netzwerkadapter vom Typ AMD PCNet. Ein Treiber für diesen Adapter ist in fast jedem Gastbetriebssystem schon von Haus aus vorhanden. In den aktuellen VMware-Versionen wird in den Gästen automatisch ein optimierter Treiber *VMware Accelerated AMD PCNet Adapter* eingerichtet, sobald die VMware Tools installiert sind (Abbildung 2.5). Dieser Treiber sorgt für eine bessere Performance bei vorhandener Gigabit-Anbindung.

Beim Standardtreiber ohne VMware Tools wird, unabhängig von der wirklichen Geschwindigkeit, immer nur eine 10-Mbit/s-Verbindung angezeigt. Trotzdem verwendet der Treiber auch eine 100-Mbit/s- oder eine Gigabit-Verbindung. Beim optimierten Treiber zeigt das Gastsystem 1Gbit/s an. Die angezeigten Geschwindigkeiten sind immer rein kosmetisch und haben nichts mit der physischen LAN-Verbindung zu tun.



Sollten Sie virtuellen Maschinen vom GSX-Server verwenden (so genannten *Legacy*-Maschinen), können Sie in der Konfiguration der Netzwerkkarte einen Adaptertyp auswählen. Es stehen *vlan*ce oder *vmxnet* zur Auswahl, wobei *vlan*ce der Standardtyp ist (Abbildung 2.4). Bei VMs, die unter den aktuellen Versionen erstellt werden, ist diese Auswahl nicht mehr vorhanden, es wird immer *vlan*ce verwendet. Sinn des Modells *vmxnet* war ursprünglich ein optimierter Treiber, speziell für dieses Modell, das von den VMware Tools installiert wird. Dadurch verbessert sich die Performance bei einer Gigabit-Anbindung. Der Nachteil ist allerdings, dass ein Gastsystem nur mit installierten VMware Tools den virtuellen Adapter erkennen kann, ohne Tools funktioniert ein *vmxnet*-Adapter nicht, weil der Treiber fehlt. Dieses Manko ist mit den neuen VMware-Versionen behoben. Es wird nur noch der Standardtyp *vlan*ce benötigt. Dieser funktioniert sowohl mit den mitgelieferten Treibern der Gastbetriebssysteme als auch mit dem optimierten Treiber aus den VMware Tools. Ein Umschalten der Typen ist nicht mehr notwendig.

**Das Modell *vmxnet* und *vlan*ce**

Zusätzlich emuliert VMware speziell für 64-Bit-Gäste einen Intel PRO/1000 Adapter, für den viele Gastbetriebssysteme eigene 64-Bit-Treiber mitbringen. Zum Experimentieren kann dieser Adaptertyp auch in 32-Bit-VMs mittels Editieren der Konfigurationsdatei eingestellt werden.

**Das Modell *e1000***

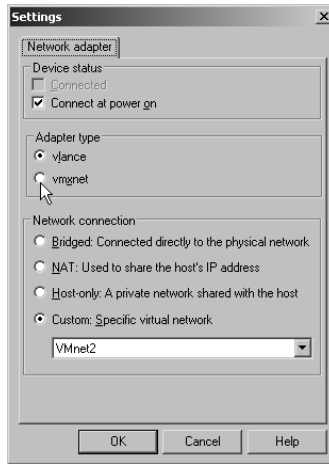
In der Konfigurationsdatei *\*.vmx* einer VM können Sie die eingestellten Adaptertypen in folgender Zeile zu jeder virtuellen Netzwerkkarte sehen und auch manuell anpassen. Fehlt der Eintrag, dann emuliert VMware standardmäßig immer den Typ *vlan*ce.

**Einträge in der Konfigurationsdatei**

```
ethernet0.virtualDev = "vmxnet"
```



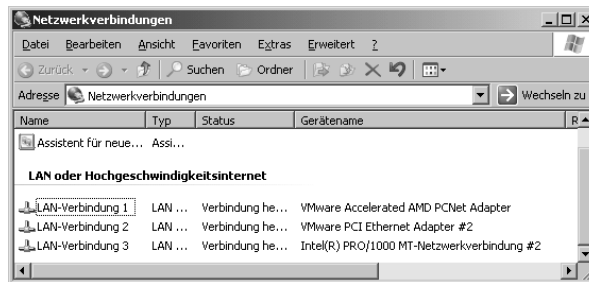
Abbildung 2.4:  
Bei Legacy-VMs  
kann der Adaptertyp  
noch manuell einge-  
stellt werden, das ist  
in den aktuellen  
Versionen nicht  
mehr nötig



Folgende Adaptermodelle erscheinen bei den entsprechenden Einträgen in der Konfigurationsdatei im Gastsystem (Abbildung 2.5):

- ▶ *vlan* – Ethernet-Adapter der AMD-PCNet-Familie  
Einen Treiber für dieses Modell bringt fast jedes Betriebssystem mit. Bei installierten VMware Tools wird ein optimierter Treiber verwendet.
- ▶ *vmxnet* – VMware PCI Ethernet-Adapter  
Der Treiber ist nur in den VMware Tools enthalten. Das Modell wird in aktuellen VMware-Versionen nicht mehr benötigt.
- ▶ *e1000* – Intel(R) PRO/1000 MT Adapter  
Dieses Modell wird für 64-Bit-Gäste emuliert, funktioniert aber auch unter 32-Bit-Gästen.

Abbildung 2.5:  
In einem Gast kann  
VMware drei ver-  
schiedene Adapter-  
modelle emulieren.  
Der AMD PCNet  
Adapter ist Standard



### Virtuelle VMware-Adapter auf dem Host

Zusätzlich existieren unter VMware, außer auf dem ESX Server, noch zwei virtuelle Netzwerkkarten auf dem Host selbst, VMware hat sie bei der Installation automatisch eingerichtet. Sie sind in der Netzwerkumgebung des Hosts als Einträge sichtbar (Abbildung 2.6). Auch diese Adapter sind jeweils mit einem internen VMnet-Switch verbunden (Abbildung 2.7).

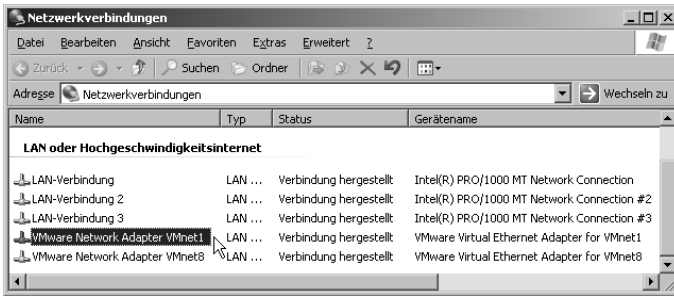


Abbildung 2.6:  
Auf dem Host installiert VMware zwei spezielle virtuelle Netzwerkkarten, über die Gäste mit dem Host kommunizieren können

- ▶ *VMware Network Adapter VMnet1 (Host-only)* – Dieser Adapter ist zuständig für eine Kommunikation des Hosts mit allen VMs, die an VMnet1 angeschlossen sind. Auch ohne physische Netzwerkkarte kann der Host somit auf die Gäste zugreifen.
- ▶ *VMware Network Adapter VMnet8 (NAT)* – Über diesen Adapter erfolgt ebenfalls eine Kommunikation der VMs mit dem Host, genau wie im VMnet1. Die besondere Funktion von VMnet8 ist aber der Dienst *VMware NAT Service*, der einen Router mit NAT-Funktion darstellt. Die VMs können darüber unter der Identität des Host-Computers ins LAN oder ins Internet zugreifen, ohne selbst sichtbar zu werden und ohne IP-Adressen aus dem LAN oder aus dem Internet zu benötigen.

Der NAT-Dienst und der virtuelle Host-Adapter *VMware Network Adapter VMnet8* sind völlig unabhängig. NAT funktioniert auch ohne den Host-Adapter und könnte genauso allein in jedem anderen VMnet laufen, z.B. im VMnet7, für das gar kein Host-Adapter existiert. Die Kommunikation der VMs mit dem Host und die Kommunikation dieser VMs über den NAT-Router ins LAN läuft parallel und unabhängig voneinander ab (Abbildung 2.7).

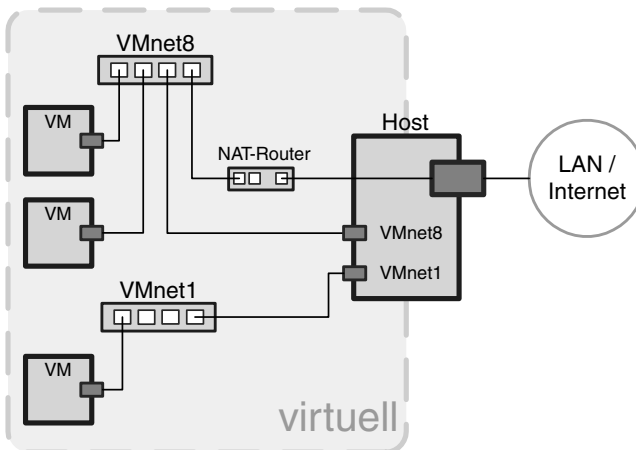
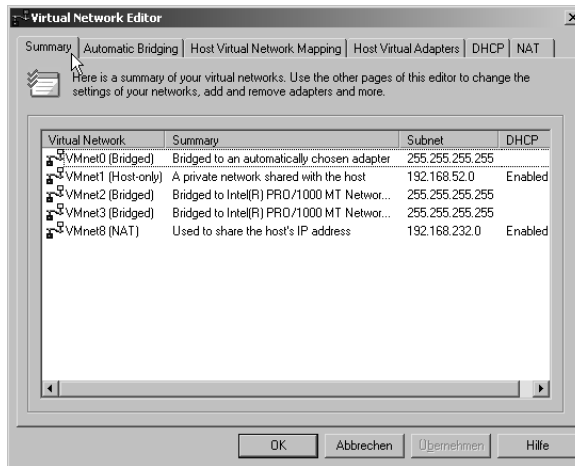


Abbildung 2.7:  
VMnet1 und VMnet8 ermöglichen die Kommunikation mit dem Host ohne physischen Adapter. Im VMnet8 läuft zusätzlich NAT

## Hostadapter konfigurieren

Im Menü VIRTUAL NETWORK SETTINGS/HOST VIRTUAL ADAPTERS können Sie jederzeit weitere Adapter anlegen oder die vorhandenen entfernen. Beim Neuanlegen müssen Sie auswählen, an welchem internen VMnet-Switch der Host-Adapter angeschlossen sein soll. In den meisten Fällen genügen bereits die beiden vorkonfigurierten Adapter, und eine weitere Erstellung ist nicht notwendig. Ein weiterer Host-only-Adapter kann höchstens nützlich sein, um komplexere virtuelle Netze mit Routing über den Host zu erstellen. Einen Überblick über alle Host-Adapter (auch die physischen) und die eingestellten Netzwerkbereiche erhalten Sie im Menü VIRTUAL NETWORK SETTINGS/SUMMARY (Abbildung 2.8). Wie Sie den automatisch voreingestellten Adressbereich der internen Netzwerke und der virtuellen Host-Adapter ändern können, erfahren Sie weiter unten bei „Konfiguration der virtuellen Switches mit Adressbereichen sowie Zuordnung von NAT und DHCP“.

Abbildung 2.8:  
In den Virtual Network Settings des Hosts erhalten Sie unter anderem einen Überblick über die Verwendung der Adapter



Wenn Sie eine der beiden vorhandenen virtuellen Host-Netzwerk-karten VMnet1 oder VMnet8 (Abbildung 2.6) auf dem Host entfernen oder deaktivieren, funktioniert bei der Verwendung der vordefinierten Einstellungen NAT oder *Host-only* für einen virtuellen Adapter keine Kommunikation mehr mit dem Host.

## 2.2.3 Die virtuellen Switches VMnet0 – VMnet9 unter VMware

### Das Herz des Netzwerks

Ein virtueller Switch vereint alle angeschlossenen virtuellen Adapter der Gäste zu einem Netzwerk. Die Konfiguration dieser internen Netze von VMware erfolgt über das Menü VIRTUAL NETWORK SETTINGS/HOST VIRTUAL NETWORK MAPPING im so genannten *Virtual*

*Network Editor.* Die Switches sind der Dreh- und Angelpunkt der gesamten Netzwerkkonfiguration. VMware verfügt über zehn interne Switches (VMnet0–VMnet9). Drei davon sind schon automatisch für bestimmte Aufgaben vorbereitet (Abbildung 2.9).

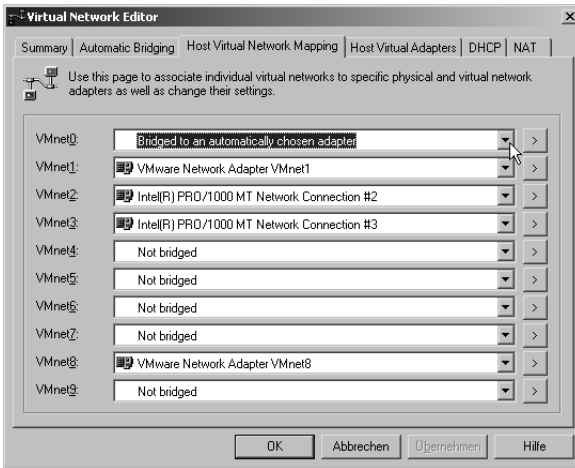


Abbildung 2.9:  
Die virtuellen Switches sind der Dreh- und Angelpunkt der Netzwerkkonfiguration unter VMware

### Funktion der reservierten Switches VMnet0, 1 und 8

Die folgenden reservierten Switches sind standardmäßig vorkonfiguriert. Sie haben die Funktionen bereits in *Teil 3, Kapitel 1*, verwendet, ohne genau die Hintergründe zu kennen.

- ▶ *VMnet0, Bridged* – Dieser Switch ermöglicht die Kommunikation mit der realen Welt über eine physische Netzwerkkarte. Der verwendete physische Adapter wird von VMware standardmäßig selbst gewählt, zu sehen an der Einstellung *Bridged to an automatically chosen adapter*.
- ▶ *VMnet1, Host-only* – Dieser Switch ermöglicht die Kommunikation mit dem Host auch ohne physische Netzwerkkarte über den Host-Adapter *VMware Network Adapter VMnet1*.
- ▶ *VMnet8, NAT* – Dieses virtuelle Netzwerk ermöglicht ebenfalls eine Kommunikation mit dem Wirt über einen virtuellen Host-Adapter und zusätzlich die Kommunikation der Gäste über NAT nach draußen ins LAN oder Internet unter der Identität des Hosts.

Auch jeder andere freie Switch könnte die Aufgaben der drei vorkonfigurierten Netzwerke übernehmen. Alle zehn virtuellen Netzwerke lassen sich flexibel verwalten.



## Zuweisen von physischen Netzwerkkarten an die freien Switches oder Verwendung als abgeschottetes Netzwerk

### Abgeschottete Netze oder bridged ins LAN

Die verbleibenden sieben freien VMnet-Switches stehen als Standard auf der Einstellung *Not bridged*. Alle an einem solchen Switch angeschlossenen VMs können dadurch nur intern untereinander kommunizieren. Damit lassen sich abgeschottete Netze aufbauen, z.B. für Testzwecke oder für eine DMZ. Wenn Sie die Liste zu einem VMnet aufklappen, erscheinen alle noch verfügbaren physischen Netzwerkkarten des Host-PC. Sind mehrere Netzwerkkarten im Host eingebaut, kann somit jedem Switch eine davon zugeordnet werden (VMnet2 und 3 in Abbildung 2.9). Wurde eine Netzwerkkarte schon einem VMnet zugewiesen, steht sie nicht mehr in der Liste zur Auswahl.

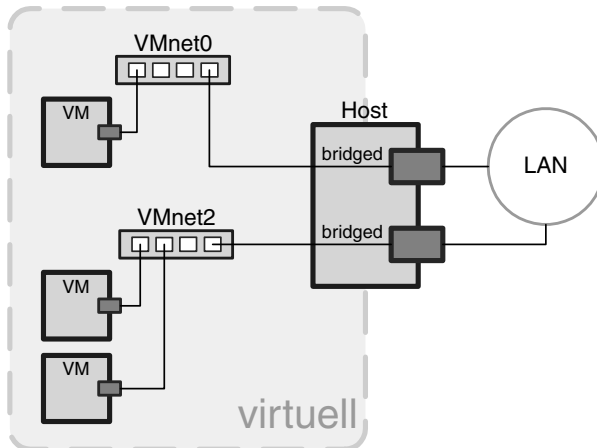


Wenn alle vorhandenen physischen Adapter anderen Switches als VMnet0 zugewiesen wurden, dann steht VMnet0 zwar immer noch auf dem Status *Bridged to an automatically chosen adapter*. Trotzdem ist VMnet0 mit keiner physischen Netzwerkkarte mehr verbunden, weil alle Adapter bereits von anderen VMnets verwendet werden.

### Mehrere physische Netzwerkkarten

Bei mehreren Netzwerkkarten im Host sollten Sie keine automatische Zuweisung verwenden, weil dann VMware für VMnet0 den ersten physischen Adapter immer automatisch wählt. Sie werden aber in Zukunft selbst bestimmen, was passiert. Sobald Sie für VMnet0 einen Adapter explizit auswählen, wird die automatische Konfiguration abgeschaltet. Sichtbar ist das unter VIRTUAL NETWORK SETTINGS/AUTOMATIC BRIDGING.

Abbildung 2.10:  
Alle Switches  
können mit physischen  
Adaptoren verbunden werden.  
Dadurch lassen sich  
VMs auf diese  
Adapter verteilen



Sobald eine physische Netzwerkkarte einem VMnet zugeordnet wurde, sind alle am Switch angeschlossenen VMs über diesen Adapter im LAN sichtbar. Damit können VMs auf bestimmte Netzwerkkarten verteilt werden, etwa um einer Maschine aus Performance-

gründen einen physischen Adapter explizit zuzuweisen oder um Testnetz und Produktion zu trennen (Abbildung 2.10). Genauso können auf diese Weise bestimmte VMs unterschiedlichen LAN-Segmenten zugewiesen werden. In *Teil 2, Kapitel 3, „Virtuelle DMZ mit Firewall und Webserver im Internet“*, werden auf diese Weise einem virtuellen DMZ-Router bestimmte physische Adapter zum Internet und zum LAN zugewiesen.

Zusätzlich lassen sich für jedes freie VMnet auch weitere virtuelle Host-Adapter hinzufügen anstelle einer physischen Netzwerkkarte – VMnet1 und VMnet8 sind bereits mit solchen Adaptern verbunden. Siehe dazu oben unter „Virtuelle Netzwerkkarten auf dem Host“.

## Virtuelle Host-Adapter

### Konfiguration der virtuellen Switches mit Adressbereichen sowie Zuordnung von NAT und DHCP

Rechts neben jedem Switch ist im Virtual Network Editor ein kleines Symbol sichtbar, über das Sie ein Subnet (IP-Netzwerkbereich) sowie die DHCP-Einstellungen für dieses virtuelle Netzwerk definieren können (Abbildung 2.11). Das funktioniert standardmäßig nur mit VMnet1 und VMnet8, weil dort bereits interne DHCP-Dienste laufen. Wie Sie auch den anderen VMnets einen DHCP-Server zuweisen können, erfahren Sie weiter unten bei „Der DHCP-Dienst in den virtuellen Netzwerken“, hier geht es nur um den Sinn der Subnet-Einstellung.

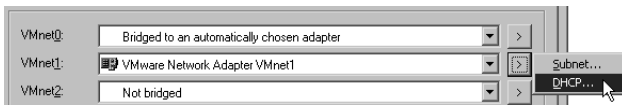


Abbildung 2.11:  
Für jedes VMnet lassen sich Einstellungen für den Adressbereich und für den DHCP-Dienst treffen

Für jeden Switch können Sie einen eigenen Subnet-Bereich festlegen (Abbildung 2.12). Dieser wird von VMware automatisch als Einstellung für den DHCP-Bereich verwendet, wenn der DHCP-Dienst in diesem Netzwerk läuft. Existiert auch ein virtueller Host-Adapter (z.B. *VMware Network Adapter VMnet1*), wird dieser von VMware immer mit der ersten Adresse aus dem von Ihnen zugewiesenen Subnet konfiguriert. Der virtuelle Host-Adapter bekommt also eine feste IP-Adresse aus diesem Bereich, z.B. 192.168.52.1, und der VMware-DHCP-Dienst verteilt dazu passende Adressen an alle angeschlossenen Gäste, z.B. 192.168.52.100-150. Damit erfolgt die gesamte interne IP-Konfiguration in diesem virtuellen Netzwerk automatisch.

## Subnet

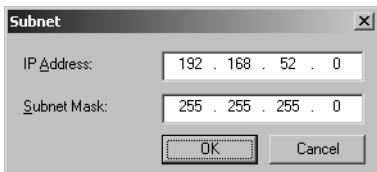


Abbildung 2.12:  
Das Subnet legt den IP-Adressbereich für das jeweilige VMnet fest. Für Bridged-Netze ohne DHCP hat das keine Auswirkungen

### **Kurze Zusammenfassung zu den virtuellen Switches am Beispiel von VMnet0, dem Bridged-Netzwerk**

Den nicht ganz trivialen Zusammenhang der VMnet-Switches und der virtuellen Adapter möchte ich an einem Beispiel zusammenfassen. Ich erwähnte bereits, ein virtueller Adapter im Modus *Custom* an VMnet0 ist das Gleiche wie ein virtueller Adapter im Modus *Bridged*. Bridged bedeutet, dass Pakete aus Gästen, die an diesem virtuellen Netzwerk angeschlossen sind, das physische LAN erreichen und umgekehrt. Aber warum genau ist VMnet0 das standardmäßige Bridged-Netz von VMware, was zeichnet dieses Netzwerk gegenüber den anderen Switches aus?

Die Sonderstellung von VMnet0 hat nur einen Grund – VMware verbindet immer automatisch eine physische Netzwerkkarte des Host-PC mit diesem virtuellen Netzwerk. Dadurch befinden sich nicht nur virtuelle Adapter an diesem Switch, sondern auch eine physische Netzwerkkarte (Abbildung 2.10). Damit klärt sich gleich ein weit verbreitetes Missverständnis auf: Es ist nicht ganz richtig, dass ein virtueller Adapter mit der Einstellung BRIDGED direkt mit einer physischen Netzwerkkarte verbunden ist. Ein Bridged-Adapter ist eigentlich nur am internen Switch VMnet0 angeschlossen – mehr nicht! Und nur weil diesem Netzwerk zusätzlich eine physische Netzwerkkarte zugewiesen wurde, können VMs am VMnet0 mit der realen Welt Daten austauschen.

Über welche physische Netzwerkkarte die Gäste an VMnet0 kommunizieren, bestimmen Sie ausschließlich am Switch VMnet0 und nicht an den virtuellen Adaptern der Gäste. Ähnlich verhält es sich mit den Switches VMnet1 und VMnet8 und ihrer Bindung an die virtuellen Host-Adapter, nur dass es sich dabei nicht um physische Netzwerkkarten handelt.



Erst die Konfiguration eines virtuellen Switches bestimmt die Möglichkeiten des Datenaustauschs der daran angeschlossenen Gäste. Einem virtuellen Adapter im Gast weisen Sie nur einen Switch zu, welche Art der Kommunikation dieser Switch ermöglicht, ob mit dem LAN oder nur intern, kann der Gast nicht beeinflussen.

#### **2.2.4 VMware Bridge Protocol – die Brücke in die reale Welt**

Über ein entscheidendes Bindeglied zwischen realer und virtueller Welt haben wir uns bisher noch gar keine Gedanken gemacht. Wie funktioniert die Kommunikation der virtuellen Switches mit den physischen Netzwerkkarten? Was verbindet die Hardware mit der Emulation, und wie gelangen die Pakete zwischen den Welten hin und her?

Das Bindeglied ist das so genannte *VMware Bridge Protocol*. Dieses Protokoll wird von VMware auf dem Host installiert und an eine physische Netzwerkkarte gebunden. Sie können es in der Netzwerkumgebung auf dem Host in den Eigenschaften Ihrer physischen Adapter sehen (Abbildung 2.13). Jede Karte, an die dieses Protokoll gebunden wurde, ist mit einem bestimmten VMnet verbunden. In den EIGENSCHAFTEN zum Bridge Protocol ist die Nummer des VMnet zu sehen, mit dem die physische Netzwerkkarte verknüpft ist.

**Verbindung zur realen Welt**

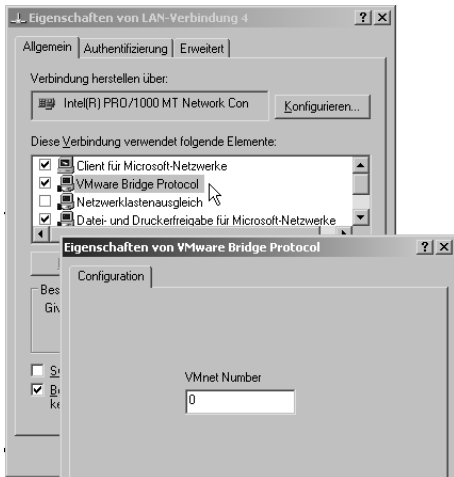


Abbildung 2.13:  
Das VMware Bridge Protocol verbindet ein VMnet mit einer physischen Netzwerkkarte

Über dieses Protokoll zapft VMware den Datenverkehr der physischen Netzwerkkarte an und leitet Pakete, die an virtuelle Adapter gerichtet sind, nach innen weiter. Umgekehrt tunnelt es die Pakete aus den VMs auf die Hardware und damit ins LAN. Das Protokoll lässt sich zwar manuell an die physischen Netzwerkkarten binden und mit der Nummer des VMnets konfigurieren, im Normalfall macht das aber VMware automatisch, sobald Sie Änderungen im Netzwerkmenü vornehmen. Die virtuellen Host-Netzwerkkarten (VMNet1 und VMNet8) benötigen dieses Protokoll übrigens nicht, da sie direkt mit den internen Switches verbunden sind.

## 2.2.5 Dienste DHCP und NAT in den virtuellen Netzen von VMware

Die von VMware bereitgestellten Dienste DHCP und NAT sind virtuelle Geräte, die ebenfalls an einem VMnet angeschlossen sind. Auf dem Host müssen dazu folgende Dienste laufen:

- ▶ VMware NAT Service
- ▶ VMware DHCP Service





Diese Dienste können auch von einem Gast mit entsprechender Software bereitgestellt werden. Wenn Sie z.B. eine interne Active Directory-Domäne nachbilden wollen, sollten Sie den DNS- und DHCP-Server des virtuellen Windows-Domänencontrollers verwenden, weil ansonsten die Kommunikation in der Domäne nicht richtig funktioniert.

## Der DHCP-Dienst im virtuellen Netzwerk

Sie können für jedes virtuelle Netz einen eigenen DHCP-Bereich definieren. Damit sparen Sie sich auch in internen *not-bridged*-Testnetzen die manuelle IP-Konfiguration aller Gäste. Sie können natürlich auch alle IP-Adressen manuell fest in den Gästen einstellen, was z.B. bei Servern sinnvoll ist.

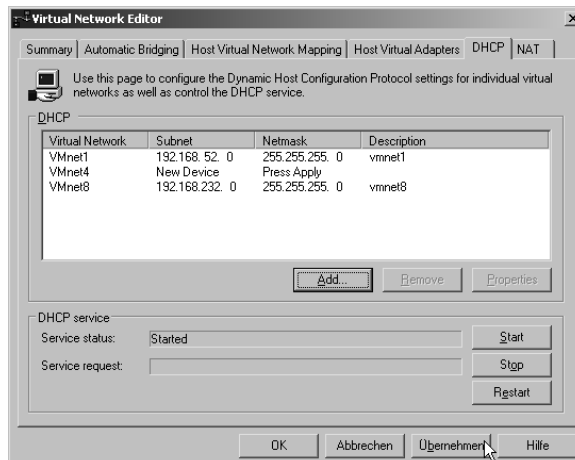


Wenn ein DHCP-Dienst in einem Bridged-Netz läuft, dann verteilt er Adressen auch ins physische LAN. Das kann den produktiven Betrieb stören, da Clients IP-Adressen aus einem falschen Netzwerkbereich bekommen.

So schalten Sie den DHCP-Dienst für ein VMnet ein:

1. Rufen Sie mittels VIRTUAL NETWORK SETTINGS/DHCP die DHCP-Einstellungen auf. Sie sehen hier alle bereits vorhandenen Bereiche und könnten diese entfernen oder ändern (Abbildung 2.14).
2. Mittels ADD gelangen Sie zum Dialog für einen neuen Bereich. Hier wählen Sie vorerst nur das gewünschte VMnet aus und bestätigen dann mit OK.
3. In der DHCP-Bereichsliste taucht jetzt Ihr neuer Eintrag auf. Unter Subnet steht dort *Press Apply*. Bestätigen Sie also Ihren neuen Bereich unbedingt noch mit dem Button ÜBERNEHMEN (Abbildung 2.14).

Abbildung 2.14:  
Nach dem Hinzufügen eines DHCP-Bereiches muss dieser vor der weiteren Konfiguration erst übernommen werden



4. Erst jetzt können Sie mit dem Button PROPERTIES in die Einstellungen wechseln und die Start- und Endadresse des automatisch zu verteilenden IP-Bereiches festlegen (Abbildung 2.15). VMware legt selbst ein Subnet fest, wenn von Ihnen in den Einstellungen zum VMnet-Switch nicht explizit ein Wert hinterlegt wurde. Das Subnet kann später jederzeit wieder direkt in den Einstellungen zum Switch geändert werden (Abbildung 2.11).
5. Mit der Lease-Time legen Sie fest, wie lange eine Station eine erhaltene IP-Adresse reserviert bekommt, bevor die Adresse verfällt und an eine andere anfragende Station vergeben werden kann. Sie können die voreingestellten Werte mit OK übernehmen.

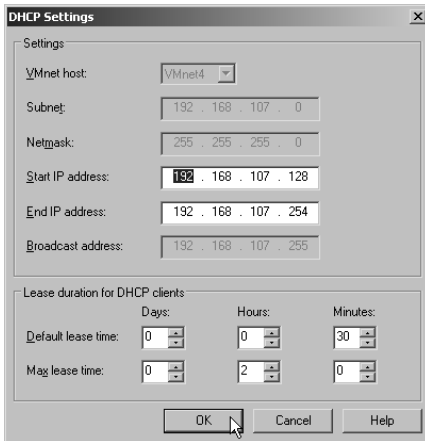


Abbildung 2.15:  
In den DHCP-Einstellungen legen Sie nur den Adressbereich fest, der im definierten Subnet verteilt wird

Es existieren zwei Dateien, in denen die Konfiguration und vor allem die ausgeteilten Adressen sichtbar sind, zu finden unter Windows in C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware.

#### Konfigurationsdateien

- *vmnetdhcp.conf* – Enthält die Konfiguration der einzelnen Bereiche.
- *vmnetdhcp.leases* – Enthält die Datenbank der ausgeteilten Adressen. Hier können Sie sich mit einem Texteditor schnell einen Überblick über die verteilten IP-Adressen und zugehörigen Rechnernamen der Gäste aller VMnets holen.

Sollten beim Versuch, eine Änderung an den Netzwerkeinstellungen im DHCP-Bereich abzuspeichern, permanent Fehlermeldungen erscheinen, dann hilft es oft, die oben genannten Dateien zu löschen und VMware neu zu starten. Sie müssen dann allerdings Ihre DHCP-Konfiguration neu anlegen.

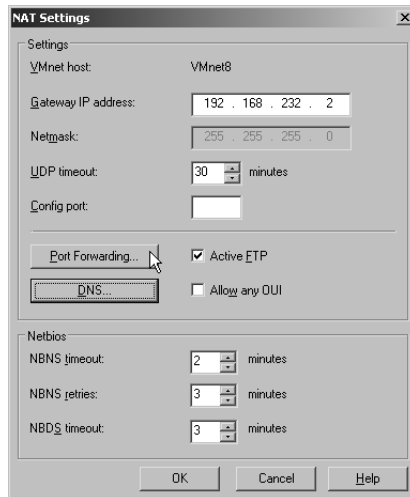


## Der NAT-Dienst im virtuellen Netzwerk

Der NAT-Dienst läuft standardmäßig bereits im VMnet8. Im Normalfall müssen Sie bei der NAT-Konfiguration keine Hand anlegen. Wenn der Host einen funktionierenden Internet- oder LAN-Zugang hat, wird dieser vom NAT-Dienst im VMnet8 automatisch verwendet. Dabei spielt es keine Rolle, ob der Zugang über das LAN, Modem oder UMTS erfolgt. Der NAT-Dienst ist immer nur für ein einziges virtuelles Netz verfügbar.

1. Rufen Sie mit VIRTUAL NETWORK SETTINGS/NAT den Konfigurationsdialog des NAT-Dienstes auf.
2. Zuerst müssen Sie das VMnet festlegen, in dem der Dienst laufen soll, Standard ist VMnet8. Wenn Sie das ändern, dann müssen Sie, bevor Sie weitermachen, den Button ÜBERNEHMEN einmal anklicken.
3. Mittels EDIT gelangen Sie in die Einstellungen des NAT-Dienstes (Abbildung 2.16).

Abbildung 2.16:  
In den NAT-Einstellungen kann Port-forwarding eingerichtet werden, und die Gateway-Adresse ist sichtbar



Die folgenden wichtigen Einstellungen stehen zur Verfügung:

### Gateway und DNS

- Die IP-Adresse des virtuellen NAT-Routers können Sie in den Einstellungen unter *Gateway IP Address* ablesen. Anpassen sollten Sie diese Adresse nur in Ausnahmefällen. Sie müssen diese Adresse aber kennen, wenn Sie Gästen, die NAT verwenden sollen, manuell feste IP-Adressen zuweisen, ohne DHCP zu verwenden. Warum?

Im Netzwerk, das NAT anbietet, sollte eigentlich ein DHCP-Dienst laufen. Dadurch werden die Gateway-Adresse und die Adresse des DNS-Servers in den Gästen automatisch auf den virtuellen NAT-Router gesetzt. Im vorkonfigurierten VMet8 ist das bereits der Fall. Dadurch können alle Gäste sofort über den NAT-Router ins Internet, und auch die DNS-Auflösung funktioniert.

Wollen Sie lieber feste IP-Adressen in den Gästen vergeben, dann müssen Sie jeder VM, die NAT verwenden will, als Gateway- und DNS-Adresse die IP-Adresse des NAT-Dienstes mitteilen, da dieser den Router spielt. Diese Adresse finden Sie hier.

- Der Button DNS – Ein Gast fragt grundsätzlich immer den NAT-Dienst nach einer DNS-Auflösung. Der NAT-Dienst fragt dann bei seinen DNS-Servern an, er spielt also einen DNS-Proxy. Normalerweise verwendet VMware den DNS-Server der funktionierenden Host-Verbindung, um für den NAT-Router Namen aufzulösen. Wenn Sie andere DNS-Server angeben wollen, müssen Sie den Haken an *Auto detect* entfernen und Ihre Server in die Liste eintragen (Abbildung 2.17).

#### DNS-Proxy

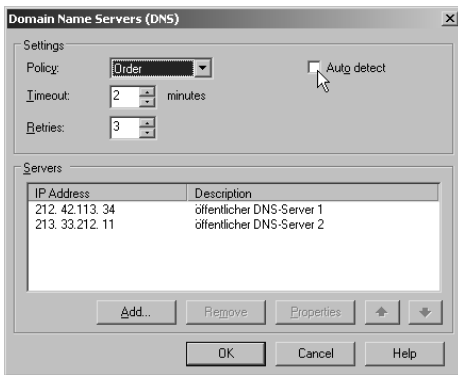


Abbildung 2.17:  
Der NAT-Dienst verwendet automatisch die DNS-Server vom Host, sie können aber auch manuell festgelegt werden

- Der Button PORTFORWARDING

Sie können an dieser Stelle die Weiterleitung bestimmter Ports an Gäste innerhalb des virtuellen Netzes definieren. Dem Portforwarding habe ich gleich im Anschluss einen eigenen Abschnitt gewidmet.

Die Datei *vmnetnat.conf* im Verzeichnis *C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware* enthält die Konfiguration des NAT-Dienstes, muss aber unter Windows nicht manuell editiert werden.

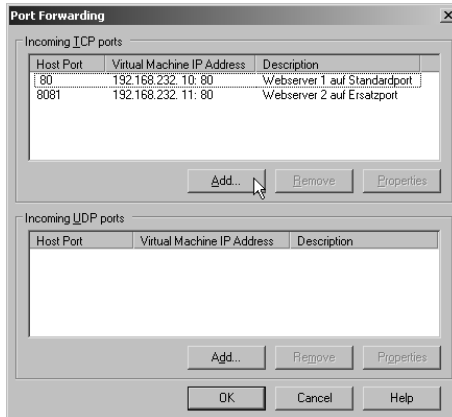
#### Konfigurationsdatei

### Portforwarding mit dem NAT-Dienst von VMware

Ein Sonderfall der NAT-Konfiguration ist das so genannte Portforwarding. Wozu brauchen Sie diese Funktion? Normalerweise schließen Sie Gäste, die das LAN erreichen sollen, einfach an ein VMnet an, das mit einer physischen Netzwerkkarte verbunden ist (*bridged*). Damit hat der Gast uneingeschränkten Zugriff auf das LAN und ist genauso erreichbar. In einigen Fällen ist es aber nicht möglich, Gäste auf diese Weise direkt ins LAN zu bringen, etwa wenn keine freien IP-Adressen aus dem LAN bekannt sind oder wenn die VM versteckt bleiben soll. Wird in diesem Falle als Ausweg ein NAT-Adapter verwendet, dann ist die VM von außen nicht mehr erreichbar. Für diesen Fall können

Sie unter VIRTUAL NETWORK SETTINGS/NAT/EDIT/PORTFORWARDING genau definieren, welche Ports doch nach innen zur VM weitergeleitet werden, z.B. Port 80 für einen Webserver (Abbildung 2.18). Der Client im LAN spricht direkt die IP-Adresse des Host-Rechners an, als würde dort der Webserver laufen. Auf Port 80 lauscht aber VMwares NAT-Dienst und leitet die Pakete nach drinnen zur festgelegten IP-Adresse des virtuellen Websters weiter. Über alle anderen Ports wird weiterhin ganz normal der Host angesprochen.

Abbildung 2.18:  
Mittels Portforwarding können trotz NAT Anfragen auf bestimmten Ports an ausgewählte VMs weitergeleitet werden



Der größte Nachteil am Portforwarding ist, dass ein Port nur genau einem Gast oder dem Host zugewiesen werden kann. Wenn mehrere virtuelle Webserver laufen, muss der NAT-Router auf verschiedenen Ports lauschen. Es kann also nur einer über den Standardport 80 angesprochen werden. Genauso können nicht der Host und eine VM gleichzeitig auf demselben RDP-Port auf eine Remotedesktop-Verbindung zur Fernsteuerung warten oder beispielsweise den gleichen VNC-Port verwenden.

## 2.2.6 Simulierte schlechte Leitungsqualität virtueller Netzwerke von VMware Workstation mit Teams

Als Hinweis erwähne ich hier noch die Möglichkeit, unter VMware Workstation eigene Netzwerke für ein Team aus virtuellen Maschinen zu erstellen (siehe Teamfunktion in Teil 2, Kapitel 1, „Eine Testumgebung mit VMware Workstation oder Server aufbauen“). In solch einem virtuellen Netzwerk können Sie schlechte Leitungsqualitäten durch verlorene Pakete oder langsame Verbindungen durch Begrenzung der Bandbreite simulieren. Dadurch lässt sich beispielsweise das Verhalten einer Replikation über eine WAN-Verbindung testen oder der Seitenaufbau einer neu entwickelten Webpräsenz über einen langsamen Internet-Zugang per ISDN oder Modem ausprobieren.

## 2.2.7 Konfiguration der virtuellen Netzwerke auf einem Linux-Host mit VMware

Unter einem Linux-Host fehlt leider die komfortable menügestützte Konfigurationszentrale. Hier ist manuelle Arbeit notwendig, um die Standard-Netzwerkfunktionen anzupassen oder zu erweitern. In den meisten Fällen kommen Sie aber glücklicherweise ohne Eingriffe aus. Häufigster Grund für eine notwendige Konfigurationsänderung ist die nachträgliche Zuweisung eines physischen Netzwerkadapters an ein bestimmtes VMnet.

### Ein VMnet unter Linux konfigurieren

Die Netzwerkconfiguration erledigt das Skript *vmware-config.pl*. Es ist das gleiche Skript, das für die Installation von VMware auf dem Host zuständig ist. Für folgenden Fälle müssen Sie dieses Skript verwenden:

**vmware-config.pl**

- ▶ Sie wollen mehrere physische Netzwerkkarten bestimmten virtuellen VMnets zuweisen. Dies wird der häufigste Anwendungsfall sein. Voraussetzung ist, Sie haben wirklich mehrere physische Netzwerkkarten in Ihrem Host!
- ▶ Um Host-only- bzw. NAT-Adapter zu entfernen oder einzurichten. Dies ist vor allem notwendig, wenn Sie nicht gleich bei der Installation VMware alle Adapter haben einrichten lassen und Sie später doch ein Host-only-Netz verwenden wollen.
- ▶ Sie benötigen zusätzliche virtuelle Host-Netzwerkadapters (wie VMnet1 und VMnet8). Das wird eigentlich nur in wenigen Test-szenarien vorkommen.

Die Konfiguration kann folgendermaßen aufgerufen werden:

```
/usr/bin/vmware-config.pl
```

Nun startet die normale VMware-Installation. Zuerst müssen wieder die üblichen Standardfragen mit den Vorgaben beantwortet werden, und einige Module werden eventuell neu übersetzt. Irgendwann erscheint folgende Frage, ab hier beginnt die Netzwerkconfiguration:

```
Would you like to skip networking setup and keep your
old settings as they are?
(yes/no) [yes] n
```

Sie müssen mit *Nein* antworten, um in die Netzwerkconfiguration zu gelangen, sonst bleiben alle Einstellungen unverändert.

### Beispiel zur Linux-Konfiguration – einem VMnet eine physische Netzwerkkarte zuweisen

Als Beispiel zur weiteren Vorgehensweise dient folgender Dialog. Er bringt Sie zur Konfiguration eines zusätzlichen Bridged-Netzwerks im VMnet2. Voraussetzung ist eine zweite funktionierende physische

Netzwerkkarte. Im Beispiel ist diese noch nicht vorhanden, und das Skript erkennt das:

```
Do you want networking for your virtual machines?
(yes/no/help) [yes] y
```

```
Would you prefer to modify your existing networking
configuration using the wizard or the editor?
(wizard/editor/help) [editor] e
```

```
The following virtual networks have been defined:
```

```
. vmnet0 is bridged to eth0
. vmnet3 is a host-only network on private subnet
192.168.7.0.
```

```
. vmnet8 is a NAT network on private subnet
192.168.244.0.
```

```
Do you wish to make any changes to the current
virtual networks settings?
(yes/no) [no] y
```

```
Which virtual network do you wish to configure?
(0-99) 2
```

```
What type of virtual network do you wish to set
vmnet2?
```

```
(bridged,hostonly,nat,none) [none] b
```

```
Configuring a bridged network for vmnet2.
```

```
All your ethernet interfaces are already bridged.
```

```
Are you sure you want to configure a bridged ethernet
interface for vmnet2?
```

```
(yes/no) [no] n
```

Hier müssen Sie mit *No* Abbrechen, da keine zweite Netzwerkkarte im Host gefunden wurde. Sie könnten alternativ ein Host-only-Netz einrichten, aber Sie wollen ja eine zweite Netzwerkkarte einbauen. Wenn Sie das getan haben und die Netzwerkkarte unter Linux ordentlich läuft, wiederholen Sie den Vorgang bis zu dieser Stelle. Jetzt kann die neue Netzwerkkarte zugewiesen werden:

```
Your computer has the following ethernet devices: eth0
eth1. Which one do you want to bridge to vmnet2? [eth1]
```

```
The following virtual networks have been defined:
```

```
. vmnet0 is bridged to eth0
. vmnet2 is bridged to eth1
. vmnet3 is a host-only network on private subnet
192.168.7.0.
```

```
. vmnet8 is a NAT network on private subnet
192.168.244.0.
```

```
Do you wish to make additional changes to the current
virtual networks settings?
(yes/no) [yes] n
```

Sie haben damit *VMnet2* den physischen Adapter *eth1* zugewiesen. Weitere Änderungen wünschen Sie nicht. Im Anschluss erfolgt noch automatisch die restliche Konfiguration von VMware, unter anderem wird beim VMware Server erneut der Port für die Remote-Konsole abgefragt. Alle Fragen können Sie mit den voreingestellten Werten beantworten. Ab jetzt ist die Vorgehensweise wieder die gleiche wie auf einem Windows-Host. Im gewohnten Einstellungsdialog in der grafischen VMware Console können Sie einem bestimmten virtuellen Adapter einer VM den Switch *VMnet2* zuweisen. Jede VM an diesem Netz ist damit über den physischen Adapter *eth1* mit dem LAN verbunden.

### DHCP und NAT auf einem Linux-Host konfigurieren

Zur individuellen Konfiguration von DHCP und NAT müssen Sie unter Linux einen Texteditor bemühen. Keine Angst, das Skript *vmware-config.pl* legt für die Standardnetze bereits eine funktionierende Konfiguration an. Nur wenn Sie besondere Einstellungen benötigen, etwa Portforwarding, müssen Sie Dateien editieren. Meist ist kein Eingriff nötig. Sie finden alle Dateien in folgenden Verzeichnissen. Ersetzen Sie im Beispiel das X mit der Nummer des VMnet, das Sie bearbeiten wollen.

```
/etc/vmware/vmnetX/nat
```

```
/etc/vmware/vmnetX/dhcpd
```

Um z.B. Portforwarding auf eine VM mit einem Webserver einzuschalten, müssen Sie in der Datei */etc/vmware/vmnet8/nat/nat.conf* folgende Sektion bearbeiten:

#### Portforwarding

```
[incomingtcp]
80 = 192.168.5.xxx:80
443 = 192.168.5.xxx:443
```

Dieses Beispiel leitet alle Pakete, die auf dem Host am Port 80 oder 443 eingeht, nach drinnen auf eine VM mit der IP-Adresse 192.168.5.xxx ebenfalls auf den Ports 80 und 443 weiter.

UDP-Verbindungen haben eine eigene Sektion:

```
[incomingudp]
```

### Custom-Netzwerke vmnet2-9 sind nicht sichtbar

Das so genannte *udev*-Dateisystem legt das Verzeichnis */dev* mit den enthaltenen Gerätedateien bei jedem Neustart dynamisch an, damit dort nicht mehr eine ellenlange Liste von Einträgen erscheint, sondern nur noch wirklich verwendete Geräte. Leider werden die Custom-Netzwerke von VMware dort nicht registriert, es erscheint nur *vmnet0* und gegebenenfalls *vmnet1* und *vmnet8*. Damit funktionieren zwar nach jeder Ausführung von *vmware-config.pl* die Custom-Netz-



werke, aber nur bis zum nächsten Systemstart. Sie können die internen Netzwerke aber manuell registrieren:

- *Debian/Ubuntu* – /etc/udev/links.conf:

```
VMware devices
M vmmon c 10 165
M vmnet2 c 119 2
...
M vmnet9 c 119 9
```

- *Suse* – /etc/udev/static\_devices.txt:

```
VMware devices
vmmon c 10 165 660
vmnet2 c 119 2 600
...
vmnet9 c 119 9 600
```

## 2.3 Die Netzwerkkonfiguration unter MS Virtual Server 2005 R2

### Was ist mit Virtual PC?

Wir konzentrieren uns bei den Microsoft-Produkten auf den großen Bruder Virtual Server, der einiges mehr an Netzwerkoptionen mitbringt als Virtual PC. Unter Virtual PC 2004 gestaltet sich die Netzwerkkonfiguration sehr unkompliziert. Zum einen existiert nur ein einziges internes Netz mit dem Namen *lokal*, zum anderen können weder der DHCP- noch der NAT-Dienst konfiguriert werden. Eigentlich wurde in *Teil 3, Kapitel 1*, schon alles gesagt. Einzig und allein die Erklärungen zur Verwendung des *Microsoft Loopbackadapters* ist für Virtual PC in diesem Kapitel zusätzlich interessant (siehe *Abschnitt 2.3.5, „Virtuelle Adapter auf dem Host – der Microsoft Loopbackadapter“*).

### 2.3.1 Virtuelle Netzwerkkarten unter Virtual Server

Microsoft Virtual Server 2005 emuliert in den VMs einen virtuellen Adapter vom Typ DEC 21140, der von den Gästen häufig als ein baugleicher Intel Ethernet Adapter erkannt wird. Die meisten aktuellen Betriebssysteme bringen für diesen Adapter eigene Treiber mit.

Jeder VM können Sie bis zu vier virtuelle Netzwerkkarten zuweisen. Die Einstellungen einer VM finden Sie in der Verwaltungswebseite z.B. über VIRTUELLE COMPUTER/KONFIGURIEREN oder im Masterstatus im Menü zu jeder VM unter KONFIGURATION BEARBEITEN. Die Netzwerkkarten lassen sich dann in der Konfiguration unter dem Eintrag NETZWERKADAPTER konfigurieren (Abbildung 2.19). Standardmäßig wird bei der Erstellung einer jeden VM bereits die erste virtuelle Netzwerkkarte automatisch eingerichtet. Mit dem Button NETZWERKADAPTER HINZUFÜGEN können Sie jederzeit weitere Adap-

ter hinzufügen, etwa wenn Ihre VM ein Router sein soll. Mit dem Haken an ENTFERNEN und anschließend OK wird ein Adapter wieder von der VM entfernt. Lassen Sie den Eintrag für die MAC-Adresse vorerst immer auf DYNAMISCH, in fast allen Fällen ist das richtig. Zum Thema MAC-Adressen gibt es weiter unten in diesem Kapitel einen eigenen Abschnitt.

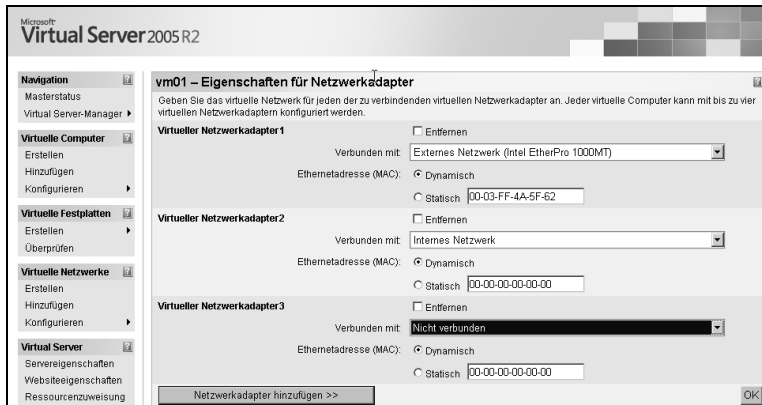
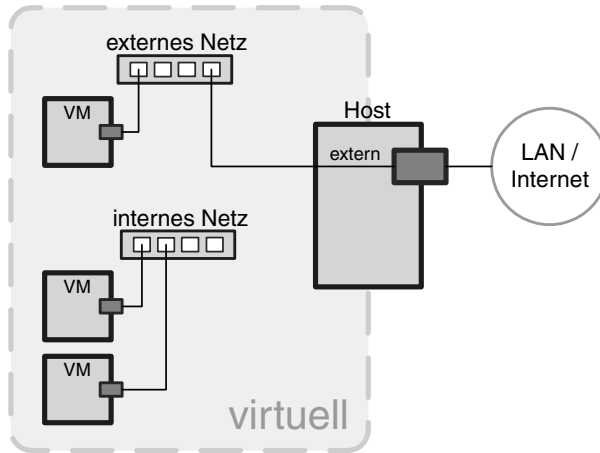


Abbildung 2.19:  
Virtual Server unter-  
stützt pro VM bis zu  
vier Netzwerkkadap-  
ter mit unterschiedli-  
chen Anschlussarten

Mit der Auswahlliste VERBUNDEN MIT entscheiden Sie, ob die virtuelle Netzwerkkarte mit dem physischen LAN kommunizieren kann oder ob der Verkehr im internen virtuellen Netzwerk bleibt (Abbildung 2.20). Folgende Optionen stehen zur Verfügung:

- ▶ *Nicht verbunden* – Mit dieser Auswahl ziehen Sie sozusagen das virtuelle Patchkabel ab, die virtuelle Netzwerkkarte ist nicht angeschlossen und kann nicht kommunizieren.
- ▶ *Internes Netzwerk* – Mit dieser Option verbinden Sie den Adapter mit einem internen Switch. Die VM kann nur mit anderen Maschinen an dem gleichen Switch kommunizieren, kein Paket gelangt nach draußen. Standardmäßig existiert unter Virtual Server vorerst nur ein einziges internes Netz, Sie können aber jederzeit weitere Konfigurieren (siehe Abschnitt 2.3.1, „*Virtuelle Netzwerkkarten unter Virtual Server*“).
- ▶ *Externes Netzwerk* – Alle virtuellen Netzwerkkarten, die mit einem externen Netzwerk verbunden sind, können ebenfalls untereinander in diesem Netz kommunizieren. Zusätzlich gelangt der gesamte Verkehr aller angeschlossenen VMs über den zugewiesenen physischen Adapter nach draußen ins LAN. Alle VMs sind uneingeschränkt zu erreichen, haben eine eigene MAC-Adresse, benötigen eindeutige IPs und treten zusammen mit dem Host als unabhängige PCs im realen Netzwerk auf. Der Host und mehrere VMs können sich dabei ein und dieselbe physische Netzwerkkarte teilen.

Abbildung 2.20:  
Interne Netzwerke  
bleiben abgeschot-  
tet, externe Netz-  
werke haben über  
einen physischen  
Adapter Verbindung  
zum LAN



Das Umstecken der virtuellen Patchkabel durch Auswahl einer anderen Einstellung funktioniert auch im laufenden Betrieb eines Gastes. So kann ein Gast sofort vom LAN in ein internes Testnetz wechseln, indem Sie in der Konfiguration des Adapters einfach ein anderes Netzwerk aus der Liste VERBUNDEN MIT wählen. Nur VMs mit Adapters am gleichen Netzwerk sehen sich direkt, genauso wie in einem physischen LAN alle Rechner am selben Switch angeschlossen sein müssen. Routing zwischen den getrennten Netzen ist nur mittels einer VM mit mehreren Netzwerkkarten möglich. Bei einem Wechsel von einem externen Netzwerk ins interne Netzwerk oder umgekehrt müssen gegebenenfalls auch die IP-Adressen des Gastes angepasst werden.

### 2.3.2 Virtuelle Netzwerke unter Microsoft Virtual Server

#### Die Zentrale des Netzwerks

Was unter VMware die virtuellen VMnet-Switches sind, das sind bei Microsoft die *virtuellen Netzwerke*, denen Sie Ihre Adapter der VMs zuweisen können. Die Konfiguration dieser Netzwerke erfolgt im Menü VIRTUELLE NETZWERKE (Abbildung 2.21). Hier können Sie neue Netzwerke hinzufügen und vorhandene Netzwerke anpassen.

Abbildung 2.21:  
Interne und externe  
Netzwerke lassen sich  
im Menü Virtuelle  
Netzwerke erstellen  
und konfigurieren



Nach einer Neuinstallation von Virtual Server existieren bereits einige virtuelle Netze, zu sehen unter VIRTUELLE NETZWERKE/KONFIGURIEREN/ALLE ANZEIGEN (Abbildung 2.22). Für jede physische Netzwerkkarte im Host hat das Setup automatisch ein *externes Netzwerk* konfiguriert und nach dem Namen der Netzwerkverbindung benannt.

Zusätzlich existiert ein einziges *internes Netzwerk*. Diese vorhandenen Netzwerke sind die, die Sie den jeweiligen virtuellen Adaptern eines Gastes im Konfigurationsdialog der VM sofort zuweisen können (Abbildung 2.19). Das im Bild sichtbare Netzwerk mit dem Namen *Loopback01* wurde bereits zusätzlich angelegt, wir kommen später noch darauf zurück.

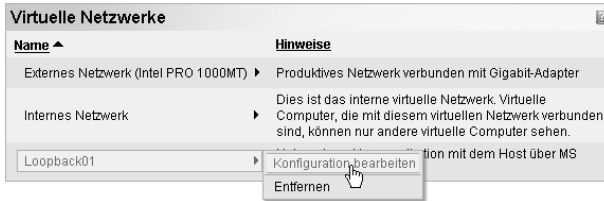


Abbildung 2.22:  
Weitere virtuelle Netzwerke können hinzugefügt oder entfernt werden. *Loopback01* wurde nachträglich konfiguriert

## Einstellungen der virtuellen Netzwerke ändern

Mittels **VIRTUELLE NETZWERKE/KONFIGURIEREN/NAME DES NETZWERKS/NETZWERKEINSTELLUNGEN** können Sie zu jedem Netzwerk dessen Einstellungen ändern. Sie können festlegen, ob und mit welchem physischen Adapter das virtuelle Netzwerk verbunden ist, und auch einen Namen für dieses Netzwerk bestimmen (Abbildung 2.23).

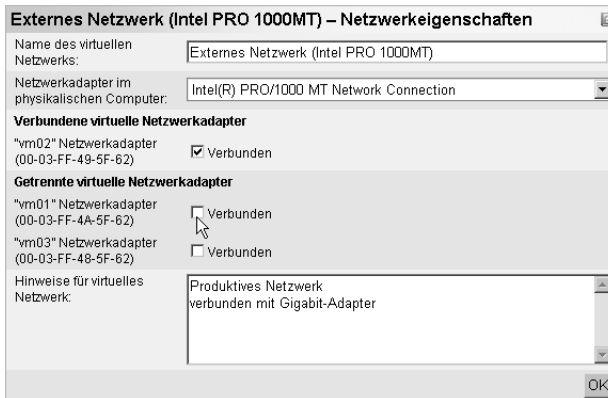


Abbildung 2.23:  
An jedes virtuelle Netzwerk können bestimmte VMs angeschlossen werden

Folgende Optionen stehen für jedes Netzwerk unter Microsoft Virtual Server zur Verfügung:

- ▶ *Name des virtuellen Netzwerks* – Ein frei wählbarer Name des Netzes.
- ▶ *Netzwerkadapter im physischen Computer* – Ein physischer Adapter oder ein Loopback-Adapter auf dem Host, der dem Netz zugewiesen werden soll. Alle VMs an diesem Netz können über den ausgewählten Adapter mit dem LAN kommunizieren. Wählen Sie anstelle einer Netzwerkkarte *Keine (nur Gäste)*, dann hat das Netzwerk sofort keinen Kontakt mehr zur Außenwelt und kann als abgeschottetes Testnetzwerk oder auch als DMZ verwendet werden.

- ▶ *Verbundene/Getrennte virtuelle Netzwerkadapter* – Diese beiden Übersichten listen alle VMs auf, welche Adapter an diesem Netzwerk angeschlossen haben und welche nicht. Hier können Sie das virtuelle Netzwerk sofort den virtuellen Netzwerkkarten verschiedener Gäste zuweisen, ohne erst in die Konfiguration jeder einzelnen VM wechseln zu müssen.



Die Zuweisung von Adaptern unterschiedlicher VMs an dieser Stelle ist sehr praktisch, um schnell mehrere Gäste ans gleiche Testnetzwerk anzuschließen oder diese wieder zu trennen.

- ▶ *Hinweise für virtuelles Netzwerk* – Hier können Sie eine frei wählbare Beschreibung des virtuellen Netzwerks eintragen.



Die Namen der automatisch eingerichteten externen Netzwerke enthalten die Bezeichnung der physischen Netzwerkkarte, die bei der Installation von Virtual Server automatisch zugewiesen wurde. Bei einer veränderten Zuweisung einer physischen Netzwerkkarte zu einem solchen virtuellen Netzwerk wird der Name des Netzwerks nicht automatisch angepasst. Wählen Sie z.B. *Keine (nur Gäste)* anstelle der bisherigen Netzwerkkarte, dann heißt das Netzwerk trotzdem noch *Externes Netzwerk Intel Pro 1000*. Das kann später zu einiger Verwirrung führen, weil Sie dadurch im Konfigurationsdialog einer VM ungewollt falsche Netzwerke auswählen, wenn die Bezeichnungen nicht mehr mit den zugewiesenen physischen Adaptern übereinstimmen. Ändern Sie am besten den Namen der Netzwerke in logische Bezeichnungen, wie *produktion*, *lan01* o.Ä.

### Neue virtuelle Netzwerke anlegen, entfernen oder von einer Konfigurationsdatei aufnehmen

Mittels VIRTUELLE NETZWERKE/ERSTELLEN können Sie weitere Netzwerke anlegen. Nach dem Anlegen können Sie diese neuen Netze wie gewohnt konfigurieren und physische Netzwerkkarten zuweisen oder ohne physische Adapter als interne Testbereiche verwenden. Weitere Netzwerke werden aus folgenden Gründen benötigt:

- ▶ Sie haben zusätzliche physische Netzwerkkarten eingebaut, die Sie bestimmten VMs zuweisen wollen. Zu jeder Netzwerkkarte sollten Sie immer ein eigenes Netzwerk anlegen.
- ▶ Sie haben einen Loopback-Adapter für die Hostkommunikation installiert (siehe Abschnitt 2.3.5, „*Virtuelle Adapter auf dem Host – der Microsoft Loopbackadapter*“), den Sie bestimmten VMs zuweisen wollen.

- Sie benötigen weitere interne Netzwerke, um eine komplexere Testumgebung mit mehreren VMs und Routing aufzubauen, ohne direkten Kontakt zur Außenwelt.

Über NETZWERKE/KONFIGURIEREN/ALLE ANZEIGEN/NAME DES NETZWERKS/ENTFERNEN kann ein virtuelles Netzwerk wieder entfernt werden. Für jedes Netzwerk existiert eine Konfigurationsdatei im Verzeichnis *C:\Dokumente und Einstellungen\All Users\Dokumente\Shared Virtual Networks* auf dem Host. Diese Dateien haben die Endung *\*.vnc*. Mittels VIRTUELLE NETZWERKE/HINZUFÜGEN können Sie die Konfigurationsdatei eines Netzwerks aufnehmen, ohne das Netzwerk neu konfigurieren zu müssen. So lassen sich z.B. komplexere Testnetzwerke samt den Gästen einfach auf einen anderen Host transportieren.

**Konfigurationsdatei eines Netzwerks**

### 2.3.3 Virtual Machine Network Services – die Verbindung zur Außenwelt

Das Bindeglied zwischen den physischen Adaptern und den virtuellen Netzwerken ist bei Microsoft das Protokoll *Virtual Machine Network Services*. Wie Sie bereits wissen, werden virtuelle Adapter der Gäste den virtuellen Netzwerken zugewiesen, wodurch alle VMs am gleichen Netzwerk miteinander kommunizieren können. Zusätzlich lässt sich einem virtuellen Netzwerk ein physischer Adapter zuweisen, das Netzwerk wird damit zum externen Netzwerk. Das Protokoll *Virtual Machine Network Services* ist dabei die Schnittstelle zum physischen Adapter. Dieses Protokoll wird von Virtual Server/Virtual PC auf dem Host installiert und an eine physische Netzwerkkarte gebunden. Sie können es in der Netzwerkumgebung in den Eigenschaften Ihrer physischen Adapter sehen (Abbildung 2.28). Nur diejenigen physischen Adapter, an die dieses Protokoll gebunden wurde, stehen in der Konfiguration unter *Netzwerkadapter im physikalischen Computer* zur Auswahl (Abbildung 2.23). Über dieses Protokoll zapft Virtual Server den Datenverkehr der physischen Netzwerkkarten an und stellt die Pakete den Gästen zur Verfügung. Umgekehrt übermittelt es die Pakete aus den VMs über den physischen Adapter ins LAN.

**Verbindung zur realen Welt**

Sollte einmal eine physische Netzwerkkarte oder ein Loopback-Adapter nicht in der Liste bei der Netzwerkkonfiguration von Virtual Server/PC zur Auswahl stehen, so muss das Protokoll *Virtual Machine Network Services* auf dem Host erst noch manuell an diesen Adapter gebunden werden. Das ist häufig der Fall bei nachträglich eingebauten Netzwerkkarten oder auch beim Microsoft Loopback-adapter.



### 2.3.4 Die Dienste DHCP und NAT in den virtuellen Netzwerken

#### NAT

Ein virtueller NAT-Router (Netzwerkadressübersetzung zur LAN-Anbindung unter der Identität des Hosts) existiert unter Virtual Server nicht. Mittels der Internet-Verbindungsfreigabe unter Windows (*Internet Connection Sharing*, kurz *ICS*) und einem Loopback-Adapter kann NAT aber über den Host selbst erfolgen. Siehe dazu *Abschnitt 2.6.2, „NAT mittels Internet-Verbindungsfreigabe direkt auf dem Host einrichten“*, weiter unten.

#### DHCP

Der von Virtual Server bereitgestellte DHCP-Server ist eine Art virtuelles Gerät, das ebenfalls an einem virtuellen Netzwerk angeschlossen ist. Diesen Dienst kann auch ein Gast bereitstellen, z.B. ein virtueller Domänencontroller. Über VIRTUELLE NETZWERKE/KONFIGURIEREN gelangen Sie zu den Einstellungen der einzelnen Netzwerke und können dort mit DHCP SERVER den Dienst einschalten und konfigurieren. Eigentlich genügt der Haken an AKTIVIERT, Virtual Server schlägt bereits Adressbereiche vor, die Sie für eine Testumgebung übernehmen können (Abbildung 2.24). Wollen Sie mit den VMs aus den internen Netzwerken auch ins Internet oder ins LAN, dann können Sie die STANDARD-GATEWAYADRESSE und den DNS-SERVER eintragen. Dazu benötigen Sie in Ihrem abgeschotteten Testnetz allerdings auch eine VM, die als Router ins physische LAN dient. Die Adresse des internen Netzwerkadapters dieser VM ist dann in den DHCP-Einstellungen des internen Netzwerks zu hinterlegen.

Abbildung 2.24:  
Für jedes Netzwerk  
kann ein DHCP-  
Dienst konfiguriert  
werden

| Internes Netzwerk – Eigenschaften von DHCP-Server |                                               |
|---------------------------------------------------|-----------------------------------------------|
| <b>Virtueller DHCP-Server</b>                     | <input checked="" type="checkbox"/> Aktiviert |
| Netzwerkadresse:                                  | 10.237.0.0                                    |
| Netzwerkmaske:                                    | 255.255.0.0                                   |
| IP-Startadresse:                                  | 10.237.0.16                                   |
| IP-Endadresse:                                    | 10.237.255.254                                |
| Adresse des virtuellen DHCP-Servers:              | 10.237.0.1                                    |
| Standardgatewayadresse:                           |                                               |
| DNS-Server:                                       |                                               |
| Einträge durch Komma trennen                      |                                               |
| WINS-Server:                                      |                                               |
| Einträge durch Komma trennen                      |                                               |
| IP-Adressen-Leasezeitraum:                        | 36 Stunden                                    |
| Lease-Erneuerungszeitraum:                        | 18 Stunden                                    |
| Lease-Neueinbindungszeitraum:                     | 27 Stunden                                    |
| OK                                                |                                               |

Wenn Sie die Internet-Verbindungsfreigabe (ICS) als NAT-Ersatz verwenden, dann dürfen Sie keinen internen DHCP-Server einschalten, da ICS bereits selbst interne IP-Adressen verteilt.



Wenn Sie bei einem externen Netzwerk den DHCP-Server von Virtual Server einschalten, verteilt dieser seine Adressen auch ans physische LAN und kann den Betrieb damit stören, weil LAN-Clients die falschen Adressen abholen.



### 2.3.5 Virtuelle Adapter auf dem Host – der Microsoft Loopbackadapter

Microsoft liefert zum Virtual PC/Server keinen Host-Adapter mit, der die direkte Kommunikation zwischen dem Wirt und den Gästen ohne physische Netzwerkkarte ermöglicht. Eine solche Verbindung kann z.B. nützlich sein, um ohne physischen Netzwerkklink vom Host aus mit Gästen kommunizieren zu können, z.B. in einer DMZ. Als Alternative ist bereits im Lieferumfang von Windows der so genannte *Microsoft Loopbackadapter* vorhanden, der als virtueller Netzwerkkartentreiber auf dem Host installiert werden kann. Der Treiber wirkt für das Host-Betriebssystem wie eine echte Netzwerkkarte. Zwar hat dieser Adapter keinerlei Buchse, über die Pakete nach draußen gelangen, dafür kann der neu installierte Adapter unter Virtual Server oder auch unter Virtual PC als Netzwerkkarte verwendet werden, über die dann eine Kommunikation mit dem Host möglich wird (Abbildung 2.25). Das funktioniert auch, wenn keinerlei LAN angeschlossen ist, z.B. bei einer Kunden-Demo.

**Verbindung ohne physischen Adapter**

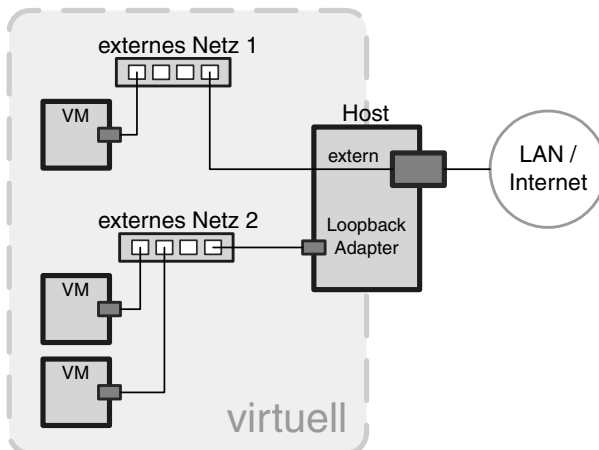


Abbildung 2.25:  
Ein Microsoft Loopbackadapter ermöglicht die Kommunikation vom Host zu den Gästen ohne physischen Link

Um mittels der Internet-Verbindungsfreigabe auf dem Host VMs über NAT ans LAN oder ans Internet anzubinden (siehe *Abschnitt*

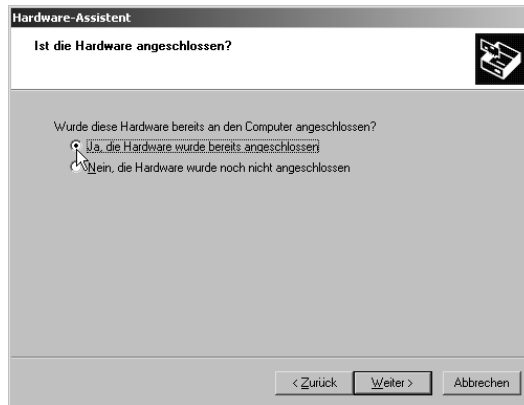


2.6.2, „NAT mittels Internet-Verbindungsfreigabe direkt auf dem Host einrichten“), ist ebenfalls eine Kommunikation der Gäste mit dem Host über einen Microsoft Loopbackadapter notwendig.

Mit folgenden Schritten lässt sich der Microsoft Loopbackadapter unter Windows Server 2003 installieren:

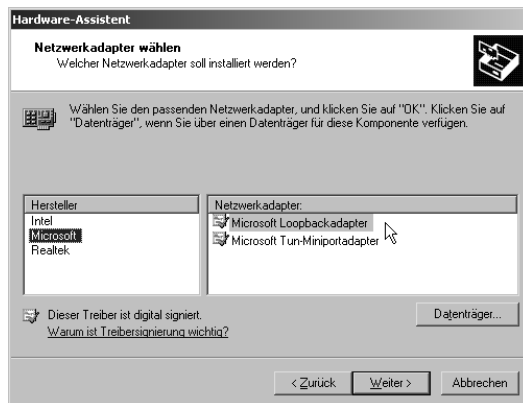
1. Wählen Sie unter SYSTEMSTEUERUNG den Punkt HARDWARE, und bestätigen Sie den Willkommensbildschirm mit WEITER. Es wird kurz nach neuer Hardware gesucht, danach behaupten Sie einfach JA, DIE HARDWARE WURDE BEREITS ANGESCHLOSSEN (Abbildung 2.26).

Abbildung 2.26:  
Um die Installation  
zu beginnen,  
behaupten Sie, die  
Hardware wäre  
angeschlossen



2. In der Liste mit vorhandener Hardware finden Sie ganz unten den Eintrag NEUE HARDWARE HINZUFÜGEN, den Sie bestätigen.
3. Setzen Sie den Punkt an HARDWARE MANUELL AUS EINER LISTE WÄHLEN, und suchen Sie in der folgenden Liste den Eintrag NETZWERKADAPTER.
4. Unter MICROSOFT finden Sie den Treiber für den *Microsoft Loopbackadapter* (Abbildung 2.27).

Abbildung 2.27:  
Der Treiber wird als  
Netzwerkadapter  
installiert



5. Bei SYSTEMSTEUERUNG/NETZWERKVERBINDUNGEN finden Sie jetzt den neuen Adapter als zusätzliche Netzwerkkarte auf dem Host.

- Binden Sie gleich das Protokoll *Virtual Machine Network Services* an den neuen Adapter, indem Sie einfach den Haken setzen (Abbildung 2.28). Erst dadurch taucht der Loopback-Adapter später in der Netzwerkkonfiguration von Virtual Server als verfügbare Netzwerkkarte auf.

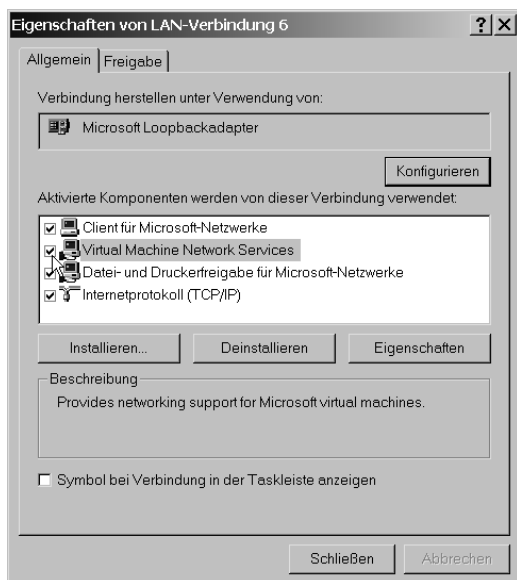


Abbildung 2.28:  
Der Microsoft Loopbackadapter kann wie jede normale Netzwerkkarte auf dem Host konfiguriert werden

- Damit Host und Gäste sich sehen, müssen Sie dem eben installierten Loopback-Adapter noch eine IP-Adresse geben, die in einem Netzwerkbereich liegt, der noch nirgendwo verwendet wird. Hat Ihre physische Netzwerkkarte z.B. die Adresse 192.168.1.22 (sie liegt also im Netzwerk 192.168.1.x), dann würde als Adresse für den Loopback-Adapter die 192.168.0.1 funktionieren (Netzwerk 192.168.0.x).

Unter Virtual PC kann der Loopback-Adapter jetzt einfach als Netzwerkkarte ausgewählt werden. Unter Virtual Server müssen Sie noch ein neues Netzwerk, z.B. mit dem Namen *Loopback01*, konfigurieren, an das der Loopback-Adapter gebunden wird (Abbildung 2.29).

#### Neues internes Netz erstellen

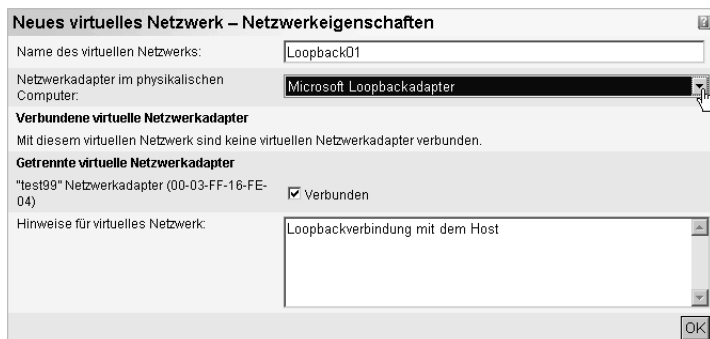
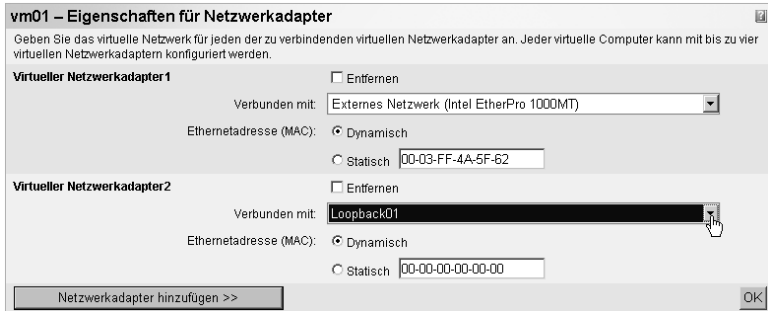


Abbildung 2.29:  
Für den Loopback-Adapter ist ein eigenes Netzwerk anzulegen

Nach dem Anlegen des Netzwerks und dem Zuweisen des Loopback-Adapters erscheint in der Liste **VERBUNDEN MIT** eines beliebigen virtuellen Adapters zusätzlich das neue Netzwerk *Loopback01*, das Sie auswählen können (Abbildung 2.30). Damit sind alle verbundenen Gäste und der Host mit seinem Loopback-Adapter am gleichen virtuellen Netzwerk angeschlossen und können miteinander kommunizieren.

Abbildung 2.30:  
Der Loopback-Adapter wird einem neu erstellten Netzwerk zugewiesen, an das schließlich ein Netzwerkadapter gebunden wird



In der VM müssen Sie natürlich dafür sorgen, dass die virtuelle Netzwerkkarte eine passende IP-Adresse aus dem gleichen Netz des Loopback-Adapters hat, in unserem Beispiel 192.168.0.23. Entweder vergeben Sie diese manuell, oder Sie konfigurieren am praktischsten den DHCP-Dienst des virtuellen Netzes *Loopback01*.

## 2.4 Zusammenfassung zum Netzwerk für alle Produkte auf einen Blick

Zum Abschluss des Exkurses können Sie sich zurücklehnen. Ich fasse noch einmal für alle Produkte einen Überblick zusammen:

- ▶ *Netzwerkkarten* – Virtuelle Netzwerkkarten werden vollständig emuliert und vom Gastsystem in der VM wie echte Hardware verwendet. Das Gastsystem bemerkt keinen Unterschied zu echter Hardware.
- ▶ *Switches* – Die Netzwerkkarten sind an virtuellen Switches angeschlossen (VMnet oder Virtuelles Netzwerk). Nur virtuelle Adapter am gleichen Switch bilden ein Netzwerk und sehen sich.
- ▶ *Interne Kommunikation* – VMs am gleichen Netzwerk (Switch) können intern ungestört mit allen verfügbaren Protokollen kommunizieren. Pakete gelangen über den virtuellen Switch von einer VM zur anderen, aber normalerweise nicht nach draußen auf den Host oder ins LAN.
- ▶ *Brücke in die reale Welt (Bridged, Externes Netzwerk)* – Um ein virtuelles Netz an die reale Welt anzubinden, muss eine physische Netzwerkkarte im Host vorhanden sein. Ein virtueller Switch wird dann über das *VMware Bridge Protocol* oder *Virtual Machine Net-*

*work Services* mit dieser Netzwerkkarte verbunden. Das virtuelle Netzwerk hat damit Verbindung zum LAN. Alle VMs mit angeschlossenen Netzwerkkarten an diesem Netzwerk haben vollen Zugriff auf die reale Welt und sind uneingeschränkt zu erreichen.

- ▶ *Host-only* – Für den Fall, dass keine echte Netzwerkkarte vorhanden ist, existieren auf dem Host ebenfalls virtuelle Adapter; unter VMware z.B. der *VMware Network Adapter VMnet1*, unter Microsoft der *Microsoft Loopbackadapter*. Diese Adapter funktionieren auf dem Host wie echte Netzwerkkarten, sind aber nicht im LAN, sondern an einem virtuellen Switch angeschlossen. Darüber kann der Host mit allen VMs kommunizieren, auch ohne physischen LAN-Anschluss.
- ▶ *DHCP* – In den virtuellen Netzwerken können virtuelle DHCP-Server IP-Adressen verteilen und damit die Konfiguration der Gäste vereinfachen. Für produktive Server sollten aber feste Adressen verwendet werden.
- ▶ *NAT* – Ein Sonderfall ist NAT. Hier existiert ein virtueller Router, der ebenfalls am virtuellen Switch angeschlossen ist, mit dem anderen Anschluss aber direkt über den Host mit dem LAN verbunden ist. Über diesen NAT-Router werden Pakete aus dem virtuellen Netz nach draußen gesendet, wobei die Absenderadresse der VM ersetzt wird. Von außen sind VMs mit NAT nur durch Portforwarding zu erreichen. Genauso macht es beispielsweise auch ein DSL-Router. NAT wird vom Microsoft Virtual Server nur über die Internet-Verbindungsfreigabe (ICS) auf dem Host unterstützt.

## 2.5 Kleines Experiment – die Welten von VMware und Microsoft verbinden

Ein abschließendes Experiment beweist, dass sich die Produkte der verschiedenen Hersteller vom Konzept her nicht grundsätzlich unterscheiden. Gleichzeitig dient das Beispiel nochmals als abschließende Wiederholung. Verbinden wir als Test einmal die gegensätzlichen virtuellen Welten von VMware und Microsoft!

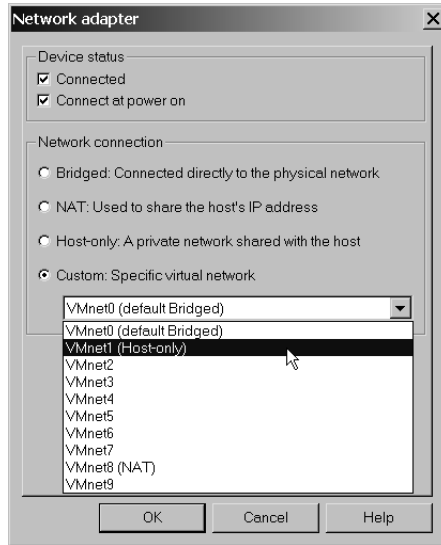
**VMware und  
Virtual Server im  
gleichen Netz**

Sie können problemlos die kostenlosen Versionen von VMware Server und Microsoft Virtual Server auf ein und demselben Host installieren. Das ist sogar sehr nützlich, um beide Produkte direkt miteinander zu vergleichen.



1. Lassen Sie unter VMware eine virtuelle Maschine (Test-VM01) laufen, die am Switch VMnet1 angeschlossen ist (Abbildung 2.31). Sie wissen, dass an diesem Switch ebenfalls der virtuelle Host-Adapter *VMware Network Adapter VMnet1* angeschlossen ist. Über diesen Adapter kann die VM unter VMware direkt mit dem Host kommunizieren.

Abbildung 2.31:  
Der Gast unter  
VMware wird an  
VMnet1 ange-  
schlossen



2. Der Gast VM01 kann seine IP-Konfiguration vom internen DHCP-Dienst von VMware beziehen. Sie sehen die bezogene IP-Adresse im Gast mit dem Befehl `ipconfig`. Schicken Sie ein paar Pings zwischen dem Host und dem Gast VM01 hin und her, um die Funktion zu testen.
3. Erstellen Sie unter MS Virtual Server ein neues Netzwerk, und geben Sie ihm den Namen *MSnet1*. Weisen Sie diesem Netzwerk die virtuelle Host-Netzwerkkarte *VMware Network Adapter VMnet1* zu (Abbildung 2.32). Sie haben diesen Adapter in der Konfiguration unter Microsoft Virtual Server nicht zur Auswahl? Dann müssen Sie zuerst manuell das Protokoll *Virtual Machine Network Services* auf dem Host anbinden. Den Microsoft Loopbackadapter benötigen Sie nicht für diesen Test. Lassen Sie DHCP für das neue Netzwerk *MSnet1* deaktiviert!
4. Lassen Sie nun unter MS Virtual Server einen Gast (Test-VM02) laufen, dessen virtuellen Adapter Sie einfach an das eben erstellte Netzwerk *MSNet1* anschließen. Konfigurieren Sie den virtuellen Adapter im Gastsystem so, dass er seine IP-Adresse über DHCP bezieht, was normalerweise die Standardeinstellung ist.

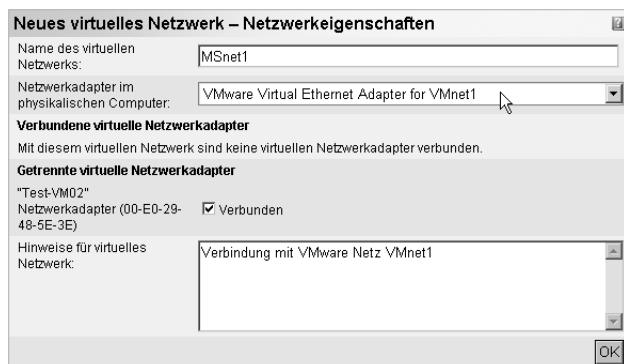


Abbildung 2.32:  
Für den Microsoft-  
Gast wird ein neues  
Netzwerk MSnet1  
erstellt und an den  
VMware Host-  
Adapter VMnet1  
gebunden

5. Schauen Sie sich in einer DOS-Box im Gast Test-VM02 mit dem Befehl `ipconfig` an, was für eine IP-Adresse Test-VM02 bezogen hat – sie müsste aus dem Bereich des Netzwerks VMnet1 von VMware stammen.

Der kuriose Trick funktioniert tatsächlich – die Gäste der Konkurrenz können untereinander und mit dem Host kommunizieren und bilden in trauter Einheit ein gemeinsames virtuelles Netzwerk. VM02 unter Microsoft Virtual Server verwendet den virtuellen Host-Adapter *VMware Network Adapter VMnet1* von VMware. Der Microsoft-Gast VM02 verwendet sogar klaglos den internen VMware-DHCP-Server von VMnet1.

Natürlich ist das in der Praxis nur eine Spielerei, aber es veranschaulicht zum Abschluss sehr schön das Zusammenspiel der Komponenten. Und sollten Sie sich noch nicht für ein Produkt entschieden haben, dann können Sie bei dieser Gelegenheit mit einer parallelen Installation sehr bequem die Produkte direkt miteinander vergleichen. Die grundlegende Funktionalität der virtuellen Netzwerke unter VMware und Microsoft ist soweit erörtert. Im Anschluss finden Sie zusätzliche Hinweise zu verschiedenen Problemstellungen.

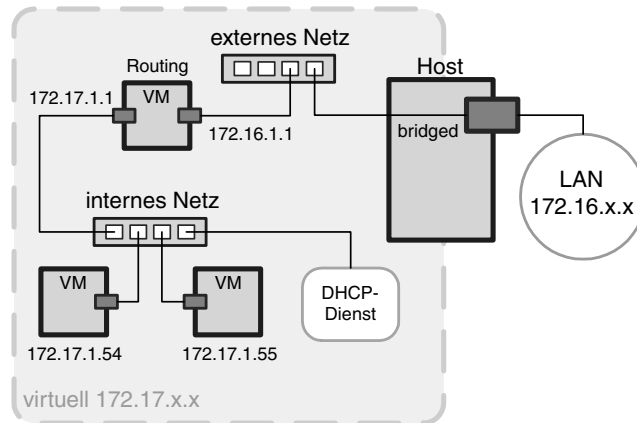
## 2.6 Virtuelle Umgebungen als eigene Netzwerksegmente ans LAN anbinden

Es gibt mehrere Möglichkeiten, die virtuellen Maschinen ans physische LAN anzubinden. Eine Möglichkeit haben Sie als Standardweg bereits kennen gelernt: Die Gäste werden einem virtuellen Netzwerk zugewiesen, das an eine physische Netzwerkkarte gebunden ist (bridged oder externes Netzwerk). Dadurch sind alle angeschlossenen Gäste als unabhängige Mitglieder im LAN verfügbar, sie benötigen IP-Adressen aus dem LAN-Bereich und sind für jeden LAN-Client sichtbar.

### 2.6.1 Routing über eine VM oder über den Host

Eine andere Möglichkeit wäre der Aufbau eines separaten LAN-Segementes für alle virtuellen Maschinen. Dazu werden die Maschinen an ein internes Netzwerk angebunden. Innerhalb dieses Netzwerks können beliebige IP-Adressen manuell festgelegt oder vom internen DHCP-Dienst verteilt werden. Sie haben diese Methode bereits kennen gelernt, um ein abgeschottetes virtuelles Testnetzwerk aufzubauen. Das interne Netzwerksegment muss aber nicht abgeschottet bleiben, es kann auch an das physische LAN angebunden werden. Dazu benötigen Sie einen Router, der die beiden Netzwerke verbindet. Dieser Router kann eine VM mit zwei Adaptionern sein, wobei einer am internen Netzwerk angeschlossen ist, der andere dagegen an einem externen (bridged) Netzwerk (Abbildung 2.33).

Abbildung 2.33:  
Für die Gäste  
können eigene Netz-  
segmente geschaffen  
werden, die mittels  
Routing über eine  
VM ans LAN ange-  
bunden sind



Der Vorteil eines solchen separaten Netzwerksegmentes besteht darin, dass alle VMs unabhängig vom physischen LAN über einen eigenen IP-Adressbereich verfügen. Weiterhin sind die VMs vom LAN aus zwar voll zu erreichen, aber die physischen LAN-Clients müssen die internen IP-Adressen kennen und auch mit den entsprechenden Routing-Einträgen versehen werden. Das ist praktisch, um Test-VMs nicht gleich im gesamten Firmennetzwerk bekannt zu machen. Weiterhin können Sie in der Router-VM Firewalls und NAT verwenden, um die virtuellen LAN-Segmente teilweise abzuschotten oder hinter dem Host zu verstecken. Die virtuellen Maschinen können auch auf mehrere separate LAN-Segmente aufgeteilt werden, z.B. Testumgebung und Produktion. In Teil 2, Kapitel 3, „Virtuelle DMZ mit Firewall und Webserver im Internet“, wird mit einer Router-VM eine virtuelle DMZ auf einem Host samt Firewall und Webservern aufgebaut.

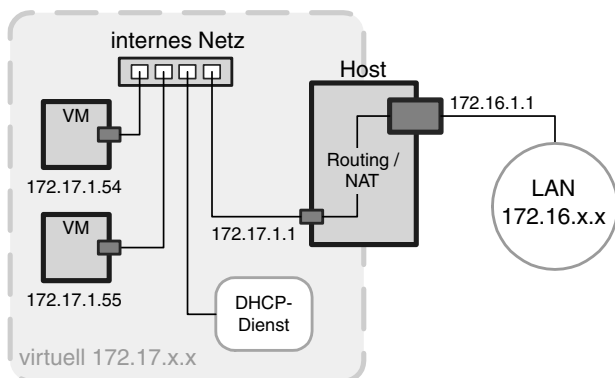


Abbildung 2.34:  
Auch direkt über  
virtuelle Host-  
Adapter (Loopback  
oder VMnet1) kann  
Verkehr aus inter-  
nen Netzen ins LAN  
geroutet werden

Die oben erwähnte Routing-VM können Sie einsparen, wenn Sie die internen Netzwerke gleich über den Host mit dem LAN verbinden (Abbildung 2.34). Unter VMware können Sie für das interne Netzwerk den Switch VMnet1 verwenden. Über den dazugehörigen Host-Adapter *VMware Virtual Ethernet Adapter for VMnet1* kann das gesamte interne Netzwerk über den Host ins physische LAN geroutet werden. Unter Microsoft Virtual Server können Sie dazu einen Microsoft Loopbackadapter verwenden.

Auf dem Wirtssystem muss bei der Anbindung des virtuellen LAN-Segementes über einen Host-Adapter der Routing-Dienst laufen, weil sonst keine Pakete vom virtuellen Netzwerk ins LAN und umgekehrt weitergeleitet werden.



In beiden Varianten ist in allen Gästen als Default-Gateway die Adresse des virtuellen Host-Adapters bzw. des internen Adapters der Router-VM einzutragen, im Beispiel die 172.17.1.1. Weiterhin benötigen die physischen LAN-Clients, die das virtuelle LAN-Segment erreichen sollen, eine Route in das virtuelle Netzwerk über die Router-VM oder über den Host, die manuell an der Kommandozeile der Clients oder im zentralen Default-Gateway des LANs festzulegen ist. Manuell können Sie den Routing-Eintrag über die Kommandozeile an den Clients festlegen:

```
route add 172.17.0.0 mask 255.255.0.0 172.16.1.1 -p
```

## 2.6.2 NAT mittels Internet-Verbindungsfreigabe direkt auf dem Host einrichten

Wenn Sie im oben genannten Beispiel den Verkehr aus dem virtuellen Segment über den Host ins LAN leiten (Abbildung 2.34), haben Sie gleichzeitig die Möglichkeit, die Windows Firewall und die so genannten Internet-Verbindungsfreigabe (*Internet Connection Sharing – ICS*) des Hosts zu verwenden. Damit können Sie nur bestimmte Ports zulas-



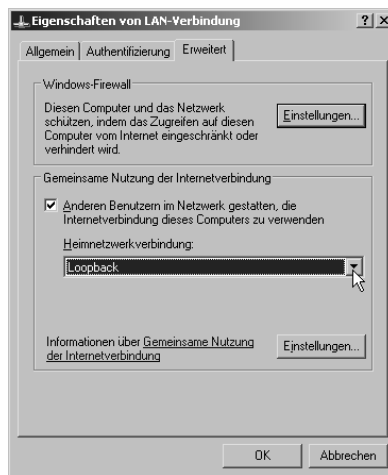
sen, unter denen das virtuelle LAN-Segment erreichbar ist. Weiterhin lässt sich damit auch für Virtual Server NAT verwenden, um VMs über die Host-Identität ins Internet oder ins LAN zu verbinden. In manchen Umgebungen wird diese Konfiguration aus Sicherheitsgründen verwendet, um die Gäste durch die NAT-Umsetzung vom LAN zu isolieren und nur bestimmte Ports der Gastsysteme aus dem LAN zugänglich zu machen. Das gesamte virtuelle Netzwerk befindet sich dann hinter der Windows-Firewall des Host-Systems.

Ich persönlich finde eine separate virtuelle Maschine als Router praktischer (Abbildung 2.33). Zum einen können Sie darin beliebige Router- und Firewall-Software betreiben, etwa IPCop oder Microsoft ISA-Server. Zum anderen kann diese VM, und damit die gesamte Konfiguration, einfach gesichert oder auf jeden anderen Host übertragen werden. Letztendlich verbraucht eine schlanke virtuelle Software-Firewall nur wenige Ressourcen, wenn es sich nicht um sehr großen Netzwerkverkehr handelt. Trotzdem will ich Ihnen folgenden Hinweis auf die Internet-Verbindungsfreigabe am Host nicht vorenthalten.

Die Windows-Firewall können Sie auf dem Host über SYSTEMSTEUERUNG/FIREWALL aktivieren oder deaktivieren. Im Reiter AUSNAHMEN können dann bestimmte Ports für die Kommunikation geöffnet werden. Weiterhin finden Sie in der Netzwerkumgebung des Hosts bei den Eigenschaften jedes Adapters unter dem Reiter ERWEITERT die Konfigurationsmöglichkeiten der Internet-Verbindungsfreigabe, zu sehen unter GEMEINSAME NUTZUNG DER INTERNET-VERBINDUNG. Sie können auf dem physischen Adapter des Hosts den Loopback-Adapter als private Netzwerkverbindung (Heimnetzwerkverbindung) festlegen (Abbildung 2.35). Weitere Informationen zur Konfiguration der Internet-Verbindungsfreigabe für Virtual Server finden Sie hier:

<http://support.microsoft.com/kb/888849/en-us>

Abbildung 2.35:  
Die Internet-Verbindungsfreigabe auf dem Host kann als NAT-Ersatz für Virtual Server dienen



Als Alternative können Sie auf einem Windows 2003 Host auch die erweiterten RAS-Dienste zur Konfiguration des Routings verwenden. Sie finden die Konfiguration unter SYSTEMSTEUERUNG/VERWALTUNG/ROUTING UND RAS.

Unter VMware wird hin und wieder von Problemen berichtet, wenn VMs über einen Wireless LAN-Adapter auf dem Host ans LAN angebunden werden. Das hängt vom Hersteller und vom Treiber des Wireless-Adapters ab. Sollte es mit dem Adapter auch bei der Verwendung des VMware NAT-Dienstes zu Problemen kommen, bietet sich als Notlösung ebenfalls die Vorgehensweise mit ICS auf dem Host an.

**Nutzung eines Wireless-Adapters im Host**

## **2.7 Performance beim Netzwerkzugriff der Gäste optimieren**

Mit welcher Geschwindigkeit die Gäste untereinander und mit dem LAN kommunizieren können, ist nicht nur von der eingebauten physischen Netzwerkkarte abhängig. Vor allem die CPU-Leistung des Host-Systems ist ein entscheidender Faktor. Weiterhin gibt es unter VMware optimierte Treiber für die emulierten Netzwerkkarten, die von den VMware Tools installiert werden.

### **2.7.1 Performance virtueller Maschinen im 100-Mbit-Netzwerk**

Stehen im Host nur 100-Mbit-Netzwerkverbindungen zur Verfügung, dann können Sie davon ausgehen, dass die Netzwerkperformance fast ohne Verluste von den VMs auf die Hardware umgesetzt wird. Das größte Problem ist die geringe Bandbreite einer einzelnen 100-Mbit-Verbindung, da sich mehrere VMs eine Netzwerkkarte und damit den gleichen Port am LAN-Switch teilen. Hier helfen nur mehrere physische Netzwerkkarten an unterschiedlichen virtuellen Netzwerken und eine Verteilung der Gäste auf diese Netzwerke (Abbildung 2.36) oder Adapter-Teaming.

### **2.7.2 Performance im Gigabit-Netzwerk mit virtuellen Adaptern**

Richtig interessant wird es erst bei der Verwendung von Gigabit-Ethernet. Hier spielt die CPU-Leistung im Host eine entscheidende Rolle. Bei hoher Belastung einer virtuellen Netzwerkkarte, etwa durch Kopiervorgänge, kann eine Host-CPU mit der Emulation der virtuellen Adapter voll ausgelastet sein. Wenn Sie während einer Kopieraktion von einem physischen Rechner in eine VM einmal die CPU-Auslastung auf dem Wirt beobachten, z.B. im Taskmanager, dann sehen Sie je nach CPU teilweise Werte von 90% und mehr. Viele

**Netzwerkperformance ist CPU-abhängig**

Anwender wundern sich, dass Kopiervorgänge zwischen zwei VMs auf dem gleichen Host im virtuellen Netzwerk teilweise langsamer ablaufen als zwischen zwei VMs auf unterschiedlichen Hosts. Das ist auch der Fall, wenn beide Gäste auf separate schnelle Datenträger zugreifen. Schauen Sie sich die CPU-Auslastung an, verstehen Sie, warum das so ist.



Die Rechenleistung ist der begrenzende Faktor für die nutzbare Bandbreite der Netzwerkanbindung in den Gästen. Aus diesem Grunde werden Sie die volle Leistung, die der Host in Ihrem physischen Gigabit-Netz erreichen kann, nur eingeschränkt in den Gästen verwenden können. Auch mehrere dediziert zugewiesene physische Netzwerkadapter für verschiedene Gäste bringen nicht unbedingt mehr Leistung, wenn nur wenige oder schwache CPUs auf dem Host zur Verfügung stehen.

### **Interrupt-Drosselung für eine bessere Performance**

Manche Netzwerkkarten unterstützen eine Funktion, nicht für jedes ankommende Ethernet-Paket einen Interrupt auszulösen, sondern erst mehrere Pakete zu sammeln. Diese Funktion nennt sich bei Intel-Adaptoren z.B. *Interrupt-Drosselungsrate* oder wird auch als *Interrupt Coalescing* bezeichnet. Durch einen höheren Wert kann die CPU im Host bei hoher Netzwerklast entlastet werden, weil für eine bestimmte übertragene Datenmenge weniger Interrupts generiert werden. Es lohnt sich, in die Dokumentation der Netzwerkkarte zu schauen, um die optimalen Einstellungen zu finden. Bei Gigabit-Intel-Adaptoren können Sie über die Netzwerkumgebung in den Eigenschaften der Netzwerkkarte auf dem Host den Wert für die Interrupt-Drosselungsrate maximieren.

In vielen Fällen fehlen 10%–25% der physischen Netzwerkperformance in einer VM, unter Umständen mehr. Einzig und allein der ESX kann es schaffen, abhängig von den Paketgrößen, nahe an den physisch möglichen Wert heranzukommen, aber auch lange nicht in jeder Situation. Natürlich müssen Sie bei solchen Betrachtungen bedenken, dass es in der Praxis nur wenige Systeme gibt, die permanent die volle Gigabit-Leistung abfordern. Wenn doch, dann sollten Sie vor der Virtualisierung unbedingt in einer Pilotumgebung Ihre Anwendungen testen. Entweder können Sie den Host mit genügend CPU-Power ausstatten, oder Sie verteilen netzwerkintensive Gäste auf verschiedene Hosts.

## Physische Netzwerkkarten bestimmten VMs zuweisen

Vor allem im produktiven Bereich ist es sinnvoll, vorhandene Netzwerkkarten dediziert bestimmten Gästen zuzuweisen. Es ist z.B. möglich, einer VM, die viel Bandbreite benötigt, eine eigene Netzwerkkarte zu geben. Die restlichen VMs können sich dagegen die Bandbreite eines anderen Adapters teilen. Ebenso wird eine Anbindung verschiedener VMs auf dem gleichen Host an unterschiedliche LAN-Segmente möglich. Da jede physische Netzwerkkarte einem eigenen virtuellen Netzwerk zugewiesen ist, können Sie Ihre VMs flexibel auf diese Netzwerke verteilen (Abbildung 2.36). Wie bereits erwähnt, wenn es um Lastverteilung geht, wird bei voller Auslastung aller Adapter die CPU allerdings zum Flaschenhals.

### Last verteilen

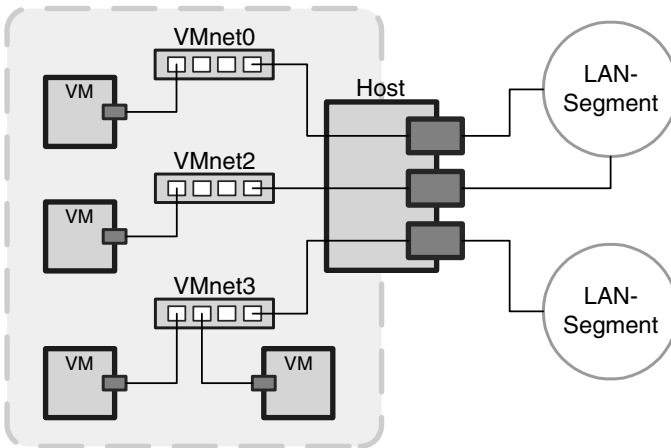


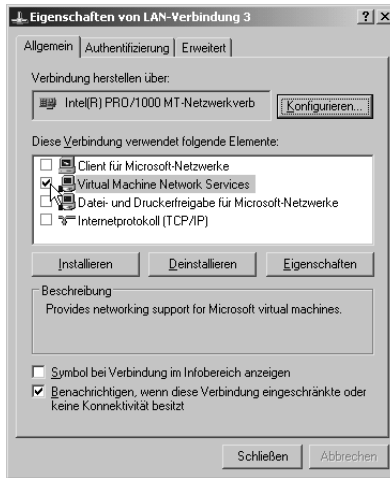
Abbildung 2.36:  
Einzelne VMs können bestimmten physischen Adaptern zugewiesen werden, mehrere VMs können sich auch einen Adapter teilen

## Isolation der Netzwerkkarten gegen „Mitlauscher“

Wenn mehrere VMs, auch nur passiv, in einem Netzwerk mithören, geht die maximale Leistung eines belasteten virtuellen Adapters ebenfalls um 5–10% zurück. Das gilt auch, wenn der Host selbst durch gebundene Protokolle auf einer physischen Netzwerkkarte mithört. Deshalb ist es sinnvolle Praxis, möglichst alle Protokolle am Host von denjenigen physischen Adaptern zu entbinden, die nur für die Gäste verwendet werden. Der Host benötigt nur eine Netzwerkkarte zur eigenen Kommunikation, etwa für Administration und Kopiervorgänge. Bei allen anderen Adaptern sollte nur das *VMware Bridge Protocol* bzw. *Microsofts Virtual Machine Network Services* gebunden sein. Sonst nichts, auch kein TCP/IP (Abbildung 2.37).

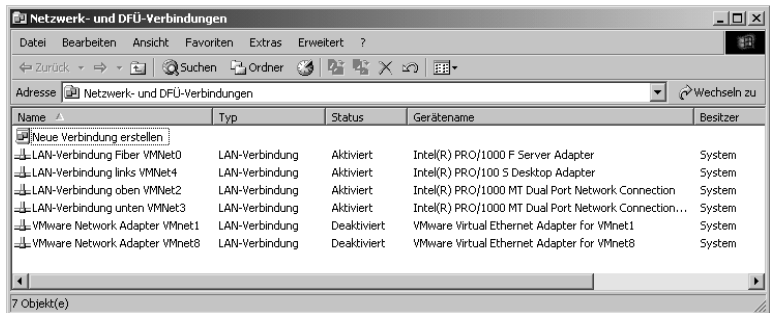
### Keine weiteren Protokolle binden

Abbildung 2.37:  
Für dedizierte physische Adapter sollte auf dem Host nur das jeweilige Bridge-Protokoll gebunden sein



Bei dieser Gelegenheit ist es zur besseren Übersicht nützlich, den Adaptern auf dem Host in der Netzwerkumgebung möglichst sinnvolle Namen zu geben (Abbildung 2.38).

Abbildung 2.38:  
Die Host-Adapter können zur besseren Übersicht umbenannt und an bestimmte virtuelle Netzwerke gebunden werden



### Optimierte Netzwerkkartentreiber in den Gästen

Durch optimierte Netzwerkkartentreiber in den Gästen wird die Performance ebenfalls verbessert. Installieren Sie deshalb immer die VMware Tools in den Gastsystemen (siehe auch „Die Adaptermodelle vlane, vmxnet und e1000 in den Gästen“).

### Probleme mit der Duplex-Einstellung der physischen Adapter

Wenn die Netzwerkperformance der Gäste besonders schlecht ist, dann kann die Ursache auch im physischen Netzwerk liegen. Ein häufiges Problem ist die unterschiedliche Einstellung der Duplex-Art oder der Übertragungsgeschwindigkeit auf Seiten des Switches bzw. der Netzwerkkarte im Host. Im besten Falle sollten beide Seiten entweder fest auf die gleichen Werte eingestellt sein, oder beide Seite verwenden eine automatische Aushandlung (*Autonegotiation*). Eine Kombination (z.B. Switch Auto, Netzwerkkarte fest eingestellt) führt häufig zu Problemen. Wenn beispielsweise der Switch der Meinung

ist, mit *full duplex* zu kommunizieren, die Netzwerkkarte aber nur auf *half duplex* eingestellt wurde, dann kommt es zu sehr vielen Paketkollisionen (*Collisions*) auf der Verbindung, und die Übertragung wird massiv behindert.

Gigabit-Ethernet muss grundsätzlich auf *Autonegotiation* stehen, da auch die Übertragungsrate anhand der Leitungsqualität eingestellt wird. Gigabit-Ethernet verwendet schon von Haus aus immer *full duplex*.

### **Teaming von Netzwerkkarten zum Lastausgleich oder zur Fehlertoleranz**

Beim Teaming werden mehrere Netzwerkkarten zur besseren Ausfallsicherheit oder auch zur Erhöhung der Performance logisch zusammengeschlossen. Dazu muss der Hersteller einen speziellen Treiber liefern, der das Management der zusammengefassten physischen Adapter übernimmt. Für das Host-Betriebssystem entsteht ein neuer logischer Adapter, der unter den Virtualisierern wie jede andere physische Netzwerkkarte verwendet werden kann.

Die Funktion der Teaming-Adapter ist vom Hersteller und dessen Treibern für die Netzwerkkarten abhängig. Nur der ESX Server unterstützt Teaming von sich aus, da er seinen eigenen Kernel und die Treiber selbst mitbringt und damit nicht abhängig von einem Wirtsbetriebssystem ist.

### **Probleme mit schlechter Performance durch Offload TCP Segmentation**

Microsoft beschreibt speziell für Virtual Server ein Problem mit sehr langsamen Netzwerkverbindungen in virtuelle Maschinen, das durch die so genannte Offload TCP Segmentation auf dem Host ausgelöst wird:

<http://support.microsoft.com/kb/888750/en-us>

### **Abschalten der beiden virtuellen VMware Adapter VMnet1 und VMnet8 auf dem Host**

Bei Leistungsproblemen mit dem Netzwerk auf einem Host unter VMware kann es in manchen Fällen helfen, die beiden Host-Adapter VMnet1 und VMnet8 auf dem Host in der Netzwerkumgebung zu deaktivieren. Vor allem bei langsamen Browsing-Vorgängen im Windows Explorer kann das helfen.

## 2.8 Eindeutige MAC-Adressen der virtuellen Adapter

Dem heiklen Thema MAC-Adressen müssen wir gesonderte Aufmerksamkeit schenken.



Physische Ethernet-Karten werden durch eine eindeutige, 48 Bit lange ID gekennzeichnet, die *Media Access Control Address*, kurz MAC-Adresse. Eigentlich sollte es weltweit keine zwei Netzwerkkarten mit der gleichen Nummer geben. Die Kommunikation aller Protokolle im LAN, egal ob TCP/IP oder IPX/SPX, läuft auf der untersten Ebene immer über diese Hardware-Nummer. Nur anhand der MAC-Adresse kommen letztendlich Pakete bei der richtigen Netzwerkkarte an. Gibt es im gleichen Netzwerk zwei Adapter mit der gleichen MAC-Adresse, dann wird keiner der beiden Adapter im LAN ordentlich kommunizieren können. MAC-Adressen-Konflikte erzeugen im Betriebssystem meist keine sichtbare Fehlermeldung, das erschwert die Fehlersuche.

### 2.8.1 MAC-Adressen beim Klonen und Kopieren von VMs automatisch anpassen

Doppelte MAC-Adressen dürften in der realen Welt eigentlich nie auftreten. In unserer virtuellen Welt ist es aber durchaus möglich, dass zwei VMs mit der gleichen MAC-Adresse existieren. Nach einem Kopiervorgang einer kompletten VM hat die Kopie erst einmal die gleichen Einstellungen wie die Vorlage. Damit haben auch die Netzwerkadapter dieselbe MAC-Adresse und stören sich gegenseitig im Netzwerk. *Keine Angst:* Normalerweise wird die MAC-Adresse einer VM automatisch festgelegt, und der Virtualisierer versucht, eindeutige Adressen zu vergeben. Auch beim Kopieren von VMs setzen die Virtualisierer die MAC-Adressen zurück und generieren neue. Meistens funktioniert das auch. In seltenen Fällen, vor allem bei unterschiedlichen Hosts im gleichen Netzwerk, kann es aber auch zu doppelten MAC-Adressen kommen.



Die MAC-Adresse eines Bridged-Adapters einer virtuellen Maschine hat nichts mit der MAC-Adresse der physischen Host-Netzwerkkarte zu tun, über welche die Kommunikation mit dem LAN abläuft. Jeder virtuelle Adapter und jeder physische Adapter müssen eine eigene MAC-Adresse haben.

## 2.8.2 MAC-Adresse in den Gästen manuell festlegen

Die MAC-Adresse wird manchmal auch von bestimmten Anwendungen benutzt, um einen Rechner eindeutig zu identifizieren. So gibt es einige Provider oder Netzwerkzugänge in Firmen, die nur dann einen Rechner authentifizieren, wenn die MAC-Adresse der Netzwerkkarte dieses Rechners vorher registriert wurde. In diesem Falle ist es ärgerlich, wenn sich die MAC-Adresse einer VM ändert. Auch Software wird manchmal auf eine MAC-Adresse registriert und lizenziert. Deshalb kann es auch beim Übernehmen einer physischen Maschine in eine VM (P2V – *physical to virtual*) notwendig werden, die alte MAC-Adresse zu erhalten und dem virtuellen Adapter eine bestimmte MAC-Adresse manuell zu vergeben.

Wenn es sich um die Virtualisierung eines physischen Rechners handelt, dann darf nach dem festen Vergeben der MAC-Adresse in der VM die originale physische Karte im LAN nie mehr in Betrieb sein, weil es sonst zu Konflikten kommt.



## 2.8.3 MAC-Adressen virtueller Adapter unter VMware und die UUID

Die MAC-Adresse ist unter VMware direkt vom *UUID* (*Universally Unique Identifier*) abhängig. Diese 128 Bit lange ID ist für jede virtuelle Maschine eindeutig. Sie wird automatisch beim Start einer VM generiert. Unter anderem ist die UUID abhängig vom Verzeichnis auf dem Host, in dem sich die VM befindet, und vom Namen der vmx-Datei. Das bedeutet, dass eine VM immer dann automatisch eine neue UUID zugewiesen bekommt, wenn die VM kopiert oder verschoben wurde bzw. wenn sich der Name der Konfigurationsdatei geändert hat. Sie werden auf eine solche Neuinitialisierung der UUID durch eine Abfrage beim Start des Gastes aufmerksam gemacht (Abbildung 2.39).

**Die UUID eines Gastes**

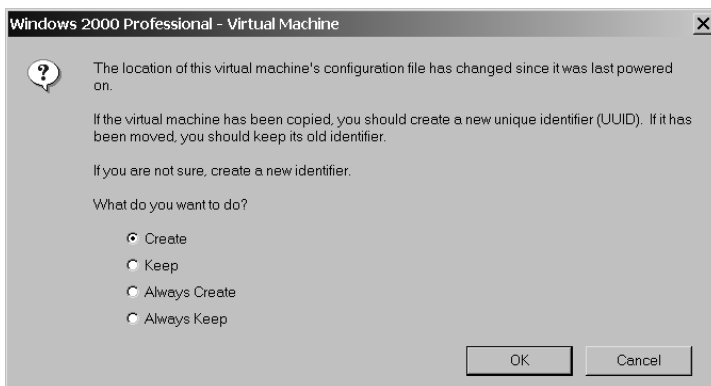


Abbildung 2.39:  
Die UUID ändert sich bei jedem Kopiervorgang oder Umbenennen einer vmx-Datei. Von ihr hängen die MAC-Adressen ab



An dieser Stelle können Sie sich entscheiden, ob die UUID der VM neu gebildet werden soll oder ob weiterhin die vorhandene Nummer verwendet wird. Die Frage erscheint einmalig nach jedem Kopieren, Verschieben oder Umbenennen der Konfigurationsdatei.

- ▶ *Create*: neue UUID wird gebildet.
- ▶ *Keep*: UUID bleibt erhalten.
- ▶ *Always Create*: Es wird in Zukunft immer nach jedem Kopieren eine neue ID ohne Nachfrage gebildet. Das ist sinnvoll bei Muster-VMs, die ständig kopiert werden.
- ▶ *Always Keep*: Die ID wird nie geändert. Das ist problematisch, wenn die VM später einmal vervielfältigt wird, weil dann zwei Maschinen die gleiche UUID besitzen. Sinnvoll ist das, wenn Sie verhindern wollen, dass sich beim Kopieren oder Verschieben der VM die UUID, und damit die MAC-Adressen, ändert.

Die beiden letzten Antworten hinterlassen in der vmx-Datei folgende Einträge:

```
uuid.action = "create"
```

oder

```
uuid.action = "keep"
```

Werden diese Einträge manuell entfernt, dann fragt VMware wieder nach jedem Kopieren oder Verschieben einer VM. Folgende weitere Einträge existieren zur MAC-Adresse in der vmx-Datei von VMware:

```
uuid.bios = "56 4d a8 bc 63 81 8a a6-3d b8 25 0f ed
73 67 a6"
ethernet0.generatedAddress = "00:0c:29:73:67:a6"
Ethernet0.addressType = "generated"
ethernet0.generatedAddressOffset = "0"
ethernet1.generatedAddress = "00:0c:29:73:67:b0"
Ethernet1.addressType = "generated"
ethernet1.generatedAddressOffset = "10"
```

### Beispiele zur UUID

Der erste Adapter einer VM (Ethernet0) erbt in seiner MAC-Adresse immer die letzten drei Stellen der UUID, weitere Adapter (Ethernet1) werden dann im letzten Byte mit einem Offset hochgezählt. Zwei Beispiele zum Umgang mit der UUID-Änderung sollen Ihnen die Verwendung verdeutlichen:

- ▶ Wenn Sie eine VM für eine Testumgebung durch Kopieren vervielfältigen, dann müssen Sie neue UUIDs (und damit MAC-Adressen) erstellen. Nur so sind die MAC-Adressen eindeutig, und die Clones können miteinander kommunizieren.
- ▶ Wenn Sie auf dem Host nur aufräumen und dabei Verzeichnisse ändern, können Sie die vorhandene UUID (und damit die MAC-Adressen) behalten.

## Feste MAC-Adressen unter VMware vergeben – offizielle Methode

Unter VMware ist es etwas umständlich, die MAC-Adresse der Gäste festzulegen. Sie müssen die Konfigurationsdatei (\*.vmx) Ihrer virtuellen Maschine editieren. Hier zuerst die offizielle Methode, die aber einige Nachteile hat:

1. Löschen Sie für einen bestimmten Adapter X folgende Zeilen:  
`ethernetX.generatedAddress`  
`ethernetX.addressType`  
`ethernetX.generatedAddressOffset`
2. Fügen Sie jetzt die Zeile mit Ihrer festen MAC-Adresse ein:  
`ethernetX.address = 00:50:56:XX:YY:ZZ`
3. Folgender Eintrag entsteht beim Start der VM dann automatisch:  
`EthernetX.addressType = "static"`

Wie Sie allerdings schon an der Syntax XX:YY:ZZ sehen, können Sie keine beliebigen MAC-Adressen vergeben. Die ersten Stellen einer MAC-Adresse spezifizieren den Hersteller der Netzwerkkarte, VMware hat dafür einen offiziellen festen Bereich. Nur die letzten drei Stellen sind frei wählbar, innerhalb enger Grenzen:

- ▶ XX muss ein Hex-Wert sein zwischen 00h and 3Fh.
- ▶ YY und ZZ müssen Hex-Werte sein zwischen 00h and FFh.

Mit dieser Methode ist es unmöglich, die Adresse einer physischen Netzwerkkarte in eine VM zu übernehmen!

## Feste MAC-Adressen unter VMware direkt im Gastbetriebssystem festlegen (inoffizielle Methode)

Soll der Adapter einer VM eine völlig unabhängige MAC-Adresse erhalten oder muss eine VM nach der Portierung von einer realen Maschine die MAC des alten physischen Adapters nachahmen, dann gibt es dafür unter VMware folgende Lösung. Im Betriebssystem in der VM kann direkt im Netzadapter eine explizite MAC-Adresse angegeben werden. Diese überschreibt dann die MAC-Adresse, die VMware eigentlich dem Adapter zugewiesen hat. Diese Methode kann in jedem Gast verwendet werden.

Der Nachteil dieser Methode ist, dass Sie bei jedem Wechsel der virtuellen Netzwerkkarte (z.B. Neuerkennung durch geänderte virtuelle Hardware) die Adresse neu einstellen müssen. Weiterhin funktioniert diese Methode unter VMware nur, wenn in der vmx-Datei keiner der beiden folgenden Einträge enthalten ist:

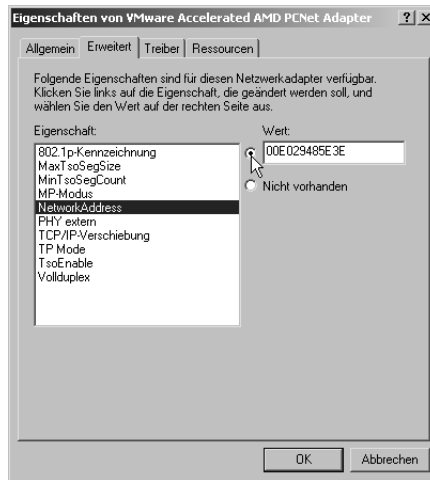
```
ethernetX.downWhenAddrMismatch = TRUE
ethernetX.noForgedSrcAddr = TRUE
```



**Windows** Die Einstellung unter Windows-Gästen finden Sie hier:

1. Öffnen Sie SYSTEMSTEUERUNG/NETZWERKVERBINDUNGEN.
2. Wählen Sie mit einem Doppelklick die Netzwerkkarte, und gehen Sie in die EIGENSCHAFTEN.
3. Wählen Sie unter Netzwerkkartentreiber KONFIGURIEREN und dort ERWEITERT.
4. Unter NETWORK ADDRESS können Sie die neue MAC-Adresse eintragen.

Abbildung 2.40:  
Eine beliebige MAC-  
Adresse kann unter  
VMware nur im  
virtuellen Adapter  
des Gastes festgelegt  
werden



**Linux** Unter Linux-Gästen kann ein Überschreiben der MAC-Adresse mit dem Befehl `ifconfig` erfolgen:

```
ifconfig ethX down
ifconfig ethX up hw ether 00:0e:6c:a3:ae:82
ifconfig ethX up
```

Das entsprechende `ifconfig`-Kommando sollte am besten im passenden Startskript oder in einer Konfig.-Datei Ihrer Distribution angepasst werden. Unter Debian z.B. in der `/etc/network/interfaces`:

```
iface eth0 inet static
pre-up /sbin/ifconfig eth0 hw ether 00:0e:6c:a3:ae:82
```

### Wie finde ich heraus, welche MAC-Adresse ein Adapter hat?

Die MAC-Adresse eines nachzuziehenden Quellsystems bekommen Sie mit folgenden Befehlen heraus:

- Unter Windows: `ipconfig /all`
- Unter Linux: `ifconfig`

In der Ausgabe erscheint eine Zeile mit der MAC-Adresse. Diese Adresse ist dann ohne Bindestriche im Adapter der virtuellen Maschine einzutragen und die VM neu zu starten:

Physikalische Adresse . . . . . : 00-0E-6A-A5-AE-80

### Kontrolle, ob die VM wirklich die zugewiesene MAC verwendet

Zur Kontrolle, ob die Manipulation erfolgreich war, können Sie von einer beliebigen anderen Station im Netz ein Ping auf die VM machen und anschließend folgenden Befehl ausführen:

```
arp -a
```

Hier muss zur IP der angepassten virtuellen Maschine die geänderte MAC-Adresse des Adapters erscheinen.

## 2.8.4 MAC-Adressen virtueller Adapter unter Microsoft Virtual PC/Server

Beim Kopieren von VMs auf einen anderen Host unter Virtual PC kann es passieren, dass die MAC-Adressen nicht angepasst werden. Um die MAC-Adresse eines virtuellen Adapters zurückzusetzen, löschen Sie den HEX-Wert aus folgender Zeile der Konfigurationsdatei (\*.vmc):

```
<ethernet_card_address type="bytes">0003FFAEFFDE</ethernet_card_address>
```

Die Zeile muss dann so aussehen, dadurch wird beim nächsten Start der VM automatisch eine neue MAC gebildet:

```
<ethernet_card_address type="bytes"></ethernet_card_address>
```

### Feste MAC-Adresse für Microsoft-Gäste vergeben

Die MAC-Adresse einer virtuellen Netzwerkkarte kann unter Virtual Server ganz flexibel und bequem in den Einstellungen jedes Adapters unter VIRTUELLE COMPUTER/KONFIGURIEREN/NAME DER VM/NETZWERKKARTEN/ ETHERNETADRESSE (MAC) festgelegt werden (Abbildung 2.41). Wenn Sie hier nichts festlegen, generiert Virtual Server eine MAC-Adresse automatisch.

#### Virtual Server

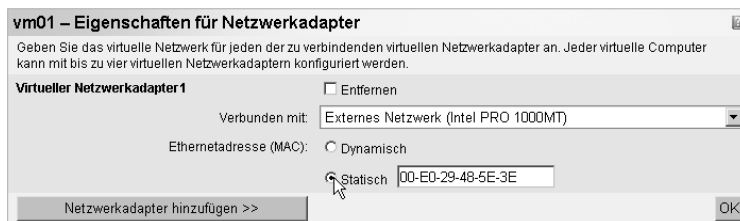


Abbildung 2.41:  
Unter Virtual Server können den virtuellen Adaptern beliebige MAC-Adressen zugewiesen werden

Unter Virtual PC werden MAC-Adressen immer automatisch gebildet. Sie können aber die Konfigurationsdatei (\*.vmc) editieren. Die MAC-Adresse finden Sie hier:

#### Virtual PC

```
<ethernet_card_address type="bytes">0003FFxxxxxx</ethernet_card_address>
```



Beim Entfernen und Neuaufnehmen einer VM in die Liste der virtuellen Maschinen (VM neu registrieren) wird von Virtual PC auch die MAC-Adresse wieder generiert und damit Ihr manueller Eintrag in der Konfigurationsdatei überschrieben.

## 2.9 Geister-Netzwerkkarten bei Änderung der virtuellen Hardware in einem Gast

Beim Wechsel des Adaptertyps, oder auch beim Upgrade der virtuellen Hardware einer VM, erkennt das Betriebssystem in der VM unter Umständen eine neue Netzwerkkarte. Der alte Adapter verschwindet in der Versenkung. Bei Windows-Gästen existiert die alte Vorgänger-Netzwerkkarte weiterhin in der Registry, ohne in der Netzwerkkonfiguration zu erscheinen. Leider behält dieser versteckte Adapter auch teilweise seine Einstellungen, vor allem eine vorher manuell zugewiesene IP-Adresse.

**IP-Adresse  
bereits in Ver-  
wendung!**

Soll nun die gleiche Adresse dem neu erkannten Adapter wieder zugewiesen werden, kommt es zu einer Fehlermeldung, die Adresse wäre bereits in Verwendung. Nach genauem Durchlesen des ellenlangen Fehlertextes kann man die Meldung zwar ignorieren. Wer aber trotzdem den verborgenen Adapter im Geräte-Manager sucht, um ihn zu entfernen, wird ihn dort nicht finden. Um dem hartnäckigen Versteckspiel ein Ende zu bereiten, hilft folgende Vorgehensweise:

1. Starten Sie eine Kommandozeile mit START/AUSFÜHREN/CMD.EXE.
2. Geben Sie hintereinander in der gleichen DOS-Box folgende Kommandos ein:  

```
set devmgr_show_nonpresent_devices=1
start DEVMGMT.MSC
```
3. Wählen Sie im so gestarteten Geräte-Manager ANSICHT/AUSGE-  
BLENDETE GERÄTE ANZEIGEN.
4. Jetzt erst ist der verloren geglaubte Adapter als ausgegrauter Eintrag zu finden. Er kann nun mit der rechten Maustaste und DEINSTALLIEREN entfernt werden.

# 3 Die virtuellen Platten als Herzstück der Gastsysteme

Virtuelle Platten sind das Herzstück einer jeden VM, schließlich beherbergen sie die Daten und die Betriebssysteminstallation des Gastes. Die versehentlich entfernte Konfigurationsdatei einer VM können Sie schnell wieder neu erstellen, haben Sie dagegen eine virtuelle Platte gelöscht, verschwindet damit das eigentliche Gastsystem oder zumindest wichtige Inhalte. Diese zentrale Rolle virtueller Datenträger ist Grund genug, ihnen ein eigenes Kapitel zu widmen.

**Die virtuelle Platte mit dem Gastsystem ist das Herzstück einer VM**

Die Workshops in *Teil 2* des Buches haben Ihnen bereits den grundlegenden Umgang mit virtuellen Platten vermittelt. In diesem Kapitel lernen Sie erweiterte Funktionen kennen – unter anderem wie Sie eine virtuelle IDE-Platte in eine virtuelle SCSI-Platte umwandeln, was der richtige Treiber für den emulierten Controllertyp im Gast ist oder wie Sie auf den Inhalt eines virtuellen Datenträgers direkt vom Host aus Zugriff erhalten.

## 3.1 Virtuelle Platten aus der Gast-Perspektive oder aus der Host-Perspektive

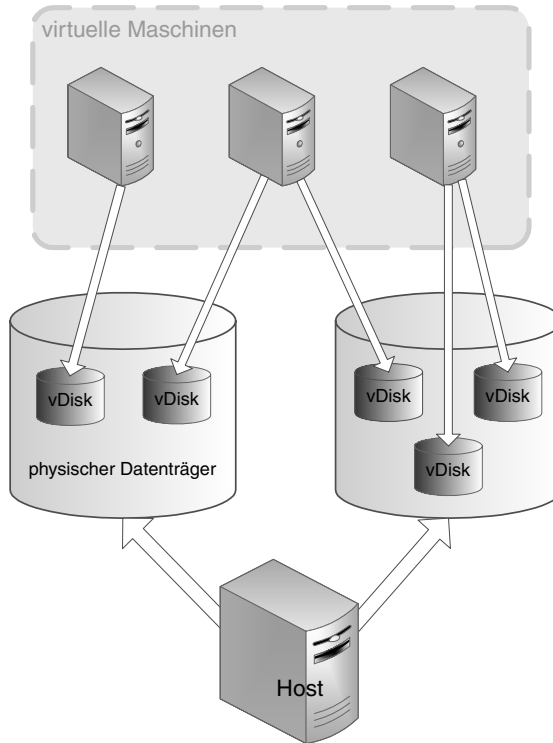
Eine virtuelle Platte kann aus zwei Perspektiven betrachtet werden. Von außen, aus der Sicht des Hosts, präsentiert sie sich völlig anders als aus der Sicht des Gastsystems innerhalb einer VM (Abbildung 3.1).

### 3.1.1 So sieht der Host eine virtuelle Platte

Aus der Sicht des Hosts sind virtuelle Platten große Dateien (ich nenne sie im Buch *Behälterdateien*), die auf einem physischen Datenträger, z.B. auf einer lokalen Festplatte, einem RAID, einem externen SAN oder auf einer Netzwerkfreigabe im LAN, untergebracht sind. Ausführliche Hinweise zu möglichen Wirtsdatenträgern finden Sie in *Teil 1, Kapitel 1, „Grundlagen virtueller Maschinen und Hinweise zur Hardware“*. Sämtliche Schreib- und Lesezugriffe der Gastsysteme leitet der Virtualisierungslayer in eine dieser Behälterdateien um. Die VM meint dabei, mit einer physischen Festplatte zu arbeiten. Auf den Host-Datenträger hat ein Gastsystem dabei keinen direkten Zugriff. Beispielsweise kann die virtuelle Platte einer Linux-VM mit *ext3*-Partition problemlos auf der physischen *NTFS*-Partition eines Windows-Hosts liegen.

**Behälterdateien auf einem physischen Datenträger**

Abbildung 3.1:  
Virtuelle Platten sind  
Behälterdateien, die  
auf verschiedenen  
physischen Daten-  
trägern eines Hosts  
liegen können



Sie können virtuelle Platten durch Kopieren der Behälterdatei einfach sichern, archivieren und weitergeben. Duplizierte virtuelle Platten lassen sich in eine neue VM einbinden, was dem Klonen eines physischen Systems mittels Imaging-Tools entspricht. Und eine virtuelle Platte versehentlich zu löschen, käme für den Gast dem Totalverlust der Daten auf einer defekten Festplatte gleich.

Sie können einem Gast auch den direkte Zugriff auf eine physische Festplatte, ohne Umwege über eine Behälterdatei, ermöglichen (siehe Abschnitt 3.5, „Physische Datenträger in einem Gast direkt verwenden – Raw Device Mapping“). Damit verschenken Sie allerdings einiges von der Flexibilität virtueller Platten, und der Leistungsgewinn kann vernachlässigt werden.

#### 3.1.2 So sieht der Gast eine virtuelle Platte

Aus der Sicht des Gastsystems in der VM ist eine virtuelle Platte ein gewöhnlicher Datenträger, der partitioniert und formatiert werden muss. Den Zugriffsvorgang auf eine virtuelle Platte beschreibt bereits Teil 1, Kapitel 1, „Grundlagen virtueller Maschinen und Hinweise zur Hardware“, als Beispiel für die Funktion einer VM. In den Gästen stehen IDE- oder SCSI-Festplatten zur Verfügung, wobei es keine Rolle spielt, auf welchem physischen Datenträger die zugehörigen Behäl-

terdateien tatsächlich residieren. Ein Gast kann auch dann über eine virtuelle SCSI-Platte verfügen, wenn im Host nur physische IDE-Platten eingebaut sind. Mit der Auswahl des emulierten Controllertyps beim Erstellen einer VM entscheiden Sie selbst, welche Art Festplatten im Gast erscheinen, Kombinationen aus IDE und SCSI sind möglich.

Im Gast muss der passende Treiber zum emulierten Controller installiert sein, damit das Betriebssystem auf den virtuellen Datenträger zugreifen kann. Einen Treiber für den physischen Datenträger, etwa für einen speziellen RAID-Controller im Host, benötigt die VM nicht, da der Virtualisierungslayer die physische Hardware vor dem Gastsystem versteckt. Verwenden Sie beispielsweise eine virtuelle IDE-Platte, genügt in der VM der standardmäßig eingerichtete IDE-Treiber. Das Thema Controllertreiber ist ein wichtiger Aspekt bei einer Migration physischer Maschinen in eine VM (*P2V – Physical to Virtual*) oder beim Transport von Gästen zwischen unterschiedlichen Virtualisierungsprodukten. Detaillierte Informationen dazu erhalten Sie unter *Abschnitt 3.7, „Virtuelle SCSI-Controller und die passenden Treiber in den Gästen“*.

**Gerätetreiber  
für die virtuellen  
Controller**

## 3.2 Arten virtueller Platten und deren grundsätzlicher Aufbau

Blieben wir vorerst bei der Sicht des Hosts auf die virtuellen Platten. Wie sind die Behälterdateien aufgebaut, und was ist beim Umgang mit Ihnen zu beachten?

### 3.2.1 Köpfe, Spuren, CHS-Geometrie und LBA-Adressierung physischer und virtueller Platten

Um die Funktion virtueller Platten besser zu verstehen, bietet sich als Einführung ein kleiner Ausflug in die Interna einer physischen Festplatte an.

#### **Aufbau einer physischen Festplatte mit Spuren, Zylindern und Köpfen**

Eine Festplatte enthält mehrere Schreib-/Leseköpfe (*Heads*), die auf einen Stapel rotierender Plattenoberflächen zugreifen. Jede Oberfläche ist in konzentrische Spuren unterteilt, auf denen die Daten in Form von magnetischen Zuständen kodiert sind. Alle jeweils übereinander liegenden Spuren der Oberflächen des Festplattenstapels bezeichnet man als *Cylinder*. Beispielsweise bilden Spur 22 von Oberfläche 0, Spur 22 von Oberfläche 1 usw. den Cylinder 22. Damit spezifiziert die Kom-



bination aus Kopfnummer und Zylinder Nummer genau eine Spur des gesamten Stapels. Jede Spur enthält wiederum gleich lange Abschnitte, die so genannten *Sektoren*. Ein Sektor ist die kleinste adressierbare Einheit einer Festplatte und enthält üblicherweise 512 Byte.

**CHS-Geometrie** Bei einem Zugriff schwenkt die Festplattenelektronik den Arm mit den Magnetköpfen auf den entsprechenden Zylinder, dann werden die Daten des Kopfes der richtigen Oberfläche, und damit einer konkreten Spur, ausgelesen. Ein Sektor der Spur muss erst durch die Umdrehung des Plattenstapels am Magnetkopf vorbeikommen. Ein bestimmter Sektor einer physischen Platte wird also mit einer Kombination aus *Cylinder*, *Head* und *Sektor* adressiert. Die Anzahl aller Zylinder und aller Köpfe (Oberflächen) einer Festplatte und die Sektoren pro Spur ergeben die so genannte *CHS-Geometrie* dieses Laufwerkes (*Cylinders/Heads/Sectors*).

**LBA-Modus** Moderne Rechner und Betriebssysteme verwenden anstelle der CHS-Adressierung häufiger eine logische Durchnummerierung aller Sektoren der Platte, beginnend bei 0. Diese Zählweise bezeichnet man als *LBA* (*Logical Block Addressing*, zu Deutsch: *Logische Blockadressierung*). Die Plattenelektronik muss dann intern die logische LBA-Sektorennummer wieder auf die eigene CHS-Geometrie umrechnen, um auf einen Sektor zuzugreifen.

#### **Aufbau einer virtuellen Platte mit sequenziellen Sektoren in Behälterdateien**

Der Controllertreiber des Betriebssystems in einer VM meint zwar, mit einer physischen Festplatte zu arbeiten, er greift aber nur auf Sektoren zu, die ihm der Virtualisierungslayer aus der Behälterdatei präsentiert. Dort liegen die 512 Byte großen Sektoren sequenziell hintereinander. Erfolgt der Zugriff aus dem Gast mittels CHS-Adressierung, etwa bei älteren Betriebssystemen oder beim Bootvorgang von Windows, muss der Virtualisierungslayer die sequenzielle Sektorennummer in der Behälterdatei errechnen. Aus diesem Grunde verfügen virtuelle Platten ebenfalls über eine CHS-Geometrie. Diese Parameter sind bei VMware abhängig von der Plattengröße sowie vom Typ IDE oder SCSI und werden in der virtuellen Platte vermerkt. Aus diesem Grunde lassen sich virtuelle SCSI-Platten unter VMware, im Gegensatz zu Microsoft, nicht einfach als IDE-Platten einbinden und umgekehrt (siehe Abschnitt 3.8.7, „Umwandeln einer virtuellen IDE-Platte in eine SCSI-Platte unter VMware“).

### 3.2.2 Virtuelle Zuwachsplatten verwenden oder den gesamten Platz der virtuellen Platte vorreservieren

Die virtuellen Platten können vom Host unterschiedlich verwaltet werden. Entweder ist die Behälterdatei nur so groß, wie vom Gast wirklich belegt wird, und sie wächst bei Bedarf Sektor für Sektor mit. Man bezeichnet diesen Typ als *Zuwachsplatte* oder auch *dynamisch erweiterbare virtuelle Festplatte* (Abbildung 3.2). Wurde ein Sektor einer solchen virtuellen Platte vom Gast noch niemals beschrieben, dann ist er in der Behälterdatei nicht vorhanden und belegt keinen Platz auf dem Host-Datenträger.

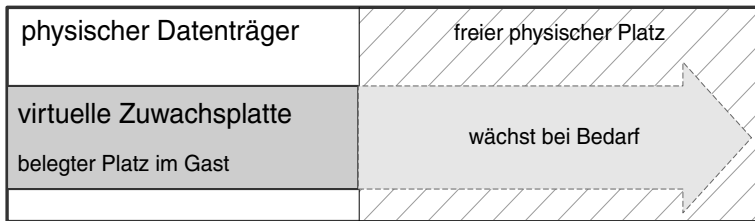


Abbildung 3.2:  
Eine Zuwachsplatte  
belegt nur den wirk-  
lich benötigten Platz  
auf dem Host

Im Gegensatz dazu kann eine Behälterdatei beim Erstellen auch bereits in voller Größe mit Nullsektoren angelegt werden, wodurch der Platz auf dem Host vollständig reserviert ist. Es handelt sich dann um eine *vorreservierte virtuelle Festplatte* (Abbildung 3.3), bei der auch ein vom Gast unbenutzter Sektor immer Platz auf dem physischen Datenträger verbraucht. Was sind die Vor- und Nachteile beider Methoden?

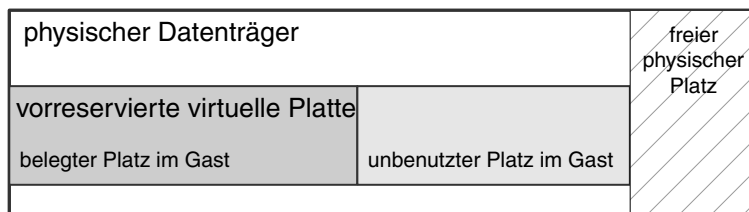


Abbildung 3.3:  
Eine vorreservierte  
virtuelle Platte  
belegt auch den vom  
Gast nicht verwen-  
deten Platz auf dem  
Host-Datenträger

#### Zuwachsplatten (growable Disks) sparen Platz auf dem Host-Datenträger

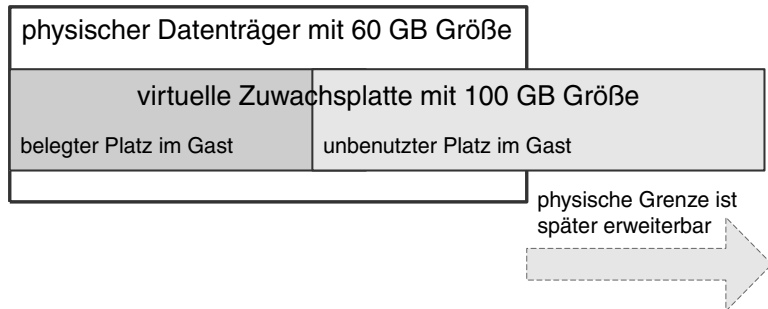
Eine Zuwachsplatte, auch als *growable Disk* (VMware) oder *dynamisch erweiterbare virtuelle Festplatte* (Microsoft) bezeichnet, beginnt als sehr kleine Datei, die sich dem Platzbedarf des Gastes anpasst. Das verschwendet vor allem in Testumgebungen keinen Speicher. Der Gast denkt dabei immer, der konfigurierte Platz der virtuellen Platte steht voll zur Verfügung.



Unter VMware Server müssen Sie beim Erstellen einer virtuellen Platte den Haken an `ALLOCATE ALL DISK SPACE NOW` entfernen, um eine Zuwachsplatte zu erhalten. Bei der VMware Workstation ist das die Standardeinstellung. Der ESX Server unterstützt keine Zuwachsplatten. Bei den Microsoft-Produkten wählen Sie `DYNAMISCH ERWEITERBARE VIRTUELLE FESTPLATTE`.

Es ist sogar möglich, virtuelle Platten zu erstellen, die größer als der physische Datenträger sind. Auf einer kleinen 10-GB-Partition können Sie eine Zuwachsplatte von 50 GB oder mehr anlegen, die für das Gastsystem voll zur Verfügung zu stehen scheint (Abbildung 3.4). Ist der physische Speicher von 10 GB aufgebraucht, kann die Behälterdatei nicht mehr weiter anwachsen. Der Explorer im Gast zeigt trotzdem 40 GB freien Speicher an, Schreibzugriffe werden allerdings blockiert. Wenn Sie keinen weiteren physischen Speicher freimachen können, müssen Sie die virtuelle Platte auf einen anderen Datenträger verschieben.

Abbildung 3.4:  
Virtuelle Zuwachs-  
platten können groß-  
zügig dimensioniert  
werden, da nur der  
wirklich benötigte  
Platz belegt wird



#### Zuwachsplatten können großzügig dimensioniert werden

Das großzügige Dimensionieren von Zuwachsplatten, unabhängig vom real verfügbaren Platz, ist beim nachträglichen Vergrößern eines physischen Datenträgers nützlich. Beispielsweise können Sie durch Hotplug-Techniken einem RAID-Controller im laufenden Betrieb Festplatten hinzufügen und auf einem Windows-Host mit dynamischen Datenträgern sofort mehr Platz auf der Host-Partition schaffen, ohne das System herunterzufahren. In den VMs muss danach keine weitere Anpassung erfolgen, wenn die Partitionen in den Gästen bereits vorausschauend in einer komfortablen Größe angelegt wurden. Eine umständliche Erweiterung, etwa mit Partitionierungstools, ist nicht notwendig.

Eine Gefahr bei der Verwendung von Zuwachsplatten besteht darin, dass eine virtuelle Platte unvermittelt mit Daten bis zu ihrer maximalen Größe gefüllt werden soll, obwohl der physische Datenträger nicht mehr so viel freien Platz hat. Das kann passieren, wenn ein Nutzer auf einen virtuellen Dateiserver große Datenmengen kopiert, in der Annahme, dass der vom Gastsystem als frei angezeigte Platz tatsächlich zur Verfügung steht. Der Gast weiß genauso wenig wie der

Anwender, dass zum weiteren Anwachsen der Behälterdatei auf dem Host kein Speicher mehr zur Verfügung steht. Im schlimmsten Falle stürzen Gastsysteme ab, weil Schreibzugriffe auf die virtuelle Systemplatte nicht mehr ausgeführt werden. Dieser Effekt betrifft alle VMs, die auf dem gleichen, gerade voll gewordenen physischen Datenträger liegen und über Zuwachsplatten verfügen.

Wenn Sie Dateien in einer Zuwachsplatte löschen, wird die Behälterdatei nicht automatisch wieder kleiner. Um sie wieder zu verdichten, ist zusätzlicher Aufwand nötig, siehe dazu: *Abschnitt 3.8.5, „Verdichten virtueller Zuwachsplatten unter VMware und Microsoft“*.



Ein weiterer Nachteil von Zuwachsplatten ist das starke Fragmentieren der Dateien auf dem Host-Datenträger, was zu Performanceverlusten führen kann. Da auch das Gastsystem selbst davon betroffen ist, habe ich das Thema Fragmentierung separat zusammengefasst, siehe *Abschnitt 3.6, „Fragmentierte Dateien auf dem Host sowie im Gast und die Auswirkungen“*.

Trotz der genannten Nachteile sind Zuwachsplatten sehr flexibel in der Ausnutzung des vorhandenen Speicherplatzes. In Testumgebungen sollten Sie ausschließlich diesen Plattentyp verwenden, eine Ausnahme sind nur gemeinsame Datenträger einer Cluster-Konfiguration, da in diesem Falle Zuwachsplatten nicht unterstützt werden. Auch in Produktionsumgebungen sind Zuwachsplatten mit einigen Vorsichtsmaßnahmen eine gute Methode, um Verschnitt durch unbenutzten Plattenplatz zu vermeiden und um dynamisch hinzugefügten Speicher ohne Aufwand den Gästen zugänglich zu machen.

**Zuwachsplatten nutzen den Platz flexibel und ohne Verschnitt**

Eine praxisbewährte Methode, um unvorhergesehenem Platzmangel auf dem Host-Datenträger vorzubeugen, ist das Erstellen mehrerer großer Dummy-Dateien als Platzhalter. Dazu können z.B. zwei bis drei unbenutzte leere virtuelle Platten mit fester Größe (*preallocated Disk* – siehe „Vorreservierte Platten fester Größe (preallocated Disks) für maximale Zugriffsgeschwindigkeit“) oder mehrere ISO-Images dienen. Diese lassen sich im Notfall löschen und schaffen damit etwas Zeit zum Reagieren, sobald es auf einem physischen Datenträger eng wird. Spätestens wenn diese letzten Reserven angegriffen sind, wird es höchste Zeit, die physische Kapazität zu erhöhen oder in den Gästen aufzuräumen. Zusätzlich ist auf dem Host eine Überwachung des freien Platzes anzuraten, die rechtzeitig Warnmeldungen absetzt oder sogar automatisch reagiert.



Als weitere Vorsichtsmaßnahme sollten Sie wenigstens die virtuellen Systemdatenträger produktiver VMs als vorreservierte Platten in einer sinnvollen Größe erstellen. Bei Windows-Servern genügen oftmals schon 5–10 GB, solange keine Datenbanken o.Ä. auf der Systemplatte des Gastes liegen. Die Gäste stürzen so bei physischem Platzmangel nicht gleich ab, weil für Schreibzugriffe auf den virtuellen Systemdatenträgern immer genügend vorreservierter Platz zur Verfügung steht.

#### **Vorreservierte Platten fester Größe (preallocated Disks) für maximale Zugriffsgeschwindigkeit**

Die Alternative zu den Zuwachsplatten ist es, auf dem Host-Datenträger Behälterdateien mit der maximalen Größe der virtuellen Platte anzulegen und den Platz damit zu reservieren, was man als *preallocated Disk* (VMware) oder *virtuelle Festplatte mit fester Größe* (Microsoft) bezeichnet.



Bei der VMware Workstation können Sie den Haken an **ALLOCATE ALL DISK SPACE NOW** setzen, um reservierte Platten zu erstellen, beim VMware Server ist der Haken standardmäßig gesetzt. Der ESX Server erstellt ohne Alternative immer Behälterdateien in der gesamten konfigurierten Größe. Unter den Microsoft-Produkten wählen Sie als Plattentyp **VIRTUELLE FESTPLATTE MIT FESTER GRÖSSE** aus, um den Platz zu reservieren.

Das Reservieren erzeugt sofort recht große Dateien und führt zu einem hohen Verschnitt durch unbenutzten Platz in den Gästen. Je mehr virtuelle Platten auf einem physischen Datenträger liegen, umso mehr Speicher wird dadurch verschwendet. Außerdem müssen Sie beim Weitergeben solcher Platten unnötig viele Nullsektoren kopieren bzw. auf DVD brennen. Die gesamte Behälterdatei vor dem Sichern zu komprimieren, ist wiederum sehr zeitaufwändig. Für eine Testumgebung eignet sich dieser Plattentyp eher nicht.

#### **Reservierte Platten verhindern Fragmentierung**

Der Vorteil reservierter Platten ist, dass die Behälterdatei auf einem leeren Datenträger an einem zusammenhängenden Stück erstellt wird und nicht nach und nach fragmentiert. Außerdem haben Sie von Beginn an den Überblick, wie viel Platz alle virtuellen Platten maximal belegen können und ob der physische Speicher wirklich ausreicht. Allerdings ist die aktuell verfügbare physische Kapazität die Grenze, Sie können die virtuellen Platten nicht großzügig mit dem Blick auf zukünftige Aufrüstungen dimensionieren. Sobald ein Gast mehr Platz benötigt, müssen Sie die virtuellen Platten, samt darin residierender Partitionen, nachträglich anpassen und vergrößern.

## Leistungsunterschiede von Zuwachsplatten und reservierten Platten

In der Performance unterscheiden sich Zuwachsplatten von reservierten Platten vor allem dann, wenn größere Datenmengen erstmalig in eine Zuwachsplatte kopiert werden. Das liegt daran, dass zuerst der Host alle hinzukommenden Sektoren verwalten muss, da die Behälterdatei anwächst. Ein Gast beschreibt auf einer virtuellen Platte allerdings nicht immer neue Sektoren, sondern verwendet viel häufiger vorhandene Sektoren, etwa beim Neuspeichern eines Dokumentes oder beim Auffüllen der Lücken gelöschter Dateien. Dadurch ist ein massives Anwachsen der Behälterdatei eher am Anfang, z.B. bei der Betriebssysteminstallation, gegeben.

Der zweite Grund, dass Zuwachsplatten in der Performance hinter reservierten Platten liegen, kann eine fragmentierte Behälterdatei sein (siehe Abschnitt 3.6, „Fragmentierte Dateien auf dem Host sowie im Gast und die Auswirkungen“).

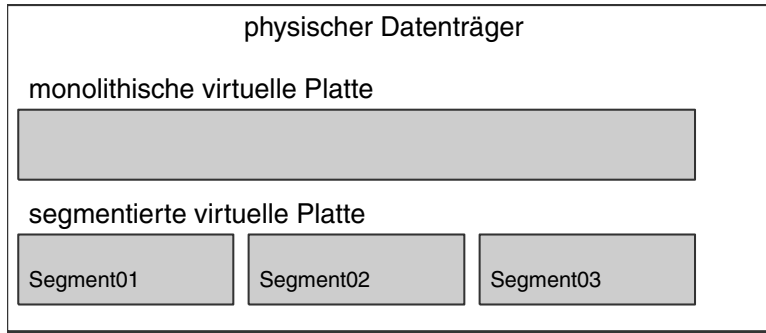
Das Erstellen einer reservierten (*preallocated*) Platte nimmt viel Zeit in Anspruch. Beim VMware Server ist es sehr ärgerlich, wenn Sie beim Erstellen einer 50-GB-Platte für eine Test-VM den standardmäßig gesetzten Haken an `PREALLOCATE ALL DISK SPACE NOW` übersehen haben. Das Anlegen der Behälterdatei dauert sehr lange, und in dieser Zeit ist die Remote Console blockiert. Beim Microsoft Virtual Server kann der Erstellungsvorgang nachträglich abgebrochen werden.



### 3.2.3 Monolithische Platten als große Dateien am Stück oder aufgeteilte Platten in 2-GB-Segmenten

Als weitere Wahlmöglichkeit beim Erstellen einer virtuellen Platte können Sie eine einzige große Behälterdatei am Stück anlegen (*monolithisch* bzw. *single disk*) oder diese Datei in Streifen einer bestimmten Größe segmentieren (*striped* oder *split disk*). Auf Host-Datenträgern mit FAT- oder FAT32-Partitionen ist das Segmentieren wichtig, um die maximale Dateigröße dieser Dateisysteme nicht zu überschreiten. Auf NTFS- oder ext3-Partitionen ist das eigentlich nicht mehr notwendig, da sie ausreichend große Dateien unterstützen.

Abbildung 3.5:  
Virtuelle Platten  
lassen sich als eine  
einzige große Datei  
oder als mehrere  
kleinere Segmente  
anlegen



Unter VMware Workstation und Server können Sie sich entscheiden – setzen Sie bei der Erstellung der Platte den Haken an SPLIT DISK INTO 2 GB FILES, dann liegt die virtuelle Platte in Segmenten zu je 2 GB vor, unabhängig davon, ob es sich um eine Zuwachsplatte oder um eine reservierte Platte handelt. Der ESX Server erstellt nur monolithische Platten, erst beim Exportieren können die Behälterdateien in Segmente aufgeteilt werden, um sie einfacher zu transportieren. Die Microsoft-Produkte teilen die Behälterdateien automatisch auf, sobald diese auf einem FAT-Dateisystem liegen, ansonsten entstehen immer monolithische virtuelle Platten.

#### Vorteile von segmentierten Behälterdateien virtueller Platten

Es bringt in einigen Fällen Vorteile, die Behälterdateien der virtuellen Platten grundsätzlich in Streifen aufzuteilen, auch wenn das Host-Dateisystem große Dateien unterstützt:

#### Segmentierte Platten lassen sich einfacher transportieren

- Es ist wesentlich einfacher, mit mehreren 2-GB-Dateien umzugehen als mit einer großen Datei von 20 GB oder mehr. Zum einen lassen sich 2-GB-Segmente auf mehrere DVDs oder Bänder verteilen. Weiterhin kann ein abgebrochener Sicherungsvorgang, z.B. auf eine langsame USB-Platte, einfacher wiederaufgenommen werden.
- Bei einer Übernahme der virtuellen Platten von einem Hosted-Produkt auf den ESX Server ist es in bestimmten Situationen ebenfalls handlicher, mit Segmenten zu arbeiten. Beispielsweise beträgt die maximale Dateigröße, die in der Service Console des ESX Servers von einer Windows-Freigabe kopiert werden kann, ebenfalls nur 2 GB (siehe auch Teil 2, Kapitel 9, „VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2“).
- Außerdem können segmentierte Behälterdateien einfacher manipuliert werden, etwa zur Umwandlung von IDE in SCSI, da diese Dateien über eine separate Kopfdatei verfügen, in der die Geometriedaten und der Controllertyp der virtuellen Platte im Textformat untergebracht sind (siehe auch Abschnitt 3.8.7, „Umwandeln einer virtuellen IDE-Platte in eine SCSI-Platte unter VMware“).

## Nachteile segmentierter Behälterdateien

Ein Nachteil segmentierter Dateien ist, dass es im Verzeichnis der VM etwas unübersichtlich wird, da eine virtuelle Platte in der Größe von 20 GB immerhin aus elf Einzeldateien besteht. Selbst bei einer Zuwachsplatte werden alle Segmente sofort angelegt, wenn auch nur in minimaler Größe. Zusätzlich entstehen bei jedem Snapshot weitere elf Einzeldateien für die Redo-Logs. Bei der Arbeit mit den multiplen Snapshots der VMware Workstation entstehen dadurch schnell Dutzende Dateien im Verzeichnis einer VM.

### 3.2.4 Empfehlungen für die Verwendung der virtuellen Plattentypen

Welchen Plattentyp Sie in der Praxis verwenden werden, hängt von Ihren Anwendungen und teilweise auch vom persönlichen Geschmack ab. Alles in allem kann ich folgende Empfehlungen geben:

#### Empfohlene Plattentypen in Testumgebungen

- ▶ Erstellen Sie Ihre virtuellen Platten in Testumgebungen möglichst als Zuwachsplatten, um unnötige Platzverschwendung zu verhindern und um das Weitergeben und Kopieren zu vereinfachen.
- ▶ Erstellen Sie monolithische Festplatten anstelle von 2-GB-Segmenten, wenn Sie mehr Übersicht im Verzeichnis Ihrer VMs haben wollen. Bei Testinstallationen werden die Gäste sowieso selten größer als 4 GB, und anstelle von drei Dateien für eine segmentierte Platte existiert so nur eine einzige Datei.
- ▶ Haben Sie dagegen größere virtuelle Platten als 4 GB, die Sie häufiger kopieren oder auf DVD brennen müssen, dann erstellen Sie möglichst 2-GB-Segmente anstelle von großen monolithischen Behälterdateien.
- ▶ Wollen Sie virtuelle Platten unter VMware manipulieren, z.B. um Tests mit den Controllertypen zu machen, dann verwenden Sie am besten segmentierte Platten. Dadurch erhalten Sie eine Kopfdatei im Textformat zum direkten Editieren.

#### Empfohlene Plattentypen in produktive Umgebungen

- ▶ Erstellen Sie alle Systemplatten produktiver Gäste immer als reservierte Platten in einer ausreichenden Größe (etwa 10 GB, wenn keine Datenbanken im Spiel sind), um Abstürze der Gäste bei fehlendem Zuwachspatz zu vermeiden. Wollen Sie für die Betriebssysteme der Gäste Zuwachsplatten verwenden, dann überwachen Sie den freien physischen Speicherplatz streng.
- ▶ Sie können für die Datenplatten produktiver VMs Zuwachsplatten verwenden, um den vorhandenen physischen Speicherplatz optimal auszunutzen und bei späteren Platzerweiterungen keine



Gäste anpassen zu müssen. Legen Sie aber zur Vorsicht Platzhalter auf dem Host-Datenträger an, die sich schnell löschen lassen, um im Notfall letzte Reserven freizumachen. Überwachen Sie unbedingt den freien Speicher.



Im Zweifelsfalle, bei Performanceproblemen oder bei üppig vorhandenem physischen Speicherplatz, erstellen Sie am besten ausschließlich reservierte Platten für produktive Maschinen, beim ESX Server haben Sie keine andere Option.

- Wenn Sie in produktiven Umgebungen unter VMware die virtuellen Platten als 2-GB-Segmente erstellen wollen, dann legen Sie für jede Platte einen eigenen Ordner an, damit alle Segmente übersichtlich an einem eigenen Ort liegen. Für Sicherungs- oder Kopiervorgänge sind Segmente teilweise handlicher, sollten Sie unter VMware einmal den Controllertyp ändern müssen, dann ebenfalls.

## 3.3 Schreibzugriffe direkt ausführen oder in Redo-Logs bzw. Differenzplatten puffern

Bei der Art der Behandlung von Schreibzugriffen auf eine virtuelle Platte spielen VMs einen ihrer größten Vorteile aus, nämlich die Möglichkeit, Veränderungen an den Daten wieder verwerfen zu können. Im Normalfall werden veränderte Sektoren sofort in die Behälterdatei geschrieben, damit ist jede Änderung an den Daten oder am Gastssystem unwiderruflich. Dieses Verhalten ist Ihnen von physischen Platten nicht anders bekannt. Im Gegensatz dazu macht es eine virtuelle Platte möglich, Schreibzugriffe abzufangen und in eigens dafür vorgesehenen Zwischenspeicher, die so genannten *Redo-Logs* oder *Undo-Logs* umzuleiten.

**Redo-Logs sind zusätzliche Behälterdateien**

Diese Logs sind nichts weiter als zusätzliche Behälterdateien, in die der Virtualisierer veränderte Sektoren schreibt, anstelle sie auf die virtuelle Platte zu übertragen. Dadurch bleibt der Inhalt der zugrunde liegenden virtuellen Platte unangetastet. Änderungen können Sie später jederzeit verwerfen oder erst nachträglich auf die virtuelle Platte übertragen. Dieses Verhalten steht in engem Zusammenhang zu den *Snapshots* und *linked Clones* von VMware, die ich in *Teil 3, Kapitel 4, „Die Snapshot- und Clone-Funktion der VMware-Produkte“* ausführlich beschreibe. Auch die so genannten Rückgängig-Datenträger der Microsoft-Produkte basieren auf dem gleichen Prinzip, ihre Verwendung wird im Praxis-Workshop in *Teil 2, Kapitel 7, „Eine virtuelle Pilotumgebung als Testfeld für produktive Einsätze“*, ausführlich vorgestellt.

### 3.3.1 Redo-Logs unter VMware einschalten

Um ein Redo-Log für eine virtuelle Platte einzuschalten, haben Sie unter VMware drei Möglichkeiten:

- ▶ *Snapshots* – Sobald Sie in einem Gast einen Snapshot setzen, entstehen im Verzeichnis der VM zu jeder Platte Dateien mit dem Anhang *-000001.vmdk*, z.B. *meine\_platte-000001.vmdk*. Diese Dateien sind die Redo-Logs. Bei der VMware Workstation entstehen bei jedem Snapshot weitere Logs mit fortlaufenden Nummern, der VMware Server unterstützt dagegen offiziell nur einen Snapshot und damit nur ein Redo-Log. Wege, das zu umgehen, finden Sie in *Teil 3, Kapitel 4*, „Die Snapshot- und Clone-Funktion der VMware-Produkte“.
- ▶ *Modus nonpersistent* – Unter VM/SETTINGS/HARDWARE können Sie jede virtuelle Platte über die Schaltfläche ADVANCED in den Modus *Independent nonpersistent* bringen. Beim Start der VM entstehen dann Redo-Logs, die auch vom Namen her sofort als solche zu erkennen sind, z.B. *meine\_platte.vmdk.REDO\_a01736*. Im Unterschied zu den Snapshots werden diese Redo-Logs beim Abschalten der VM automatisch gelöscht, wodurch Änderungen immer verloren gehen. Damit können Sie eine Platte jedes Mal automatisch auf ihren Grundzustand zurücksetzen lassen.
- ▶ *Modus undoable* – Durch Manipulation der Konfigurationsdatei *\*.vmx* einer VM können Sie die virtuelle Platte auf den Modus *undoable* setzen. Dabei entstehen für die entsprechende Platte ebenfalls Redo-Logs im Format *meine\_platte.vmdk.REDO\_xyyyyy*. Im Gegensatz zum Modus *Independent nonpersistent* bleiben diese Logs erhalten, wenn Sie die VM abschalten. Sie entscheiden selbst, was mit den Änderungen passiert. VMware unterstützt dieses Vorgehen offiziell nicht mehr, man kann es aber für verschiedene Erweiterungen verwenden. Beispielsweise existiert ein Tool, um unter dem VMware Player mehrere Snapshots zu erzeugen (siehe ebenfalls *Teil 3, Kapitel 4*).

### 3.3.2 Rückgängig-Datenträger und Differenzplatten unter Microsoft aktivieren

Unter Microsoft existieren zwei Möglichkeiten, virtuelle Platten vor direkten Schreibzugriffen zu schützen:

- ▶ Sobald Sie in den Eigenschaften einer VM unter FESTPLATTEN den Haken an RÜCKGÄNGIG-DATENTRÄGER AKTIVIEREN setzen, entstehen beim Start der VM für jede virtuelle Platte Undo-Logs. Sie erkennen die Dateien am Vorsatz *VirtualPCUndo*, dem durch eine ID ergänzten Plattenamen und an der Erweiterung *\*.vud*, z.B.: *VirtualPCUndo\_meine\_platte\_0\_0\_0\_17522807032006.vud*. Auch unter Microsoft Virtual Server beginnen die Logs mit *VirtualPCUndo*.

- Microsoft unterstützt eine weitere Methode, um Änderungen an einer virtuellen Festplatte zu verhindern, die so genannten *Differenzplatten*. Sie funktionieren im Prinzip wie Redo-Logs und setzen auf eine zugrunde liegende virtuelle Platte auf. Vom Umgang her sind Differenzplatten allerdings eher virtuellen Platten gleichzustellen, da sie manuell in einen Gast eingebunden werden und da kein Automatismus zur Verwaltung existiert.

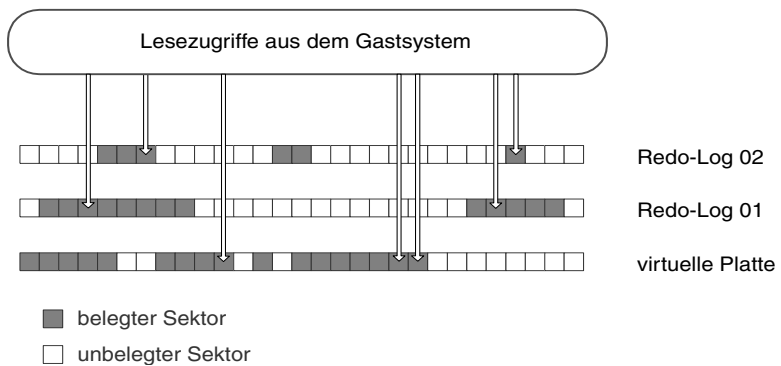
### 3.3.3 Wie funktionieren Redo-Logs und Differenzplatten konkret?

**Schreibzugriffe werden ins Redo-Log umgeleitet**

Sobald eine virtuelle Platte ein aktives Redo-Log besitzt, z.B. nach einem Snapshot (VMware) oder bei aktivem Rückgängig-Datenträger (Microsoft), werden alle veränderten Sektoren nur noch in diesem Redo-Log abgelegt. Lesezugriffe kombinieren das Redo-Log und die zugrunde liegende virtuelle Platte (Abbildung 3.6).

Zuerst schaut der Virtualisierer im Redo-Log nach, ob er einen angeforderten Sektor dort findet. Wenn ja, dann liefert er diesen Sektor auf die Anfrage des Gastes zurück. Sollte sich der Sektor nicht im Redo-Log befinden, wird er aus der virtuellen Platte gelesen. Sind mehrere Redo-Logs kaskadiert, z.B. durch aufeinander folgende Snapshots der VMware Workstation, dann muss der Virtualisierer von oben nach unten überprüfen, ob der Sektor irgendwo vorhanden ist. Ein Lesezugriff liefert immer den Sektor im letztmöglichen Redo-Log, also den aktuellsten Stand. Das Gleiche gilt für Microsofts Differenzplatten.

Abbildung 3.6:  
Beim Lesen von Sektoren werden alle Redo-Logs mit der virtuellen Platte kombiniert, geschrieben wird immer ins aktuellste Log



#### Wie groß kann ein Redo-Log werden?

Wird ein Sektor der virtuellen Platte niemals verändert, dann ist er im Redo-Log auch nicht vorhanden, weil Redo-Logs immer wie Zuwachsplatten funktionieren. Auch wenn es sich um eine reservierte Platte handelt, beginnt das Redo-Log mit einer minimalen Größe. Erst wenn der Gast einen Sektor beschreibt, wird dieser im Redo-Log belegt. Wenn das Gastsystem einen bestimmten Sektor der virtuellen Platte mehrfach beschreibt, dann wird er im Redo-Log immer wieder geän-

dert und nicht jedes Mal neu angehängt. Das bedeutet, ein Redo-Log kann niemals größer werden als die zugrunde liegende virtuelle Platte. Ein extremes Beispiel verdeutlicht die Funktion:

Sobald Sie unter VMware einen Snapshot setzen bzw. bei Microsoft die Rückgängig-Datenträger aktivieren, schalten Sie damit ein Redo-Log für jede virtuelle Platte der VM ein. Wenn Sie jetzt im Gast alle Sektoren einer Platte verändern, etwa durch große Kopieraktionen, dann ist am Ende jeder Sektor der virtuellen Platte einmal im zugehörigen Redo-Log enthalten. Lesezugriffe liefern dadurch nur noch Sektoren aus dem Redo-Log zurück, die zugrunde liegende virtuelle Platte wird überhaupt nicht mehr gelesen und auch nicht beschrieben. So praxisfremd, wie sich dieses Beispiel anhört, ist es nicht. Wenn Sie beispielsweise ein Betriebssystem auf einer leeren virtuellen Platte bei aktivem Redo-Log installieren, dann landet die gesamte Installation im Log. Das passiert z.B., sobald Sie in einer neuen VM vor der Installation einen Snapshot setzen. Dadurch wird kein einziger Sektor in die eigentliche virtuelle Platte geschrieben. Handelt es sich um eine Zuwachsplatte, ist das Redo-Log am Ende wesentlich größer als die Behälterdatei selbst.

**Ein Redo-Log kann maximal so groß wie die virtuelle Platte werden**

Ein weiteres Beispiel ist das Durchführen einer Defragmentierung im Gastsystem, wodurch das Redo-Log stark anwachsen kann, da der Sortiervorgang der Dateiblöcke viele Sektoren auf der virtuellen Platte neu schreibt.

## 3.4 Die Dateien und Konfigurationseinträge der virtuellen Platten einer VM

Nachdem Sie alle theoretischen Aspekte virtueller Platten und deren Behälterdateien kennen gelernt haben, wenden wir uns der praktischen Seite zu – wie sehen die Dateien der virtuellen Platten aus, und wo finden Sie diese? Standardmäßig werden virtuelle Platten im Verzeichnis der zugehörigen VM angelegt. Virtuelle Platten bestehen entweder aus einer einzigen Datei oder einem ganzen Satz zusammengehöriger Dateien, je nach Typ.

### 3.4.1 Dateien virtueller Platten unter VMware

Unter VMware haben virtuelle Platten die Endung *\*.vmdk*. Die Behälterdateien liegen im Verzeichnis der virtuellen Maschine, lassen sich aber genauso in jedem anderen beliebigen Pfad unterbringen. Für segmentierte Dateien kommen wegen der besseren Übersicht Unterordner wie *sys*, oder *data01* in Frage, um die vielen zugehörigen Segmente an einem Ort zu haben.

#### Sinnvolle Benennung der virtuellen Platten unter VMware

Wenn Sie keinen anderen Namen vergeben, dann benennt der VMware Wizard beim Erstellen einer VM die Platten nach dem gewählten Betriebssystem, z.B. *Windows 2000 Professional.vmdk*. Bei dieser Benennung verlieren Sie allerdings schnell die Übersicht darüber, was sich in einer virtuellen Platte konkret befindet – ist das jetzt der Testserver mit Windows 2003 oder die Systemplatte mit der produktiven Oracle-Datenbank? In den Workshops habe ich aus diesem Grunde bereits eine andere Benennung empfohlen. Sie können den Namen der VM, etwa *testserver01*, mit einem Kürzel für die Verwendung der Platte ergänzen, z.B. *sys* für System und *data01* für die Daten. Im Beispiel ergibt das *testserver01\_sys.vmdk*, bzw. *testserver01\_data01.vmdk*.



Der VMware Wizard für eine neue VM erfragt den Namen der Platte nur im Custom-Modus, im Modus Typical verwendet er immer die Bezeichnung des gewählten Betriebssystems. Bei der neuen Erstellung einer virtuellen Platte über VM/SETTINGS/HARDWARE/ADD können Sie dagegen immer den Namen ändern oder auch einen anderen Ordner wählen.

#### Behälterdateien der virtuellen Platten unter VMware

Welche Dateien zu einer virtuellen Festplatte gehören, hängt davon ab, ob sie monolithisch oder in Segmenten vorliegt bzw. ob Redo-Logs vorhanden sind. Viele Plattentypen verfügen, neben den Behälterdateien mit dem Inhalt der Sektoren, zusätzlich über eine Kopfdatei (*Headerfile*), die im Textformat wichtige Parameter der virtuellen Platten enthält, z.B. die CHS-Geometrie und den Controllertyp. Ich komme an einem praktischen Beispiel weiter unten noch darauf zurück, siehe Abschnitt 3.8.7, „Umwandeln einer virtuellen IDE-Platte in eine SCSI-Platte unter VMware“.

##### **Monolithische Zuwachsplatte**

Eine *monolithische Zuwachsplatte* besteht nur aus einer einzigen Datei, die mit dem Platzbedarf des Gastes mitwächst. Die Parameter der Platte befinden sich nicht in einer separaten Kopfdatei, sondern sind direkt am Anfang in der Behälterdatei untergebracht:

```
meine_monodisk.vmdk
```

##### **Monolithische reservierte Platte**

Eine *monolithische reservierte Platte* besteht aus einer Kopfdatei im Textformat und einer einzelnen Behälterdatei in voller reservierter Größe der virtuellen Platte. Die Kopfdatei trägt den Namen der Platte, die Behälterdatei ist mit der Erweiterung *-flat* ergänzt:

```
meine_monodisk.vmdk
meine_monodisk-flat.vmdk
```

Eine *segmentierte Platte* verfügt ebenfalls über eine Kopfdatei, wobei es keine Rolle spielt, ob es sich um eine Zuwachsplatte oder um eine reservierte Platte handelt. Die eigentlichen Daten sind in 2 GB großen durchnummerierten Segmenten untergebracht. Auch bei Zuwachsplatten werden alle Segmente bereits angelegt, allerdings nur in minimaler Größe. Bei reservierten Platten ist jedes Segment dagegen sofort 2 GB groß. Eine 6 GB große Platte besteht beispielsweise aus fünf Dateien, wobei die Kopfdatei keine Nummer hat. Zuwachsplatten tragen vor der Segmentnummer ein *-s*, vorreservierte Platten ein *-f*.

#### Segmentierte Platte

```
meine_splitdisk.vmdk
meine_splitdisk-s001.vmdk
meine_splitdisk-s002.vmdk
meine_splitdisk-s003.vmdk
meine_splitdisk-s004.vmdk
```

Übrigens enthält im Beispiel das vierte Segment mit dem Namen `meine_splitdisk-s004.vmdk` einen kleinen Übertrag der Gesamtkapazität, da neben den Sektordaten auch einige Verwaltungsinformationen in den Dateien enthalten sind, eigentlich würden drei Segmente für 6 GB genügen.



#### Lock-Datei für die Dateisperre bei laufendem Gast unter VMware

Sobald die Platte von einem Gast verwendet wird, erstellt VMware eine Lock-Datei (*\*.lck*). Damit verhindert VMware die gleichzeitige Benutzung einer virtuellen Platte von verschiedenen VMs. Sollten Sie das für Experimente doch einmal tun wollen, dann lässt sich mit dem Parameter `disk.locking = "false"` in der *vmx*-Datei die Sperre unterdrücken (siehe Cluster-Workshop in Teil 2, Kapitel 8, „Cluster mit VMs und einem iSCSI Target als externem Speicher“). Für jede virtuelle Platten existiert jeweils eine Lock-Datei:

```
meine_monodisk.lck
meine_splitdisk.lck
```

Nach Abstürzen kann manchmal die Lock-Datei erhalten bleiben, ohne dass ein Gast die Platte verwendet. In diesem Falle lässt sich der Gast nicht wieder starten, Sie müssen erst die Lock-Datei manuell löschen.



### Redo-Logs einer virtuellen Platte unter VMware

**undoable oder nonpersistent**

Zusätzlich existieren gegebenenfalls Redo-Logs zu jeder Platte im Modus *undoable* oder *nonpersistent*. Die angehängte Nummer REDO\_xxxxxx vergibt VMware zufällig, z.B.:

```
meine_monodisk.vmdk.REDO_a01680
```

bzw.

```
meine_splitdisk.vmdk.REDO_a02696
meine_splitdisk-s001.vmdk.REDO_a02696
meine_splitdisk-s002.vmdk.REDO_a02696
meine_splitdisk-s003.vmdk.REDO_a02696
meine_splitdisk-s004.vmdk.REDO_a02696
```

**Snapshot**

Bei einem Snapshot der aktuellen Versionen VMware Workstation 5 oder VMware Server sehen die Redo-Logs etwas anders aus, die typische Erweiterung REDO fehlt. Stattdessen wird eine Nummer direkt an den Namen der Platte angehängt, anhand dieser Nummer -xxxxxx ordnet VMware die Redo-Logs dem entsprechenden Snapshot zu:

```
meine_monodisk-000001.vmdk
```

bzw.

```
meine_splitdisk-000001.vmdk
meine_splitdisk-000001-s001.vmdk
meine_splitdisk-000001-s002.vmdk
meine_splitdisk-000001-s003.vmdk
meine_splitdisk-000001-s004.vmdk
```



Für jedes Redo-Log existiert bei laufender VM zusätzlich eine Lock-Datei \*.lck.

### 3.4.2 Die Parameter der virtuellen Platten in der Konfigurationsdatei (\*.vmx) unter VMware

In der Konfigurationsdatei \*.vmx einer VM werden die Platten durch verschiedene Einträge beschrieben. Beim Hinzufügen einer Platte erstellt VMware die Einträge automatisch, Sie müssen in der Datei eigentlich nie etwas verändern. Nur für bestimmte Erweiterungen, z.B. Wechsel des virtuellen Controllertyps oder Hinzufügen mehrerer Snapshots beim VMware Server, sollten Sie direkt in der Datei editieren. Nur im VMware Player erreichen Sie die meisten Funktionen ausschließlich durch direktes Editieren.

## Controllermodell und angeschlossene virtuelle Platten unter VMware

Zuerst muss der Controller für die Platten eingeschaltet sein, im Beispiel der erste SCSI-Controller. Jede VM kann vier virtuelle SCSI-Controller (Nummer 0–3) verwenden, standardmäßig wird nur der Controller 0 benutzt. Ist eine der folgenden Zeilen nicht vorhanden oder hat den Wert `False`, dann steht der entsprechende Controller im Gast nicht zur Verfügung:

```
scsi0.present = "TRUE" | "FALSE"
scsi1.present = "TRUE" | "FALSE"
scsi2.present = "TRUE" | "FALSE"
scsi3.present = "TRUE" | "FALSE"
```

Welcher SCSI-Controller jeweils emuliert wird, bestimmt dieser Parameter, fehlt die Zeile, dann emuliert VMware immer `BusLogic`. Dieser Eintrag kann nach dem Erstellen einer VM nur noch manuell in der Konfigurationsdatei geändert werden:

```
scsi0.virtualDev = "buslogic" | "lsilogic"
```

Für jede virtuelle Platte existiert ein eigener Eintrag, hier sind am ersten SCSI-Controller mit der Nummer 0 zwei Platten mit der SCSI-ID 0 und mit der SCSI-ID 1 angeschlossen:

```
scsi0:0.present = "TRUE" | "FALSE"
scsi0:0.fileName = "meine_monodisk.vmdk"
scsi0:1.present = "TRUE" | "FALSE"
scsi0:1.fileName = "meine_splitdisk.vmdk"
```

Jede VM verfügt über zwei IDE-Kanäle, an die jeweils zwei Platten angeschlossen werden können. Der IDE-Controller wird, im Gegensatz zu den SCSI-Controllern, nicht mit einem separaten Eintrag eingeschaltet. Zwei IDE-Platten am ersten IDE-Kanal (Nummer 0) würden folgende Einträge in der Konfigurationsdatei hinterlassen:

```
ide0:0.present = "TRUE" | "FALSE"
ide0:0.fileName = "meine_monodisk.vmdk"
ide0:1.present = "TRUE" | "FALSE"
ide0:1.fileName = "meine_splitdisk.vmdk"
```

## Redo-Logs der virtuellen Platten unter VMware aktivieren

Weiterhin ist in der Konfiguration ersichtlich, ob die virtuelle Platte ein Redo-Log verwendet, diese Zeile kann in der Konfigurationsdatei auch fehlen:

```
scsi0:0.mode = "independent-nonpersistent"
scsi0:1.mode = "independent-persistent"
ide0:0.mode = "persistent"
ide1:0.mode = "undoable"
```



Folgende Modi stehen zur Verfügung, die meisten Funktionen sind nur für Snapshots relevant, die ausführlich in *Teil 3, Kapitel 4, „Die Snapshot- und Clone-Funktion der VMware-Produkte“*, behandelt werden:

- ▶ *persistent* – Das ist der Standardmodus jeder Platte, fehlt der Eintrag in der Konfigurationsdatei, gilt dieser Wert. Eigentlich besagt der Parameter, dass die Platte immer direkt beschrieben wird, aber mit dem neuen Format der Snapshots seit Workstation 5 oder VMware Server stimmt das nicht mehr. Auch wenn es widersprüchlich klingt – nur eine Platte im Modus *persistent* kann Snapshots haben.
- ▶ *independent-persistent* – Eine Platte in diesem Modus wird immer direkt beschrieben, auch wenn die VM mit einem Snapshot läuft. Sie können damit Platten betreiben, deren Änderungen immer permanent bleiben und bei einem REVERT nicht verworfen werden, z.B. die Arbeitsplatte mit wichtigen Daten. Die Einstellung dazu finden Sie unter VM/SETTINGS/HARDWARE bei einer virtuellen Platte unter ADVANCED.
- ▶ *independent-nonpersistent* – Eine Platte in diesem Modus hat immer ein Redo-Log, ob die VM mit einem Snapshot läuft oder nicht. Dieses Redo-Log wird beim Abschalten der VM immer automatisch verworfen, wodurch alle Änderungen verloren gehen.
- ▶ *undoable* – Dieser Modus wird von VMware offiziell eigentlich nur noch für so genannte *legacy*-VMs aus älteren Versionen unterstützt und lässt sich nur manuell einschalten. Eine Platte in diesem Modus hat ebenfalls immer ein Redo-Log, das aber auch nach dem Ausschalten erhalten bleibt. Sobald Sie eine Platte manuell in diesen Modus bringen, funktionieren die regulären Snapshots der aktuellen VMware-Versionen nicht mehr, interessant kann dieser Modus beim VMware Player sein, um mehrere Snapshots oder linked Clones zu erzeugen.

Wenn sich eine Platte im Modus *independent-nonpersistent* oder *undoable* befindet, wird in der Konfigurationsdatei noch das zugehörige Redo-Log angegeben, z.B.:

```
scsi0:0.redo = ".\meine_vplatte.vmdk.REDO_a01680"
```



Für Kenner früherer VMware-Versionen dürfte interessant sein, dass nur Platten im Modus *undoable* oder *independent-nonpersistent* noch Redo-Logs im herkömmlichen Format verwenden. Im Falle eines Snapshots unter VMware Server oder Workstation 5 wird das Redo-Log nicht mehr mit dem Parameter *.redo* in der Konfigurationsdatei angegeben, sondern bei jedem Snapshot automatisch direkt als Plattenname eingetragen, z.B.:

```
ide0:0.fileName = "meine_vplatte-000001.vmdk"
```

### 3.4.3 Dateien und Konfiguration der virtuellen Platten unter Microsoft

Virtuelle Platten unter Microsoft haben die Endung \*.vhd. Es werden immer monolithische Platten erstellt:

meine\_vplatte.vhd

Nur wenn die virtuelle Platte auf einer FAT-Partition liegt, wird die Behälterdatei automatisch beim Anwachsen in Segmente aufgeteilt.



Zu jeder virtuellen Platte kann zusätzlich ein Undo-Log existieren, sobald die Rückgängig-Datenträger aktiviert sind, z.B.:

VirtualPCUndo\_meine\_vplatte\_0\_0\_0\_17522807032006.vud

Die Manipulationsmöglichkeiten sind unter Microsoft geringer als unter VMware. In der praktischen Arbeit mit den virtuellen Platten werden diese auch nicht benötigt. Es ist ganz einfach möglich, eine virtuelle IDE-Platte ohne jede Umstellung an einem virtuellen SCSI-Controller zu betreiben und umgekehrt. Voraussetzung ist natürlich, dass die richtigen Treiber im Gast installiert sind. Weiterhin können Sie unter Microsoft keine unterschiedlichen Formate der Behälterdateien wählen, wie segmentiert oder monolithisch, mit Kopfdatei oder ohne Kopfdatei, wodurch keine Umwandlungen möglich bzw. notwendig sind.

Wenn Sie trotzdem einen Blick auf die interne Konfiguration werfen wollen, finden Sie diese in den Konfigurationsdateien der Gäste, z.B. *meine\_vm.vmc*, im XML-Format:

- ▶ In der Sektion `<scsi_adapter>` sind alle vier möglichen SCSI-Controller jeweils unter `<scsi_controller id="x">` bereits eingetragen.
- ▶ Der Parameter `<controller_count>` bestimmt, wie viele SCSI-Controller aktiv sind.
- ▶ Die IDE-Controller befinden sich in der Sektion `<ide_adapter>`.
- ▶ Unter `<pathname>` finden Sie den Pfad zur jeweils verwendeten virtuellen Platte an den Controllern. Die Namen der Undo-Logs werden nicht in der Konfigurationsdatei vermerkt.

## 3.5 Physische Datenträger in einem Gast direkt verwenden – Raw Device Mapping

Als besondere Form des Datenträgerzugriffs können Sie einen Gast direkt auf eine physische Platte zugreifen lassen. Dabei leitet der Virtualisierungslayer Zugriffe nicht mehr in eine Behälterdatei um, sondern die VM schreibt und liest vom physischen Datenträger.



Wenn Sie eine physische Platte in eine VM einbinden, wird trotzdem eine virtuelle Platte erstellt. Diese besteht aber nur aus einer Kopffdatei, welche die Parameter und die Verknüpfung zu der physischen Platte enthält. Physikalische Platten können in einer VM auch mit einem Redo-Log vor Schreibzugriffen geschützt werden.

### 3.5.1 Physische Platten unter VMware einbinden

Unter VMware wählen Sie beim Erstellen einer neuen Platte über VM/SETTINGS/HARDWARE/ADD/HARD DISK den Punkt USE A PHYSICAL DISK. Dabei stehen zwei Optionen zu Verfügung:

**Gesamte Platte  
oder nur eine  
Partition**

- *Use entire disk* – die gesamte Platte mit allen vorhandenen Partitionen wird im Gast verwendet – sehr gefährlich!
- *Use individual partitions* – der Gast hat nur auf einige ausgewählte Partitionen Zugriff. Damit kann ein Bereich der Festplatte ausschließlich für die VM reserviert werden, und die Gefahr ist geringer, das Host-System zu kompromittieren.



Unter VMware können Sie für physische Platten auch den Modus independent-nonpersistent einstellen, um Änderungen in Redo-Logs zu puffern. Damit lässt sich beispielsweise erst einmal testen, ob der Gast die richtige Partition verwendet, bevor Sie ihn auf die physische Platte zugreifen lassen. Sobald eine VM Zugriff auf eine physische Platte hat, können Sie keinen Snapshot mehr setzen!

### 3.5.2 SCSI-Geräte, wie Streamer, in einem VMware-Gast verwenden

Neben physischen Platten kann VMware auch auf physische SCSI-Geräte zugreifen, etwa auf einen Streamer, um z.B. Datensicherungssoftware in einer VM zu verwenden. Wählen Sie dazu unter VM/SETTINGS/HARDWARE/ADD ein GENERIC SCSI DEVICE.

Sollte der Zugriff nicht funktionieren oder ein Gerät steht gar nicht zur Auswahl, dann müssen Sie direkt in der Konfigurationsdatei editieren. Folgendermaßen binden Sie einen Streamer, der im Host physisch am Controller 0 mit der SCSI-ID 3 angeschlossen ist, in Ihre VM an den virtuellen Controller 1 mit der SCSI-ID 5:

```
Scsil:5.present = "true"
scsil:5.deviceType = "scsi-passthru"
scsil:5.fileName = "scsi0:3"
```

### **3.5.3 Physische Platten unter Microsoft einbinden**

Unter Microsoft erstellen Sie mit dem Assistenten eine neue virtuelle Platte und wählen als Typ **VERKNÜPFTE VIRTUELLE FESTPLATTE**. Sie können nur komplette physische Festplatten einbinden, die Beschränkung auf einzelne Partitionen ist nicht möglich.

#### **Microsoft Virtual PC 2004**

Unter Microsoft Virtual PC kann eine verknüpfte Festplatte wie jede andere virtuelle Platte einer VM zugewiesen werden. Den beim Erstellen standardmäßig gesetzten Schreibschutz, sichtbar am ausgegrauten Kästchen im Dialogfenster, können Sie allerdings nur dann aufheben, wenn keine der Partitionen dieser physischen Platte vom Host-System verwendet wird, das bedeutet, wenn kein Laufwerksbuchstabe zugeordnet ist. Der zusätzliche Schutz einer physischen Platte mittels aktiviertem Rückgängig-Datenträger ist möglich.

#### **Microsoft Virtual Server 2005 R2**

Unter Microsoft Virtual Server ist die Verwendung physischer Platten stark eingeschränkt und dient ausschließlich dazu, eine physische Platte in eine virtuelle Platte zu überführen, was Sie für einen P2V-Vorgang verwenden können, indem Sie den Datenträger der Quelle in den Host einbauen.

Eine mit einer physischen Festplatte verknüpfte virtuelle Platte kann unter Virtual Server keiner VM zugewiesen werden.



Über **VIRTUELLE FESTPLATTEN/ÜBERPRÜFEN/VIRTUELLE FESTPLATTE KONVERTIEREN** können Sie die verknüpfte physische Festplatte in eine virtuelle Platte kopieren. Zum Kopieren sind folgende Voraussetzungen zu erfüllen:

- ▶ Wählen Sie als Ziel einen anderen physischen Datenträger als den zu übernehmenden.
- ▶ Wollen Sie von der übernommenen virtuellen Festplatte später booten, müssen Sie vorher dafür sorgen, dass der richtige Controllertreiber im Quellsystem installiert ist.

### 3.5.4 Gefahren bei der Verwendung physischer Platten in einer VM

Physische Platten in einen Gast einzubinden ist nicht ganz ungefährlich. VMs und Host dürfen niemals gemeinsam auf den gleichen Datenträger zugreifen. Keinesfalls dürfen Sie die physische Systemplatte des Hosts in eine VM einbinden, obwohl sich das auf den ersten Blick zum Datenaustausch eignen würde. Warum funktioniert das nicht?

#### Gegenseitiges Überschreiben von Sektoren

Betriebssysteme, wie Windows oder Linux, sind nicht darauf ausgelegt, gemeinsam von verschiedenen Rechnern auf dieselbe Festplatte zuzugreifen, sie gehen davon aus, einen Datenträger immer zur alleinigen Verfügung zu haben. Mit dieser Voraussetzung übertragen die Systeme Daten oftmals nicht sofort auf die Platte, puffern diese in Schreibcaches im RAM. Auch die *FAT* (*File Allocation Table*, *Dateizuordnungstabelle*) wird im Hauptspeicher vorgehalten, damit sich nicht jedes Mal die Schreib-/Leseköpfe bewegen müssen, um das Verzeichnis der Platte zu lesen. In der FAT ist vermerkt, welche Sektoren noch frei sind und welche bereits von Dateien belegt wurden.

Würden mehrere Systeme gleichzeitig auf denselben Datenträger zugreifen, wüsste also das eine nicht, was das andere gerade tut. Vermeintlich freie Sektoren, die in der FAT des einen Systems noch nicht als belegt vermerkt sind, könnte das andere System aber bereits mit Daten beschrieben haben. Wenn *System A* Daten schreibt, müsste *System B* eigentlich darüber informiert werden, welche Sektoren jetzt belegt sind, sonst stimmt der zwischengespeicherte Stand der FAT im RAM von *System B* nicht mehr mit der Realität überein. Dieser Austausch von Informationen findet aber nicht statt. Ein gemeinsamer Schreibzugriff würde früher oder später zum Datenchaos führen, da beide Systeme sich gegenseitig vermeintlich freie Sektoren überschreiben.

In der physischen Welt ist es kaum möglich, die gleiche Festplatte in zwei Rechner einzubauen. Bei virtuellen Maschinen kann aber jeder Mann mit ein paar Mausklicks konfigurieren, dass eine VM die physische Systemplatte des Hosts mitbenutzt, was zu schweren Fehlern führen kann.

### 3.5.5 Dual-Boot-Konfigurationen lassen Systeme wahlweise auf der Hardware oder in einer VM laufen

#### Linux direkt auf Hardware oder unter Windows im Gast

Ein möglicher Einsatzzweck für die Benutzung physischer Platten in einem Gast sind Dual-Boot-Konfigurationen, bei denen z.B. eine Linux-Installation wechselseitig entweder nativ auf der Hardware des Hosts oder in einer virtuellen Maschine unter Windows laufen kann. Das Vorgehen bietet sich für den Fall an, dass Sie Linux neben

Ihrer normalen Arbeit unter Windows in einer VM testen wollen und das Linux-System hin und wieder Zugriff auf die physische Hardware benötigt, etwa wegen einer FireWire-Karte zur Videobearbeitung oder einfach zum Performancevergleich.

Sie können in diesem Beispiel Linux zuerst auf Ihrem physischen Rechner in einer separaten Partition installieren und testen. Sobald Sie wieder in der gewohnten Windows-Umgebung arbeiten wollen, starten Sie den Host unter Windows und binden dort die physische Linux-Partition in eine neue VM ein. Jetzt können Sie die Linux-Installation nebenbei in einer VM betreiben und weiterhin ausprobieren, ohne auf Ihre Windows-Umgebung verzichten zu müssen. Sie können Linux auch jederzeit wieder direkt auf der Hardware ausführen, indem Sie den Host neu booten. Voraussetzung dafür ist ein Bootmanager auf dem physischen PC, mit dem Sie zwischen Ihren Betriebssystemen wählen können. Weiterhin müssen im Dual-Boot-System, das auf der Hardware oder in einer VM laufen soll, die richtigen Festplattencontrollertreiber für die physische Hardware und für die virtuelle Hardware gleichermaßen installiert sein, am einfachsten gelingt das mit IDE-Platten.

Achten Sie darauf, dass Sie der VM nur den Zugriff auf die physische Linux-Partition gestatten, um einen Zugriff auf die Partitionen des Host-Systems zu verhindern. Gegebenenfalls müssen zusätzlich die Einträge im Boot-Menü, beispielsweise von GRUB oder Lilo, angepasst werden, weil die Festplatten in der VM anders nummeriert sein können, als wenn das System direkt von der Hardware startet.



Im Extremfall könnten Sie unter Linux (wenn es von Hardware gestartet ist) dann wiederum den Windows-Host in einer VM laufen lassen. Windows XP und 2003 sind für Dual-Boot-Installationen allerdings weniger geeignet, da bei jedem Wechseln zwischen Hardware und VM immer wieder neue Hardware erkannt wird und damit ständige Neuregistrierungen notwendig sind. Das ist schade, weil durch die Verwendung von Hardware-Profilen in Windows alle Bedingungen zum wechselseitigen Booten auf Hardware und in einer VM gegeben wären. Einzige Ausnahme sind Volumenlizenzen mit den dazugehörigen Datenträgern ohne Registrierungszwang, die aber nur Behörden oder großen Firmen zur Verfügung stehen.

**Neue Windows-Registrierung notwendig**

## 3.6 Fragmentierte Dateien auf dem Host sowie im Gast und die Auswirkungen

Eine Ursache für die schlechte Leistung eines Rechners kann ein fragmentiertes Dateisystem sein, auf physischen Computern genauso wie in virtuellen Maschinen. Vor allem beim Starten eines Betriebssystems, bei größeren Kopieraktionen oder bei Auslagerungsvorgängen, macht sich ein Leistungsabfall bemerkbar.

### Verstreute Sektoren wieder sortieren

Fragmentieren bedeutet, dass die Sektoren, die zu einer Datei gehören, nicht mehr am Stück hintereinander auf der Festplatte liegen, sondern über den gesamten Datenträger verstreut sind. Dabei wechseln sie sich mit den belegten Sektoren anderer Dateien ab, wodurch die Schreib-/Leseköpfe mehr Bewegungen ausführen müssen, um eine bestimmte Datei am Stück lesen zu können. Das kostet Performance und verlangsamt Plattenzugriffe. Fragmentierung spielt bei virtuellen Maschinen an zwei Stellen eine Rolle:

- ▶ Einmal kann das gesamte Dateisystem innerhalb einer VM fragmentiert sein, wie es auch bei physischen Rechnern üblich ist. Dagegen hilft nur ein regelmäßiger Defragmentierungslauf im Gastsystem.
- ▶ Zusätzlich können bei VMs auch die Behälterdateien der virtuellen Platten auf dem Host-Datenträger fragmentiert sein. Dagegen helfen ebenfalls Defragmentierungsläufe auf dem Host. Eine weitere Lösung ist das Anlegen reservierter virtueller Platten auf einem leeren unfragmentierten Datenträger.



Legen Sie eine reservierte virtuelle Platte auf einem bereits stark fragmentierten Datenträger an, dann hat das keinerlei positiven Effekt, da die Behälterdatei nur noch in den Lücken zwischen bereits belegten Sektoren angelegt werden kann. Damit ist der Platz zwar reserviert, aber trotzdem in Fragmenten über die gesamte Platte verteilt.

### Defragmentieren nützt nicht immer

Das Defragmentieren des Host-Datenträgers kann aber in manchen Fällen auch keinerlei positiven Effekt bringen. Je mehr virtuelle Platten auf einem physischen Datenträger liegen und je mehr in den Gästen parallel gearbeitet wird, umso öfter müssen die Schreib-/Leseköpfe ständig größere Strecken zurücklegen, da die Gäste wechselseitig auf völlig verschiedene Behälterdateien zugreifen. Sie sehen einmal mehr, dass man bei der Arbeit mit virtuellen Maschinen nicht immer pauschal auf althergebrachte Aussagen vertrauen kann, es kommt jedes Mal auf die konkrete Situation an.

Unter VMware können Sie unter VM/SETTINGS/HARDWARE bei einer virtuellen Platte mit dem Button DEFRAGMENT eine bestimmte Behälterdatei auf dem Host defragmentieren, ohne gleich einen Defragmentierungslauf über den gesamten physischen Datenträger auszuführen.



Auch die Auslagerungsdatei in den Gästen und auf dem Host kann defragmentiert sein, was sich auf die Leistung des Gesamtsystems sehr negativ auswirken kann, wenn wenig RAM vorhanden ist oder wenn viele VMs gleichzeitig laufen. Erstellen Sie deshalb für den Host immer eine Auslagerungsdatei fester Größe, wenn möglich auf einem anderen Datenträger als den für die VMs. Sie erreichen das über SYSTEMSTEUERUNG/SYSTEM/ERWEITERT mit dem Button EINSTELLUNGEN bei SYSTEMLEISTUNG. Dort können Sie unter dem Reiter ERWEITERT die Einstellungen für den VIRTUELLEN ARBEITSSPEICHER ändern. Mit gleichen Werten unter BENUTZERDEFINIERTER GRÖSSE legen Sie den Platz der Auslagerungsdatei fest. Unter einem Linux-Host verwenden Sie dazu eine separate Swap-Partition.

#### Sonderfall Auslagerungsdatei

#### Virens Scanner auf dem Host

Neben defragmentierten Dateien kann auch ein Virens Scanner auf dem Host eine virtuelle Maschine ausbremsen. Konfigurieren Sie Virens Scanner immer so, dass sie virtuelle Platten (Endung \*.vmdk bzw. \*.vhd) nicht in die Echtzeitüberwachung aufnehmen.



## 3.7 Virtuelle SCSI-Controller und die passenden Treiber in den Gästen

Nachdem wir uns bis jetzt ausschließlich mit der Sicht des Hosts auf die virtuellen Platten beschäftigt haben, kommen wir nun zur Sicht des Gastes. In einer VM spielt der emulierte Controller bei der Verwendung virtueller Platten die entscheidende Rolle. Die Virtualisierer stellen Controller vom Typ IDE oder SCSI zur Verfügung, die Sie bei der Erstellung einer VM auswählen können. VMware emuliert zwei verschiedene SCSI-Modelle von LSI Logic oder BusLogic, Microsoft emuliert einen Adaptec-Controller. Die Verwendung von IDE-Platten ist unproblematisch, weshalb ich mich hier auf die SCSI-Controller konzentriere.

#### Die Sicht des Gastes auf die virtuellen Platten





Virtuelle SCSI-Platten sind in einer virtuellen Maschine wegen des SCSI-Protokolls schneller als IDE-Platten und gestatten eine größere Anzahl angeschlossener Geräte. Sollten Sie jedoch an Treiberproblemen scheitern, ist die einfachste Lösung immer die Verwendung einer virtuellen IDE-Platte, da alle Betriebssysteme dafür Treiber mitbringen. Die Performance ist nicht optimal, genügt aber in den meisten Fällen vollauf. Läuft das Gastsystem einmal, kann es einfacher sein, den richtigen SCSI-Treiber nachträglich zu installieren und den Controller umzustellen. Beachten Sie bei der Übernahme physischer Maschinen unbedingt die Hinweise in *Teil 3, Kapitel 6, „P2V – physische Server in virtuelle Maschinen übernehmen“*, zur Installation des Standard IDE-Controllers.

In folgenden Situationen spielt der passende Treiber zum emulierten Controller eine wichtige Rolle:

- ▶ Wird der emulierte SCSI-Controller vom Betriebssystem nicht unterstützt, scheitert bereits die Installation. Dann hilft nur eine Diskette mit den Treibern oder die Installation auf eine virtuelle IDE-Platte.
- ▶ Bei einem nachträglichen Wechsel des Controllermodells kommt es häufig zu einem BlueScreen mit der Meldung *Inaccessible Boot Device* bzw. *Stop 0x0000007b*. Das Gastsystem kann beim Startvorgang ohne den passenden Treiber nicht mehr auf seinen eigenen Systemdatenträger zugreifen.
- ▶ Auch bei der Übernahme eines physischen Rechners in eine VM (P2V) oder von Gästen von anderen Produkten (V2V) müssen Sie dafür sorgen, dass der richtige Treiber im Gastsystem installiert ist, sonst läuft die neu übernommene Maschine in der VM ebenfalls in einen BlueScreen, siehe auch *Teil 3, Kapitel 6*.

#### 3.7.1 SCSI-Controllertypen und die passenden Treiber in den Gästen unter VMware

**Nicht jeder Treiber funktioniert mit jedem Gastsystem**

VMware emuliert als SCSI-Hardware wahlweise einen LSI Logic- oder einen BusLogic-Controller. Beim Erstellen einer VM müssen Sie sich entscheiden, welcher Typ verwendet wird. Eine nachträgliche Änderung ist nur durch manuelles Editieren der Konfigurationsdatei möglich. Die Wahl eines bestimmten Controllertyps hängt vom Betriebssystem in der VM ab, nicht alle kommen auf Anhieb mit ihren integrierten SCSI-Treibern zurecht. NT4 und W2k verfügen schon über funktionierende Treiber für den BusLogic-Controller, Windows 2003 dagegen nur für den LSI Logic. Windows XP funktioniert auf Anhieb gar nicht mit den emulierten SCSI-Controllern, sondern kann nur mit zusätzlichen Treibern auf virtuelle SCSI-Platten zugreifen. Beim Neuanlegen einer VM empfiehlt der Hardware-Wizard von VMware deswegen auch folgende Controller und Plattentypen:

| Betriebssystem | Controllertyp | Modell                                |
|----------------|---------------|---------------------------------------|
| NT 4           | SCSI          | BusLogic                              |
| Windows 2000   | SCSI          | BusLogic                              |
| Windows XP     | IDE           | (SCSI nur mit Zusatztreibern möglich) |
| Windows 2003   | SCSI          | LSI Logic                             |
| Windows Vista  | SCSI          | LSI Logic                             |
| Linux          | SCSI          | LSI Logic (je nach Distribution)      |

Tabelle 3.1:  
VMware empfiehlt  
beim Erstellen einer  
VM das Controller-  
modell anhand der  
von den Gastsystem-  
en mitgelieferten  
Treiber

### Der spezielle VMware Virtual SCSI Driver

Als Alternative zu den in Betriebssystemen integrierten Treibern bietet VMware für Windows 2000, XP und 2003 einen speziellen *VMware SCSI Treiber* an, der mit dem emulierten BusLogic-Adapter (nicht mit dem LSI Logic) zusammenarbeitet. Er sollte anstelle des normalen BusLogic-Treibers installiert werden, VMware verspricht damit eine Verbesserung der Performance.

Viel wichtiger ist aber, dass dieser Treiber in fast allen Betriebssystemen installiert werden kann, ohne dass die Hardware wirklich vorhanden ist. Damit können Sie beispielsweise vor einem P2V-Vorgang diesen Treiber bereits im Quellsystem vorinstallieren, was sicherstellt, dass die Ziel-VM booten kann. Den Treiber finden Sie entweder in der ISO-Datei der VMware-Tools oder in einer aktuellen Version auf der Webseite von VMware, er funktioniert für alle VMware-Produkte:

**Treiber vorinstal-  
lieren vor P2V**

[www.vmware.com/download/server/drivers\\_tools.html](http://www.vmware.com/download/server/drivers_tools.html)

### Nachträgliches Installieren des richtigen SCSI-Treibers in einem funktionierenden Gast

Wenn Sie bereits ein lauffähiges Gastsystem haben, z.B. auf einer IDE-Platte, ist der einfachste Weg zur Installation des richtigen Treibers, eine zusätzliche SCSI-Platte in die VM einzubinden. Beim Starten des Gastes erkennt das System mittels Plug&Play neue Hardware und installiert die Treiber. Sind bereits die VMware Tools im Gast eingerichtet, dann erfolgt auch die Installation des VMware SCSI-Treibers unter Windows XP automatisch. Sie können ohne Angst vor einem BlueScreen ausprobieren, ob der Zugriff auf die virtuelle SCSI-Platte funktioniert, und erst anschließend die IDE-Platte in eine SCSI-Platte umwandeln (siehe Abschnitt 3.8.7, „Umwandeln einer virtuellen IDE-Platte in eine SCSI-Platte unter VMware“).

### Vorinstallieren des richtigen SCSI-Treibers auf einem Quellsystem

Wollen Sie dagegen ein physisches System klonen, dann ist es ratsam, den richtigen Treiber bereits in der Quelle vorzuinstallieren. Ansonsten müssen Sie später in der Ziel-VM Änderungen vornehmen oder

diverse Tools bemühen (siehe Teil 3, Kapitel 6, „P2V – physische Server in virtuelle Maschinen übernehmen“). Das Vorinstallieren des richtigen Treibers ist unproblematisch, wenn Sie ein paar Hinweise beachten.

#### Windows 2000 und XP

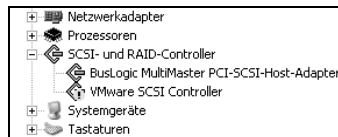
Unter Windows 2000 Workstation und Server sowie unter Windows XP kommen Sie mit dem VMware SCSI-Treiber am schnellsten zum Ziel. Richten Sie ihn folgendermaßen als neue Hardware ein, z.B. unter Windows XP:

1. Wählen Sie SYSTEMSTEUERUNG/HARDWARE.
2. Setzen Sie den Punkt bei JA, DIE HARDWARE WURDE BEREITS ANGESCHLOSSEN, obwohl das nicht stimmt.
3. Wählen Sie in der Liste ganz unten NEUE HARDWARE HINZUFÜGEN.
4. Setzen Sie den Punkt an HARDWARE MANUELL AUS EINER LISTE WÄHLEN.
5. Wählen Sie aus der Liste SCSI/RAID-CONTROLLER, und klicken Sie anschließend auf den Button DATENTRÄGER.
6. Navigieren Sie zum Speicherort des VMware-Treibers, und wählen Sie den VMWARE SCSI-CONTROLLER.
7. Windows moniert eventuell den fehlenden Logo-Test, setzen Sie die Installation trotzdem fort.
8. Nach erfolgter Installation hat der Treiber im Grätemanager ein gelbes Ausrufezeichen, da der Kontroller noch nicht existiert. Trotzdem kann das vorbereitete physische System auf eine leere virtuelle SCSI-Platte geklont werden (siehe Teil 3, Kapitel 7). Das funktioniert auch, wenn im Quellsystem ursprünglich nur IDE-Platten vorhanden waren!



Das Controllermodell der Ziel-VM muss *BusLogic* sein, nur dazu ist der VMware SCSI-Treiber kompatibel.

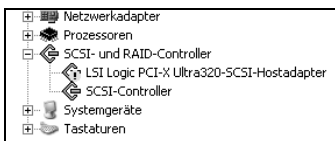
Abbildung 3.7:  
Der neu aufgetauchte BusLogic-Treiber kann im Gast in einen VMware SCSI-Controller umgewandelt werden



9. Nach dem Hochfahren der geklonten VM erscheinen zwei Einträge im Gerätemanager des Gastes, ein BusLogic-Controller und der vorinstallierte VMware SCSI-Controller, Letzterer mit einem gelben Ausrufezeichen (Abbildung 3.7). Das stört nicht die Funktion, aber der Ordnung wegen können Sie den gelb markierten VMware SCSI-Treiber deinstallieren und den übrig bleibenden BusLogic mittels rechter Maustaste und TREIBER AKTUALISIEREN in einen VMware SCSI-Controller umwandeln. Nach einem Neustart ist das System fertig.

Der Weg mit dem VMware SCSI-Treiber funktioniert auch unter Windows Server 2003, und Sie können diesen Treiber durchaus zum Vorinstallieren verwenden. Der Vollständigkeit halber sollten Sie wissen, dass Windows Server 2003 bereits einen eigenen LSI Logic-Treiber mitbringt, der von VMware empfohlen wird. Bei einer Neuinstallation von Windows 2003 in einer VM wird dieser Treiber automatisch verwendet. Zum Vorinstallieren dieses Treibers in einem vorhandenen physischen System vor einem Klonvorgang ist dagegen ein kleiner Trick notwendig:

1. Suchen Sie auf der Windows 2003-Quellmaschine in der Datei `c:\windows\inf\pnpscsi.inf` den Abschnitt `[ControlFlags]`.
2. Löschen Sie darunter die Zeile `ExcludeFromSelect = *`. Ohne diese Manipulation würde der Hardware-Assistent bei der Installation den Controller nicht anbieten, weil die entsprechende Hardware noch nicht eingebaut ist.
3. Jetzt lässt sich über SYSTEMSTEUERUNG/HARDWARE, wie oben beim VMware SCSI-Controller beschrieben, ein neuer SCSI/RAID-Controller hinzufügen. Wählen Sie mittels ALLE GERÄTE ANZEIGEN den LSI LOGIC PCI-X ULTRA320-SCSI-HOST-ADAPTER aus.
4. Der vorinstallierte Treiber erscheint nach dem Klonvorgang der Quellmaschine im Gerätemanager des Gastes mit einem gelben Ausrufezeichen, und nach dem ersten Start der geklonten Maschine taucht zusätzlich ein einfacher SCSI-CONTROLLER auf (Abbildung 3.8). Dieser kann mittels rechter Maustaste und TREIBER AKTUALISIEREN nochmals in den richtigen LSI LOGIC PCI-X ULTRA320-SCSI-HOST-ADAPTER umgewandelt werden, den gelb markierten Treiber können Sie deinstallieren. Das hat nur kosmetische Effekte, keine funktionellen.

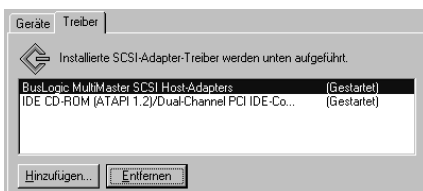


## Windows 2003

Abbildung 3.8:  
Auch unter Windows 2003 kann der SCSI-Controller nachträglich in den LSI Logic-Treiber umgewandelt werden.

Unter Windows NT 4 funktioniert der VMware SCSI-Treiber nicht. Aber dafür lässt sich der BusLogic-Treiber von der Windows NT Installations-CD verwenden:

1. Wählen Sie SYSTEMSTEUERUNG/SCSI-ADAPTER/TREIBER.
2. Installieren Sie den BUSLOGIC MULTIMASTER SCSI HOST-ADAPTER (Abbildung 3.9).



## Windows NT 4

Abbildung 3.9:  
Unter Windows NT wird der BusLogic-Treiber unterstützt

3. Achten Sie darauf, dass unter SYSTEMSTEUERUNG/GERÄTE der Dienst BUSLOGIC nicht deaktiviert ist, aktivieren Sie ihn gegebenenfalls.

Alle geklonten Systeme sollten mit den vorinstallierten Treibern starten und die virtuelle SCSI-Platte erkennen. Damit ist auch ein P2V-Vorgang auf einen virtuellen SCSI-Datenträger, z.B. beim ESX Server, kein Problem mehr, auch ohne Tools zum automatischen Anpassen des Gastsystems. Voraussetzung ist allerdings immer, dass im Gast der richtige Controllertyp passend zum Treiber in der VM eingestellt wurde.

#### Nachträgliches Umwandeln der Kontrollertypen LSI Logic und BusLogic in VMware-Gästen

Um nachträglich das Controllermodell von LSI Logic auf BusLogic oder umgekehrt zu wechseln, editieren Sie die \*.vmx-Datei der virtuellen Maschine. Dazu ist folgende Zeile mit dem Modell zu ersetzen:

```
scsi0.virtualDev = "buslogic"
```

oder

```
scsi0.virtualDev = "lsilogic"
```



Der Typ *buslogic* ist Standard und erscheint nicht immer explizit in der Konfigurationsdatei. Fehlt die Zeile, gilt *buslogic*.

Nach der Umwandlung fragt VMware beim nächsten Start, ob die virtuelle Platte dem neuen Kontrollertyp angepasst werden soll, was Sie gefahrlos mit JA bestätigen können. Dabei wird nur der Textstring *buslogic* oder *lsilogic* in der Kopfdatei oder in der Behälterdatei angepasst und nichts konvertiert oder verändert. Bei einem erneuten Wechsel passt VMware den Eintrag wieder an. Sie sollten vor der Änderung die richtigen Treiber im Gastsystem installieren, sonst startet der Gast mit einem BlueScreen.

#### 3.7.2 Der virtuelle SCSI-Controller unter Microsoft

Microsoft emuliert einen *Adaptec AIC-7870 PCI SCSI Controller* in den Gästen, für den die meisten Systeme eigene Treiber mitbringen. Zusätzlich liefert Microsoft einen beschleunigten SCSI-Treiber mit den *Virtual Machine Additions* mit. Ein SCSI-Controller erscheint dann im Gerätemanager als *VM Additions Accelerated SCSI Controller*. Sollte die Installation des optimierten Treibers nicht automatisch erfolgen, dann müssen Sie den vorhandenen SCSI-Adapter manuell über den Gerätemanager mittels TREIBER AKTUALISIEREN auf den optimierten Treiber ändern, sobald die Additions installiert sind. Das Vorgehen ist genauso unkompliziert, wie bereits für VMware beschrieben, Sie können es auch bei Microsoft nachlesen:

[support.microsoft.com/kb/840575/en-us](http://support.microsoft.com/kb/840575/en-us)

### Der SCSI Shunt-Treiber beschleunigt die Installation

Für die Neuinstallation von Windows in einem Gast mit SCSI-Platte finden Sie im Installationsverzeichnis von Virtual Server eine virtuelle Diskette mit dem Namen *SCSI Shunt Driver.vfd*. Diese enthält den optimierten Treiber, der mittels **[F6]** bei der Installation im Gast eingebunden werden kann. Die Installation läuft damit wesentlich schneller als mit den systemintegrierten SCSI-Treibern.



### Umwandeln einer virtuellen IDE-Platte in eine SCSI-Platte unter Microsoft

Unter Microsoft Virtual Server können Sie mittels **VIRTUELLE COMPUTER/KONFIGURIEREN/FESTPLATTEN** bei jeder virtuellen Platte einfach die Zuordnung von einem IDE-Kanal auf eine SCSI-ID ändern. Voraussetzung dazu ist, dass ein SCSI-Controller in der VM vorhanden ist, wenn nicht, können Sie über **VIRTUELLE COMPUTER/KONFIGURIEREN/SCSI-ADAPTER/SCSI-ADAPTER HINZUFÜGEN** einen hinzufügen.

Im Gastsystem muss der SCSI-Treiber vorher installiert sein, damit die VM danach booten kann. Am einfachsten ist es, vor dem Wechsel eine zusätzliche leere SCSI-Platte einzubinden, die VM zu starten und bei installierten *Virtual Machine Additions* im Gast den SCSI-Controller erkennen zu lassen. Wenn Sie dann testen, ob der Zugriff auf die temporär eingebundene SCSI-Platte funktioniert, können Sie sicher sein, dass der Gast nach dem Anschlusswechsel bootet.

**Virtual PC kennt keine SCSI-Platten**

## 3.8 Tools und Tricks für die Arbeit mit virtuellen Platten

Zusätzlich zum täglichen Umgang mit den virtuellen Platten existieren einige Tools und Hinweise, die Ihnen in einigen Situationen das Leben erleichtern können.

### 3.8.1 Einbinden virtueller Platten am Host mit VMware DiskMount

Um auf den Inhalt einer virtuellen Platte zuzugreifen, müssen Sie nicht immer eine VM starten. Eine virtuelle Platte kann mit dem Tool *vmware-mount.exe* direkt an einem Windows-Rechner als Laufwerksbuchstabe eingebunden werden. Damit können Sie beispielsweise aus einer Sicherungskopie Dateien extrahieren oder in einer nicht startenden VM die *boot.ini* editieren. Der VMware Server bringt das Tool bereits mit, für die Workstation finden Sie es hier:

[www.vmware.com/download/ws/drivers\\_tools.html](http://www.vmware.com/download/ws/drivers_tools.html)

**Direkter Dateizugriff vom Host**

Nach der Installation befindet sich die *vmware-mount.exe* im Verzeichnis `C:\Programme\VMware\VMware DiskMount Utility`. An der

Kommandozeile können Sie beispielsweise die virtuelle Platte *meine\_platte.vmdk* dem Laufwerk *F:* zuordnen:

```
vmware-mount f: "d:\vmaschinen\testvm\meine_
platte.vmdk"
```

Sollte die virtuelle Disk mehrere Partitionen enthalten, wird mit dem Parameter */v:partnummer* die Nummer der gewünschten Partition angegeben, Standard ist die Nummer 1. So wird die zweite Partition der virtuellen Platte dem Laufwerk *G:* zugeordnet:

```
vmware-mount g: /v:2 "d:\vmaschinen\testvm\meine_
platte.vmdk"
```

Die Zuordnungen können so wieder aufgehoben werden:

```
vmware-mount f: /d
vmware-mount g: /d
```

#### 3.8.2 Erstellen und Verändern virtueller Platten mit VMware vDisk Manager

##### Virtuelle Platten vergrößern oder konvertieren

Mit dem *VMware vDisk Manager* lassen sich virtuelle Platten an der Kommandozeile erstellen und in gewissen Grenzen verändern. Eine Wandlung von IDE in SCSI ist nicht möglich, Sie können aber Zuwachsplatten in reservierte Platten konvertieren, Platten vergrößern oder monolithische Platten in Segmente aufteilen. Sie finden das Tool im Installationsverzeichnis Ihrer VMware-Version, z.B. *C:\Programme\VMware\VMware Workstation*. Ein Aufruf ohne Parameter zeigt Ihnen alle Funktionen und die Syntax an. Folgende Funktionen stellt das Tool bereit:

- ▶ Virtuelle Festplatten erstellen.
- ▶ Eine virtuelle Festplatte auf das Shrinken vorbereiten (Ausnullen). Die virtuelle Platte muss dazu vorher mit *vmware-diskmount* auf dem Host gemountet werden.
- ▶ Virtuelle Platten shrinken.
- ▶ Virtuelle Festplatten vergrößern. Die Partitionen in der Platte müssen allerdings nachträglich angepasst werden.
- ▶ Virtuelle Festplatten konvertieren, z.B. von Zuwachs auf vorreserviert und umgekehrt oder von monolithisch auf 2-GB-Streifen.
- ▶ Virtuelle Festplatten umbenennen. Nützlich vor allem bei segmentierten Platten.

Dieser Befehl erstellt z.B. aus einer virtuellen monolithischen Zuwachsplatte eine Zuwachsplatte in 2-GB-Segmenten, wodurch Sie eine editierbare Kopfdater erhalten oder eine große Platte auf mehrere DVDs verteilen können:

```
vmware-vdiskmanager.exe -r meine_singledisk.vmdk -t 1
meine_splitdisk.vmdk
```

### 3.8.3 Grafische Oberflächen für die Kommandozeilentools von VMware

Auf der Webseite <http://petruska.stardock.net/software/VMware.html> werden interessante Erweiterungen für die genannten VMware-Kommandozeilentools angeboten:

- ▶ *VMware DiskMount GUI* – bietet eine grafische Oberfläche für das VMware DiskMount Tool.
- ▶ *VMware DiskManager GUI* – bietet eine grafische Oberfläche für `vmware-vdiskmanager.exe`.
- ▶ *Virtual DiskFactory* – ist eine stark erweiterte grafische Oberfläche für `vmware-vdiskmanager.exe` mit zusätzlichen Funktionen.

### 3.8.4 Direktes Mounten virtueller Platten von Microsoft

Das Tool WinImage ermöglicht das Mounten von Microsofts virtuellen Platten (\*.vhd), ähnlich dem Tool VMware Disk Mount:

<http://www.winimage.com/winimage.htm>

### 3.8.5 Verdichten virtueller Zuwachsplatten unter VMware und Microsoft

Wenn eine Zuwachsplatte einmal Platz auf dem physischen Datenträger belegt, gibt sie diesen nicht wieder frei, auch wenn Dateien im Gast gelöscht werden. Um die Platte wieder zu verkleinern, existieren verschiedene Möglichkeiten.

Reservierte virtuelle Platten (virtuelle Festplatten fester Größe) können nicht verkleinert werden, diese Funktion existiert nur für Zuwachsplatten.



Als Vorbereitung sollten Sie im Gast bei der Gelegenheit gleich aufräumen und temporäre Ordner sowie übrig gebliebene Dateien löschen, damit sich der Vorgang des Verdichtens auch lohnt und möglichst viele unbenutzte Sektoren entfernt werden. Auch eine Defragmentierung kann nicht schaden. Gelöschte Dateien im Papierkorb des Gastes sind für die Shrink-Funktion immer noch benutzte Bereiche der virtuellen Platte und können nicht entfernt werden. Leeren Sie also vorher unbedingt den Papierkorb.



## Komprimieren virtueller Festplatten mit Shrink oder virtuelle Festplatte komprimieren

Sie können die *Shrink-Funktion* von VMware bzw. die Funktion *Virtuelle Festplatte komprimieren* von Microsoft verwenden. Diese Funktionen entfernen alle unbenutzten Sektoren aus der Behälterdatei. Dabei wird der physische Platz auf dem Host-Datenträger wieder frei, die Behälterdatei wird kleiner. Als Vorbereitung müssen Sie im Gast alle unbenutzten Sektoren mittels bestimmter Tools mit Nullen überschreiben, nur diese Sektoren können aus der Behälterdatei entfernt werden. Führen Sie das Ausnullen nicht durch, kann die Komprimierungsfunktion keinen Platz freigeben, weil von außen nicht ersichtlich ist, welche Sektoren vom Gastsystem unbenutzt sind. Weiterhin benötigen Sie genügend Platz auf dem physischen Datenträger, da der Shrink-Vorgang mit temporären Kopien der virtuellen Platten arbeitet.



Die Funktion des Verdichtens der Festplatte kann sehr lange dauern und auch den Host spürbar ausbremsen, vor allem wenn nur ein physischer Datenträger im Host vorhanden ist, da alle Aktionen auf der gleichen Platte durchgeführt werden müssen. Während dieser Zeit ist der Gast blockiert.

### Shrink unter VMware

Unter VMware können Sie im Gast in den VMware Tools unter dem Reiter SHRINK mit der Funktion PREPARE TO SHRINK unbenutzte Sektoren mit Nullen überschreiben. Anschließend führen die Tools auch gleich die Shrink-Funktion aus, die je nach Größe der virtuellen Platte sehr lange dauern kann. Die Shrink-Funktion steht nicht zur Verfügung, wenn die VM einen Snapshot, eine eingebundene physische Festplatte oder eine Platte im Modus nonpersistent hat.

### Virtuelle Festplatte komprimieren unter Microsoft

Microsoft liefert ein ISO-Image mit Namen *Precompact.iso*, bzw. *Virtual Disk Precompact.iso* mit, das Sie als virtuelle CD in den Gast einbinden können. Darauf befindet sich das Tool zum Ausnullen unbenutzter Sektoren. Sie finden die ISO-Datei auf dem Host im Installationsverzeichnis von Virtual Server bzw. Virtual PC. Anschließend können Sie mit VIRTUELLE FESTPLATTEN/ÜBERPRÜFEN/VIRTUELLE FESTPLATTE KOMPRIMIEREN die unbenutzten Sektoren aus der virtuellen Platte entfernen. Das funktioniert nur, wenn die virtuelle Platte nicht verwendet wird.

## Virtuelle Platten mit einem Imaging-Tool komprimieren als schnellere Alternative für alle Produkte

Als Alternative zu den Funktionen der Virtualisierer können Sie den Inhalt einer virtuellen Platte mit einem Imaging-Tool auf eine neue, leere virtuelle Platte übertragen, das ist in vielen Fällen der schnellste Weg. Ein Imaging-Tool blendet unbelegte Sektoren meistens selbst aus, indem es beim Anfertigen des Images in der Dateizuordnungs-

tabelle nachschaut und nur wirklich belegte Sektoren mitkopiert. Aus diesem Grunde müssen Sie sich nicht um das Ausnullen der Sektoren kümmern.

Ein großer Vorteil dieser Methode ist, dass Sie selbst bestimmen können, wo die virtuelle Zielplatte liegt, z.B. auf einem externen Datenträger oder im LAN, was den Vorgang deutlich beschleunigen kann, wenn der Host nur eine langsame Festplatte hat.

**Das Übertragen eines Images ist schneller**

Weiterhin können manche Tools den Platteninhalt sogar im laufenden Betrieb des Gastes übertragen. In Verbindung mit vorhergehender Sicherung, mit Rücksetzen des Archivbits und nachfolgender inkrementeller Übertragung der geänderten Dateien ermöglicht Ihnen das eine Verdichtung virtueller Platten mit minimaler Ausfallzeit des Gastsystems. Sie können folgendermaßen vorgehen:

1. Binden Sie in die VM mit der zu verdichtenden Zuwachsplatte eine neue virtuelle Platte ein. Diese Platte sollte auf einem anderen physischen Datenträger oder im LAN liegen. Die VM muss dazu kurz neu gestartet werden.
2. Starten Sie die VM von einer CD, idealerweise ein ISO-Image, mit Ihrem bevorzugten Imaging-Programm, oder verwenden Sie ein Imaging-Programm im laufenden Gastsystem.
3. Übertragen Sie den Inhalt der Quellplatte auf die neue virtuelle Platte. Die meisten Imaging-Programme übertragen nur belegte Sektoren, wodurch die Zielplatte nur den benötigten Platz auf dem Host benutzt.
4. Entfernen Sie die Quellplatte aus der VM, und binden Sie an Ihrer Stelle die neue Platte ein. Kopieren Sie die verdichtete Platte gegebenenfalls auf den Host, wenn sie auf einer Netzwerkfreigabe abgelegt war.

### 3.8.6 Vergrößern virtueller Platten

Um eine virtuelle Platte nachträglich zu vergrößern, existieren ebenfalls zwei Möglichkeiten:

- ▶ Sie können den Inhalt mit einem Imaging-Tool auf eine zweite virtuelle Platte übertragen, die in ausreichender Größe angelegt wurde. Bei dieser Gelegenheit verschwinden bei Zuwachsplatten auch unbenutzte Sektoren, und die Partitionen werden ebenfalls von den meisten Imaging-Tools gleich mit vergrößert. Die Quelle bleibt erhalten, was mehr Sicherheit bietet, sollte der Vorgang abbrechen.
- ▶ Sie können die virtuelle Platte unter VMware mit dem Tool *vmware-vdiskmanager.exe* vergrößern. Danach sind die Partitionen im Gast auf die neue Größe anzupassen. Bei dynamischen Windows-Datenträgern im Gast kann der freie Platz einfach zugewie-

sen werden, bei normalen Partitionen benötigen Sie eine Tool, das die Vergrößerung durchführt, wie z.B. Symantec Partition Magic. Diese Methode ist etwas umständlich.

```
vmware-vdiskmanager.exe -x 20Gb meine_vplatte.vmdk
```



Bei der Vergrößerung mittels `vmware-vdiskmanager.exe` kann unter Umständen der Gast wegen einer veränderten CHS-Geometrie nicht mehr starten, siehe „Probleme nach der Änderung der CHS-Geometrie“.

#### 3.8.7 Umwandeln einer virtuellen IDE-Platte in eine SCSI-Platte unter VMware

Die Kopfdatei einer segmentierten virtuellen Platte enthält einige Informationen, die sich manipulieren lassen. Als Beispiel soll die Konvertierung einer IDE-Platte in eine SCSI-Platte dienen.



Um eine IDE-Platte in eine SCSI-Platte zu konvertieren, können Sie auch wieder auf ein Imaging-Programm zurückgreifen. Übertragen Sie in einer VM den Inhalt der IDE-Platte auf eine SCSI-Platte. Bei größeren virtuellen Platten kann der Vorgang sehr lange dauern, er erspart Ihnen aber Manipulationen an den virtuellen Platten. Um eine virtuelle Platte auf den ESX Server zu übertragen, können Sie den *VMware Virtual Machine Importer* verwenden, der auch automatisch den Plattentyp der Gäste anpasst, siehe Teil 2, Kapitel 9, „*VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2*“.

Unter VMware ist es nicht möglich, eine virtuelle IDE-Platte einfach an einem SCSI-Controller zu betreiben, da beide Typen unterschiedliche CHS-Geometriedaten benutzen und außerdem den Controller-typ in der eigenen Konfiguration hinterlegt haben. Um IDE in SCSI zu wandeln, müssen einige Parameter geändert werden, was dank der Kopfdatei im Textformat möglich ist. Eine monolithische Platte enthält diese Informationen dagegen direkt in der Behälterdatei, was das Editieren erschwert und gefährlich macht. Die umzuwandelnde IDE-Platte sollten Sie deshalb vor der Aktion mit dem `vmware-vdiskmanager.exe` in eine segmentierte Platte umwandeln. Damit haben Sie auch gleich eine Sicherungskopie, weil die originale Platte erhalten bleibt.

#### Editieren einer monolithischen Datei

Sie können mit einem geeigneten Editor zwar auch direkt in der monolithischen Datei editieren, darauf sollten Sie aber nur im Notfall, etwa bei Platzmangel, zurückgreifen. Beachten folgende Hinweise, wenn Sie nicht in einer textbasierten Kopfdatei, sondern direkt in der Behälterdatei editieren:

- ▶ Sie benötigen einen Text- oder Hex-Editor, der nicht erst die gesamte Datei in den Speicher laden will, sondern direkt editieren kann. Das beherrscht z.B. *UltraEdit* mit der Option `ADVANCED/CONFIGURATION/GENERAL/OPEN FILE WITHOUT TEMPFILE` (siehe Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“).
- ▶ Verwenden Sie keinesfalls Word oder ähnliche Textverarbeitungsprogramme, da diese mit eingefügten Formatierungen die Struktur in der Behälterdatei zerstören.
- ▶ Arbeiten Sie keinesfalls im Einfügemodus, um die Dateilänge nicht zu verändern und die gesamte Struktur der Datei durcheinanderzubringen.
- ▶ Löschen Sie nichts, ebenfalls wegen der Dateilänge, sondern überschreiben Sie zu entfernende Passagen mit Leerzeichen.
- ▶ Ändern Sie nur Stellen, von denen Sie genau wissen, was sie bedeuten.

### Anpassen der CHS-Geometrie und des Controllertyps

Ich gehe im Folgenden davon aus, dass Ihre IDE-Platte als segmentierte Datei mit einer Kopfdatei im Textformat vorliegt. Sie benötigen einen Texteditor, der Dateien im Unix-Format lesen kann, weil sonst keine Zeilenumbrüche in der Kopfdatei erkannt werden:

**Die Kopfdatei  
direkt bearbeiten**

1. Erstellen Sie für die VM mittels `VM/SETTINGS/HARDWARE/ADD` eine zusätzliche virtuelle SCSI-Platte in genau derselben Größe wie die umzuwandelnde IDE-Platte. Erstellen Sie diese SCSI-Platte in Segmenten, um eine Kopfdatei im Textformat zu erhalten. Es genügt eine Zuwachsplatte, sie wird nur als Dummy benötigt und kann später wieder gelöscht werden.
2. Starten Sie die VM, und lassen Sie im Gastsystem den SCSI-Controller erkennen. Testen Sie, ob der Zugriff auf die SCSI-Platte funktioniert. Damit stellen Sie sicher, dass die VM später von der umgewandelten IDE-Platte bootet, weil die richtigen Controllertreiber bereits installiert sind.
3. Fahren Sie die VM herunter, und entfernen Sie aus Ihrer VM die umzuwandelnde IDE-Platte und die eben erstellte SCSI-Platte mittels `VM/SETTINGS/HARDWARE/REMOVE`.
4. Laden Sie die Kopfdateien beider virtueller Platten in einen Editor. Sie finden die Dateien im Verzeichnis der VM. Es sind die *vmdk*-Dateien ohne fortlaufende Nummer mit geringer Dateigröße.
5. Kopieren Sie den Abschnitt mit den Geometriedaten und dem Adaptertyp aus der SCSI-Platte, und ersetzen Sie die Einträge in

der IDE-Platte damit. Die benötigten Zeilen sehen beispielsweise folgendermaßen aus, ändern Sie nur diese Parameter:

```
ddb.geometry.cylinders = "1044"
ddb.geometry.heads = "255"
ddb.geometry.sectors = "63"
ddb.adapterType = "buslogic" | "lsilogic"
```

6. Speichern Sie die Kopfdatei ab, und nehmen Sie die umgewandelte IDE-Platte über VM/SETTINGS/HARDWARE/ADD wieder in Ihre VM auf, sie erscheint jetzt als SCSI-Platte.

#### **Probleme nach der Änderung der CHS-Geometrie**

Sollten Sie nach dem Ändern Probleme mit dem Start des Gastsystems haben, dann schauen Sie bitte in *Teil 3, Kapitel 6, „P2V – physische Server in virtuelle Maschinen übernehmen“*, dort sind folgende Probleme beschrieben:

- Die VM bootet nicht bei unterschiedlicher CHS-Geometrie von Quelle und Ziel.
- Die SCSI-Emulation hat teilweise Probleme mit Partitionen größer als 8 GB (*In13*).

#### **CHS-Geometrie einer virtuellen Platte selbst berechnen**

Das Erstellen der Dummy-Datei bei der Umwandlung von IDE in SCSI hat zwei Vorteile: Sie können dadurch gleich den Treiber im Gast automatisch erkennen lassen, und Sie bekommen die benötigten Geometriedaten der SCSI-Platte von VMware frei Haus. Die Geometriedaten können Sie aber auch selbst berechnen. Dazu befindet sich eine Excel-Tabelle mit dem Algorithmus auf der Buch-CD.

# 4 Die Snapshot- und Clone-Funktion der VMware-Produkte

Ein wichtiger Grund, warum virtuelle Maschinen vor allem in Testumgebungen das Leben für Admins, Entwickler und Consultants wesentlich erleichtern, sind die so genannten Snapshots von VMware Workstation, Server und ESX Server zur komfortablen Sicherung von Zuständen eines Gastsystems. Sollten Sie mit VMware gerade die ersten Schritte wagen, fragen Sie sich wahrscheinlich, wozu Snapshots dienen. Arbeiten Sie bereits damit, interessieren Sie sicherlich ein paar Hintergründe und Tricks dazu. Linked oder Full Clones sowie Teams sind weitere Themen dieses Kapitels.

**Redo-Logs, multiple Snapshots und linked Clones**

Zusätzlich erfahren Sie in einem praktischen Workshop in *Abschnitt 4.4, „Multiple Snapshots von VMware Workstation und ESX Server 3“* alles über den Umgang mit mehreren Snapshots und über die technischen Hintergründe.

## 4.1 Was ist ein Snapshot, und wozu brauchen Sie das?

Stellen Sie sich vor, Sie haben gerade in einer virtuellen Maschine ein sauberes Betriebssystem installiert, die aktuellen Patches aus dem Internet geholt und all die vielen Einstellungen erledigt, um das System an Ihre Anforderungen anzupassen. Jetzt können Sie endlich die Beta-Version eines eben heruntergeladenen Programms in der VM testen. Schade nur, dass die Software den Gast zum Absturz bringt und dabei offensichtlich das neu eingerichtete System beschädigt hat – es bootet nicht mehr. Nach einigen Reparaturversuchen geben Sie entnervt auf und installieren das Betriebssystem in der VM von Grund auf neu. Natürlich hätten Sie vorher eine Kopie der virtuellen Platte sichern können, aber oftmals denkt man nicht daran, oder es ist kein Platz bzw. keine Zeit, um vor jedem Test die komplette VM zu kopieren.

**Ein Snapshot sichert Systemzustände**

Ein Snapshot ist die Lösung für solche Probleme. Er friert den momentanen Zustand eines Gastes auf Mausklick kurz ein und sichert diesen Status. Der Vorgang geht sehr schnell und benötigt kaum Platz, Sie können sofort im Gastsystem weiterarbeiten. Alle Änderungen, die Sie ab jetzt in der VM vornehmen, schreibt VMware nicht mehr direkt auf die virtuellen Platten. Stattdessen leitet VMware Schreibzugriffe des Gastsystems in *Redo-Logs* um, das sind zusätzliche Dateien, die zu jeder virtuellen Platte bei einem Snapshot entstehen.

Alle geänderten Sektoren werden in den Redo-Logs gepuffert und lassen sich jederzeit per Mausklick verwerfen, wodurch die Änderungen am Gastsystem seit dem letzten Snapshot wieder verschwinden.

## 4.2 Besonderheiten der Snapshots unter VMware

Im Prinzip bieten die Snapshots mit ihren Redo-Logs unter VMware eine ähnliche Funktionalität wie die Differenzplatten oder Rückgängig-Datenträger von Microsoft Virtual PC und Virtual Server (siehe Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“). Zwei Besonderheiten zeichnen die Snapshots von VMware aus.

### 4.2.1 Snapshots im laufenden Betrieb sichern auch den Laufzeitzustand einer VM

Fast alle vorgestellten VMware-Produkte, bis auf den Player, bieten die Möglichkeit, einen Snapshot im laufenden Betrieb einer virtuellen Maschine anzulegen. Dabei sichert VMware den RAM-Inhalt und den Status des Gastes. Bei Bedarf können Sie diese Sicherung zurückladen, worauf das Gastbetriebssystem sofort genau an der gleichen Stelle wie zum Zeitpunkt des Snapshots weiterarbeitet, inklusive aller geöffneten Applikationen, die VM muss dazu nicht erst booten. Ein Snapshot im laufenden Betrieb entspricht ungefähr dem Suspend-Modus einer VM, nur dass Sie zu dem gleichen abgespeicherten Zustand immer wieder zurückkehren können. VMware Workstation und der ESX Server verwalten mit ihren multiplen Snapshots sogar mehrere solcher eingefrorenen Zustände des gleichen Gastes. VMware Server lässt nur einen aktuellen Snapshot pro VM zu, ein weiterer Snapshot überschreibt den Vorgänger.

### 4.2.2 Multiple Snapshots von VMware Workstation und ESX Server 3 sichern mehrere Zustände eines Gastsystems

#### Wiederanlaufpunkte erstellen

Eine Besonderheit von VMware Workstation 5.5 und auch von ESX Server 3 ist die komfortable Verwaltung mehrerer Snapshots, wodurch die Sicherung verschiedener aufeinander folgender Systemzustände möglich wird. So können Sie z.B. eine Betriebssysteminstallation in mehrere unabhängige Wiederanlaufpunkte gliedern, etwa einen Zustand nach der Grundinstallation, einen Zustand mit Service Pack, einen mit Applikation A usw. Zu jedem dieser Zustände wechseln Sie per Mausklick in einen übersichtlichen Snapshot-Manager,

ohne die anderen Zustände zu verwerfen (siehe auch Abbildung 4.2 weiter unten). So schalten Sie beispielsweise in ein und derselben VM blitzschnell zwischen einer Systemversion mit Service-Pack und einer Version ohne Service-Pack hin und her.

## 4.3 So funktionieren Snapshots unter allen VMware-Produkten

Grundsätzlich ist das Prinzip eines Snapshots bei allen VMware-Produkten gleich. Unterschiede gibt es nur in der Bedienung und in den Funktionen.

**VMware Player**

Dem VMware Player fehlt die Möglichkeit, Snapshots anzulegen und zu verwalten. Er kann aber immer wieder zu einem Snapshot der VM zurückkehren, der vorher unter VMware Workstation oder VMware Server gesichert wurde. Dadurch lassen sich Gäste im Player jederzeit auf einen sauberen Grundzustand zurücksetzen. Diese Vorgehensweise beschreibe ich ausführlich in *Teil 2, Kapitel 5, „Virtuelle Umgebungen mit dem VMware Player weitergeben“*.

Mit allen anderen im Buch vorgestellten VMware-Produkten können Sie in den Gästen jederzeit einen Snapshot setzen, auch im laufenden Betrieb. Der VMware Server unterstützt allerdings immer nur einen aktuellen Snapshot pro Gast. VMware Workstation und ESX Server 3 reizen dagegen die Möglichkeiten der Snapshots voll aus, Sie können mehrere Snapshots zu unterschiedlichen Zeitpunkten setzen und zu jedem dieser gespeicherten Zustände wechseln.

**VMware Server  
und Workstation**

Das Sichern verschiedener Zustände mit mehreren Snapshots ist beim VMware Server zwar nicht eingebaut, es gibt aber Tricks, das in gewissen Grenzen doch zu ermöglichen (siehe *Abschnitt 4.7, „Multiple Snapshots und linked Clones unter VMware Server und VMware Player“*).



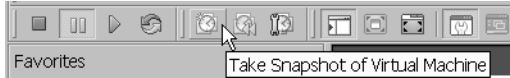
### 4.3.1 Die Funktionen Snapshot und Revert zum Sichern und Verwerfen von Zuständen eines Gastes

Zur Bedienung der Snapshots existieren bei allen VMware-Produkten die beiden Funktionen SNAPSHOT und REVERT, unabhängig davon, ob multiple Snapshots zum Einsatz kommen oder nicht. Sie finden Snapshot/Revert entweder im Menü VM/SNAPSHOT oder als Schaltflächen in der Symbolleiste (Abbildung 4.1). Die Funktion SNAPSHOT sichert den derzeitigen Zustand des Gastsystems.



Die Funktion REVERT verwirft alle aufgelaufenen Änderungen und kehrt zum zuletzt gesicherten Zustand wieder zurück. Die im Menü des VMware Servers zusätzlich verfügbare Funktion REMOVE SNAPSHOT überführt die VM wieder in den Zustand ohne Snapshot (siehe auch Abschnitt 4.7.5, „Entfernen des Snapshot-Status beim VMware Server“).

Abbildung 4.1:  
Zum Anlegen und  
Verwerfen eines  
Snapshots existie-  
ren Schaltflächen in  
der Werkzeugleiste



Die Grundfunktion von Snapshot/Revert ist bei allen Produkten gleich und universell einsetzbar. VMware Workstation 5.5 und ESX Server 3 haben zusätzlich einen Manager, um mehrere Snapshots zu verwalten. Zu diesen multiplen Snapshots komme ich weiter unten in diesem Kapitel.

### 4.3.2 Was passiert beim Setzen eines Snapshots?

#### Vor dem ersten Snapshot

Solange Sie in einem Gast arbeiten, ohne den ersten Snapshot gesetzt zu haben, funktioniert die VM wie ein physischer Rechner:

- ▶ Alle Änderungen an Dateien oder Verzeichnissen werden sofort auf die virtuelle Festplatte geschrieben und lassen sich nicht mehr rückgängig machen.
- ▶ Ein Herunterfahren des Gastes schließt alle offenen Anwendungen. Um später weiterarbeiten zu können, müssen Sie das Gastsystem erst neu hochfahren, und alle Applikationen wieder starten.
- ▶ Schalten Sie den Gast ohne Herunterfahren einfach ab (VM/POWER/POWEROFF), gehen ungespeicherte Änderungen der Applikationen im Gast verloren, und das Dateisystem auf der virtuellen Platte kann beschädigt werden. Das entspricht einem Stromausfall bei einem physischen Computer.

#### Nach dem ersten Snapshot

Nach einem Snapshot verhält sich der Gast nach außen zwar immer noch wie ein physischer Rechner. In dem Moment, als Sie den Button SNAPSHOT angeklickt haben, sind aber zwei entscheidende Dinge mit der VM passiert:

- ▶ Für jede virtuelle Platte hat VMware ein Redo-Log erstellt, in dem alle Schreibzugriffe gepuffert werden. Die virtuellen Platten werden nicht mehr direkt beschrieben, die Änderungen in den Redo-Logs lassen sich jederzeit verwerfen.
- ▶ VMware hat den aktuellen RAM-Inhalt und den momentanen Zustand des Gastes zum Zeitpunkt des Snapshots abgespeichert.

Dieser Zustand des Gastsystems kann jederzeit wieder hergestellt werden.

Die beiden Veränderungen an der virtuellen Maschine schauen wir uns im Folgenden etwas genauer an.

Ob ein Snapshot in der VM existiert, können Sie auf den ersten Blick an der Schaltfläche REVERT erkennen (Abbildung 4.1). Ist diese ausgegraut, dann hat die VM keinen Snapshot, und alle Änderungen werden unwiderruflich auf die virtuelle Platte geschrieben.



### Einschalten der Redo-Logs zur Pufferung von Schreibzugriffen

VMware erstellt bei einem Snapshot zu jeder virtuellen Platte der VM eine separate Datei, in die ab sofort alle Schreibzugriffe des Gastes umgeleitet werden, das *Redo-Log*. Der Zugriff erfolgt sektorenweise, das bedeutet, sobald der Gast einen Sektor beschreibt, legt VMware diesen im Redo-Log ab. Auf die zugrunde liegende virtuelle Platte greift der Gast nur noch lesend zu. Veränderte Sektoren präsentiert VMware dem Gast aus dem Redo-Log, unveränderte Sektoren weiterhin von der virtuellen Platte. Das Gastsystem bemerkt von dieser Umleitung nichts.

**Redo-Logs enthalten geänderte Sektoren**

Die Redo-Logs liegen meist im Verzeichnis der VM. In den aktuellen Versionen der VMware-Produkte sind die Redo-Logs eines Snapshots mit einer fünfstelligen Zahl gekennzeichnet, bei mehreren Snapshots werden die zugehörigen Redo-Logs aufsteigend durchnummeriert. Beispielsweise entsteht für eine virtuelle Platte mit dem Namen *vm01\_sys.vmdk* beim ersten Snapshot ein Redo-Log *vm01\_sys-00001.vmdk*. Beachten Sie, dass die Nummerierung der Dateien nicht immer der Reihenfolge der Snapshots entsprechen muss.

Redo-Logs sind immer Zuwachsplatten, auch wenn Sie reservierte virtuelle Platten verwenden, sie belegen also nur den Platz, der von geänderten Sektoren wirklich benutzt wird. Ist Ihre virtuelle Platte nicht monolithisch, sondern in 2-GB-Streifen aufgeteilt, dann wird das Redo-Log ebenfalls in Streifen erstellt, es entstehen also mehrere Dateien mit der Nummer -00001. Zum konkreten Aufbau der virtuellen Platten und der Funktion der Redo-Logs finden Sie in *Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“*, weitere Informationen im *Abschnitt 5.3.3, Wie funktionieren Redo-Logs und Differenzplatten konkret?*.

In älteren VMware-Versionen waren die Dateien der Redo-Logs noch an ihrer Endung *.REDO* zu erkennen. Die aktuellen Programmversionen verwenden nur noch für virtuelle Festplatten im Modus *Independent persistent/nonpersistent* dieses Format.



### Abspeichern des Status und des RAM-Inhaltes eines Gastes bei einem Snapshot

Wenn Sie den Snapshot setzen, während das Gastsystem gerade läuft, sichert VMware zusätzlich den RAM-Inhalt des Gastes und dessen internen Status, z.B. die momentanen Registerinhalte der CPU, in Dateien auf dem Host. Das Speichern kann ein paar Sekunden dauern, wenn Sie der VM viel RAM zugewiesen haben. Während der Sicherung ist der Gast eventuell kurz eingefroren. Die aktuellen Versionen von VMware beherrschen dieses Speichern auch im Hintergrund, ohne den Gast zu unterbrechen. Sie können das Verhalten unter EDIT/PREFERENCES/PRIORITY/TAKE AN RESTORE SNAPSHOT IN THE BACKGROUND einstellen. Zum Testen der Snapshots ist es besser, diese Funktion abzuschalten, weil Sie dann sehen, wann der Speichervorgang abgeschlossen ist. Die Dateien mit dem gesicherten Status des Gastes liegen im Verzeichnis der virtuellen Maschine auf dem Host:

- ▶ \*.vmem – enthält den RAM-Inhalt zum Zeitpunkt des Snapshots.
- ▶ \*.vmsn – enthält den Status der VM zum Zeitpunkt des Snapshots.

### 4.3.3 Die Revert-Funktion zur Rückkehr zu einem gesicherten Zustand

Sobald die Snapshot-Funktion die VM gesichert hat, können Sie sofort weiterarbeiten. Das Gastsystem bemerkt keinen Unterschied zum Zustand ohne Snapshot, dagegen steht für Sie als Anwender ab diesem Moment die Revert-Funktion zur Verfügung, die Folgendes leistet:

- ▶ Mit einem Klick auf REVERT löscht VMware die aktuellen Redo-Logs und legt neue leere Logs an. Sämtliche Änderungen an den virtuellen Platten seit dem letzten Snapshot sind damit verworfen.
- ▶ Zusätzlich schreibt VMware die gesicherten Register der CPU und den RAM-Inhalt in die VM zurück, wenn der letzte Snapshot im laufenden Betrieb erfolgte.

**Revert stellt einen konsistenten Zustand her**

Nach einem Revert steht die VM wieder an derselben Stelle wie in dem Moment, als Sie zuletzt die Schaltfläche SNAPSHOT betätigt haben, und der Gast hat alles vergessen, was seitdem passiert ist. Alle Applikationen, die in dem Moment des Snapshots geöffnet waren, laufen wieder, und alle ungespeicherten Änderungen, etwa ein geöffnetes Word-Dokument, befinden sich wieder im RAM. Das Gastsystem hat somit einen konsistenten Zustand, selbst wenn Sie die VM zwischenzeitlich hart abgeschaltet haben. Wurde der Snapshot im ausgeschalteten Zustand der VM gesetzt, dann ist die VM nach dem Revert ebenfalls aus und muss erst hochgefahren werden.

## Praktisches Beispiel zum Zurücksetzen einer VM mit Revert

Zur Veranschaulichung der Funktion von Snapshot/Revert können Sie selbst folgenden Test durchführen:

1. Starten Sie eine VM mit einem funktionierenden Gastsystem.
2. Kopieren Sie in diesem Gast auf der virtuellen Platte eine größere Datei, z.B. mit dem Windows Explorer, und setzen Sie mitten im Kopiervorgang einen Snapshot.
3. Nach dem kurzen Einfrieren der VM zum Speichern des Snapshots arbeitet die VM weiter, und der Kopiervorgang der Datei im Gast geht normal zu Ende.
4. Sobald Sie REVERT anklicken, setzt VMware die VM zurück. Der Gast befindet sich plötzlich wieder mitten im Kopiervorgang, an der gleichen Stelle des Fortschrittsbalkens. Der Vorgang endet abermals erfolgreich. Das lässt sich beliebig wiederholen.

Haben Sie den Snapshot dagegen gesetzt, während der Gast die Datei über das Netzwerk auf einen anderen Rechner kopierte, dann bricht nach einem Revert der vermeintlich offene Kopiervorgang jedes Mal ab. Das liegt daran, dass der Gast mitten in einem Ablauf erwacht, der für den Zielrechner im LAN längst beendet ist. Der Status der VM stimmt nicht mehr mit dem Zustand des Zielrechners überein. Dieses Beispiel macht bereits einige Probleme bei der unvorsichtigen Verwendung von Snapshots deutlich, so kann ein versehentlich zurückgesetzter produktiver Domänencontroller im Netzwerk ein regelrechtes Chaos auslösen.

**Probleme bei einem Revert**

### 4.3.4 Den nächsten Snapshot im Gast setzen

Früher oder später müssen Sie sich entschieden, was mit den aufgelaufenen Änderungen in Ihrem Gastsystem seit dem letzten Snapshot geschehen soll. Sie können einfach immer weiterarbeiten, wobei VMware die Redo-Logs mit den Änderungen fortschreibt. Sobald Sie allerdings die Folgen eines fehlgeschlagenen Tests verwerfen wollen, gehen dabei alle bisherigen Änderungen seit dem Snapshot verloren. Das können auch gewollte Änderungen sein, wie Patches oder System-einstellungen, die Sie inzwischen am Gastsystem getätigt haben. Irgendwann ist es also an der Zeit, den aktuellen Zustand der VM mit einem neuen Snapshot zu sichern.

**Was passiert mit den aufgelaufenen Änderungen?**

Sie sollten zwischen Änderungen am Gastsystem unterscheiden, die nur zum Testen dienen, und solchen Änderungen, die Sie bewusst am System vornehmen, z.B. die Installation eines neuen Tools oder die Aktualisierung von Patches. Gewollte Änderungen sollten Sie von Zeit zu Zeit mit einem erneuten Snapshot festschreiben, um spätere ungewollte Änderungen, z.B. die Folgen einer Virusinfektion, problemlos verwerfen zu können.



### Weitere Snapshots unter VMware Server erstellen

**Es kann nur ein Snapshot existieren**

Die einzelnen VMware-Produkte unterscheiden sich in der Verwaltung nachfolgender Snapshots. Der VMware Server überträgt bei jedem erneuten Snapshot die Änderungen aus den aktuellen Redo-Logs unwiderruflich auf die virtuellen Festplatten, sie lassen sich danach nicht mehr verwerfen. Anschließend erstellt der Server neue leere Redo-Logs für weitere Änderungen. Überlegen Sie sich also beim VMware Server genau, wann Sie einen weiteren Snapshot erstellen, es gibt kein Zurück. Setzen Sie einen Snapshot aber auch nicht zu spät, weil sonst sehr viele gewollte Änderungen auflaufen, die dann bei einem Revert ebenfalls verschwinden würden.



Es ist in Testumgebungen eine bewährte Praxis, vor erwünschten Änderungen im Gast, z.B. vor einem Update, immer erst zum letzten Snapshot zurückzukehren, um das System zu bereinigen. Danach können Sie die Änderungen an einem sauberen Zustand des Gastsystems durchführen und anschließend sofort einen neuen Snapshot setzen. Ohne das vorherige Bereinigen kann es passieren, dass Sie Ihre erfolgreichen Änderungen zusammen mit vorher unwissentlich eingeschlichenen Fehlern auf die virtuelle Platte übernehmen. Diese Fehler würden Sie dann im Gastsystem nicht mehr los.

**Vorgänger-Snapshots bleiben erhalten**

### Mehrere Snapshots unter VMware Workstation und ESX Server

VMware Workstation 5.5 und ESX Server 3 entschärfen das Problem mit den unwiderruflich festgeschriebenen Änderungen beim nächsten Snapshot, weil diese Produkte den Inhalt der Redo-Logs nicht automatisch auf die virtuelle Platte übertragen. Stattdessen hebt VMware bei jedem Snapshot die aktuellen Redo-Logs auf und legt für die weiteren Änderungen neue leere Redo-Logs mit anderen Versionsnummern an. Wurde der Snapshot im laufenden Betrieb durchgeführt, speichert VMware zusätzlich den aktuelle RAM-Inhalt und den Systemzustand der VM ebenfalls in nummerierten Dateien ab, die dem Snapshot zugeordnet sind. Auf die Funktion multipler Snapshot gehe ich in einem detaillierten Praxisbeispiel unter *Abschnitt 4.4, „Multiple Snapshots von VMware Workstation und ESX Server 3“*, ein.



Trotz der Möglichkeit multipler Snapshots funktionieren die beiden Schaltflächen SNAPSHOT und REVERT bei VMware Workstation und ESX Server prinzipiell genauso wie beim VMware Server – SNAPSHOT sichert den aktuellen Zustand, REVERT kehrt zum letzten gesicherten Zustand zurück. Der Unterschied zum VMware Server ist allein die Tatsache, dass alle einmal gesicherten Zustände unter VMware Workstation und ESX Server erhalten bleiben, damit Sie später bei Bedarf dorthin zurückkehren können.

## 4.3.5 Beispiele für die Verwendung von Snapshots

Den Nutzen des beschriebenen Zusammenspiels von Snapshot und Revert verdeutlichen Ihnen als Zusammenfassung zwei Beispiele.

### Erreichte Installationsstände sichern und Wiederanlaufpunkte setzen

Der erste Anwendungszweck liegt auf der Hand – sobald Sie vorhaben, in einer VM etwas zu tun, bei dem Sie sich nicht ganz sicher sind, wie es ausgeht, sollten Sie vorher einen Snapshot setzen. Das kann der Fall sein, wenn Sie im Gastsystem eine neues Programm installieren, einen Patch einspielen oder irgendetwas testen wollen. Geht etwas schief, können Sie mit einem Revert sofort zum Stand vor dem Unglück zurückkehren. Das funktioniert unabhängig davon, ob der Snapshot im laufenden Betrieb oder im ausgeschalteten Zustand der VM erstellt wurde. Ein Snapshot im laufenden Betrieb spart die Zeit des Herunter- und Hochfahrens des Gastsystems.

**Snapshots vor jedem Test**

### Schnellstart mit gleichzeitigem Bereinigen von Testsystemen

Ein weiteres Beispiel nutzt vor allem die Möglichkeit, einen Snapshot im laufenden Betrieb zu tätigen. Mitarbeiter im Support benötigen ständig andere Betriebssysteme und andere Konfigurationen, um die Probleme von Kunden sofort nachstellen zu können. Ohne Snapshots müssten die Mitarbeiter jedes Mal erst warten, bis eine VM hochgefahren ist, was z.B. bei einem virtuellen Test-Domänencontroller recht lange dauern kann. Wurde dagegen einmal von jedem benötigten System ein Snapshot im laufenden Betrieb gemacht, dann genügt ein Klick auf REVERT. Das System ist in wenigen Sekunden bereit, und selbst geöffnete Applikationen stehen sofort zur Verfügung. Das würde natürlich mit dem Suspend-Modus ebenfalls funktionieren. Mit einem REVERT sind aber auch gleich alle Änderungen anderer Mitarbeiter oder des letzten Tests verworfen, was besonders bei zentralen Testumgebungen nützlich ist. Der Supportmitarbeiter kann nach getaner Arbeit die VM einfach im laufenden Betrieb ausschalten, ohne sich um den Zustand des Systems zu kümmern, das nächste Revert stellt immer eine konsistente Umgebung her.

**Supportumgebung**

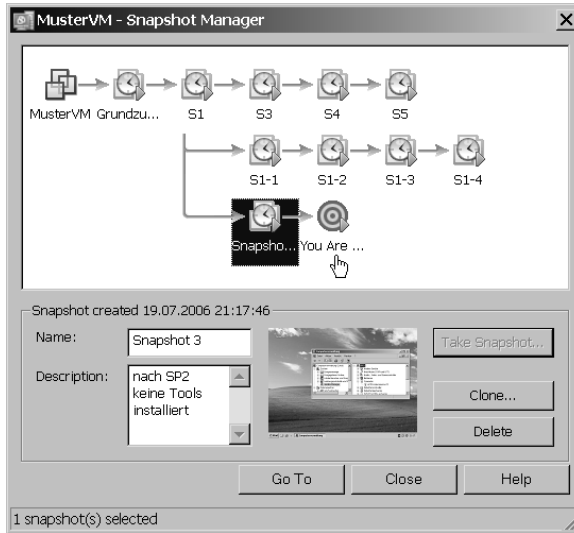
## 4.4 Multiple Snapshots von VMware Workstation und ESX Server 3

Die multiplen Snapshots von VMware Workstation 5.5 und ESX Server 3 erweitern die Möglichkeiten von VMware in Testumgebungen enorm. Ich beschreibe die Funktion im Folgenden exemplarisch an der VMware Workstation 5.5, die Aussagen gelten auch für den ESX Server 3.



Einige erweiterte Hinweise zu den Redo-Logs des ESX Servers, z.B. zum so genannten *Hot-Backup*, finden Sie in Teil 2, Kapitel 9, „VMware Infrastructure 3 mit ESX Server 3 und Virtual Center 2“.

Abbildung 4.2:  
Der Snapshot  
Manager der  
VMware Worksta-  
tion verwaltet alle  
Snapshots über-  
sichtlich in einer  
Baumstruktur



Die VMware Workstation kann, im Gegensatz zum VMware Server, mehrere Snapshots anlegen, die Verwaltung übernimmt der so genannte *Snapshot Manager*. Er listet alle vorhandenen Snapshots auf, und Sie können mit einem Doppelklick auf einen Eintrag in einer Art Baumstruktur sofort zu einem der gespeicherten Zustände wechseln (Abbildung 4.2). Zwei Dinge sind daran besonders interessant:

- ▶ Sie können beliebig zwischen den vorhandenen Snapshots des Gastes hin und her wechseln, ohne einen gespeicherten Zustand zu verwerfen. Wenn Sie beispielsweise mit dem Testen an Snapshot 1 fertig sind, kehren Sie wieder zum Snapshot 4 zurück und umgekehrt.
- ▶ Sie können in der Abfolge der Snapshots auch Verzweigungen anlegen. Anstatt von Snapshot 1 einfach zu Snapshot 4 zurückzu-kehren, legen Sie einen weiteren Snapshot an, der dann von Snapshot 1 einen neuen unabhängigen Zweig eröffnet (Snapshot S1-1 in Abbildung 4.2).

#### 4.4.1 Der Nutzen mehrerer Snapshots an einigen Beispielen

Einige Beispiel zeigen Ihnen den Nutzen mehrerer Snapshots:

##### Vorteile für Train- er, Admin oder Programmierer

Als Trainer gliedern Sie Abläufe für die Lehrgangsteilnehmer in meh-rere Wiederanlaufpunkte, etwa die Einrichtung eines Servers oder einer Applikation. Geht einem Lehrgangsteilnehmer bei einem Schritt

etwas schief, kann er sofort beim letzten Wiederanlaufpunkt neu ansetzen und muss nicht den gesamten Vorgang wiederholen.

Beim Aufbau eines Vorlageclients für ein Rollout oder beim Installieren eines Musters für einen Terminalserver mit vielen Applikationen können Sie jeden einzelnen Schritt mit einem Snapshot sichern und so jederzeit zu früheren Zuständen zurückkehren. Damit spüren Sie Fehler auch später noch auf oder wiederholen die letzten Installationsschritte. Weiterhin ermöglicht der Snapshot Manager eine übersichtliche Dokumentation aller Einzelschritte.

Als Programmierer oder Webdesigner installieren Sie in Ihrer VM eine ältere Windows-Version mit Internet Explorer 5.5. Anschließend setzen Sie einen Snapshot und installieren Internet Explorer 6, nach einem weiteren Snapshot installieren Sie Internet Explorer 7. Jetzt wechseln Sie zum Testen Ihrer entwickelten Webseiten innerhalb von Sekunden zwischen den unterschiedlichen Versionen.

*Linked Clones* sind eine weitere nützliche Funktion, die ebenfalls die Technologie der Snapshots ausnutzt. Im Gegensatz zu mehreren Snapshots können Sie mit linked Clones die verschiedenen Zustände einer VM sogar parallel zur selben Zeit als separate Systeme laufen lassen. Sie benötigen dazu aber auch genügend CPU- und Hauptspeicherressourcen. Siehe dazu *Abschnitt 4.6, „Linked Clones und Full Clones unter VMware Workstation“*.



#### 4.4.2 Ein praktischer Workshop zum Umgang mit multiplen Snapshots

Es gibt beim Umgang mit den multiplen Snapshots einige Dinge zu beachten. Diese Grundlagen veranschaulicht das folgende praktische Testbeispiel, das Sie sofort nachvollziehen können. Sie legen in einer VM Schritt für Schritt eine Verzeichnisstruktur an und setzen dabei Snapshots. In der Praxis könnte es sich dabei um die Installation einer Applikation in mehreren Schritten oder um den Aufbau eines Servers mit verschiedenen Diensten handeln.

##### **Der Snapshot Manager und die Schaltflächen zum Verwalten mehrerer Snapshots**

Sie erzeugen mit der Schaltfläche **SNAPSHOT** in der Werkzeugleiste Snapshots und kehren mit **REVERT** zum jeweils letzten Zustand zurück. Ein neuer Snapshot überschreibt unter VMware Workstation nicht den Vorgänger, alle gespeicherten Zustände bleiben erhalten. Die entstandenen Sicherungen verwalten Sie mit dem Snapshot Manager (Abbildung 4.2). Sie erreichen ihn über das Menü **VM/SNAPSHOT/SNAPSHOT MANAGER** oder über ein Symbol in der Werkzeugleiste (Abbildung 4.3).



Abbildung 4.3:  
Der Snapshot  
Manager kann über  
eine Schaltfläche in  
der Werkzeugleiste  
gestartet werden



**YOU ARE HERE im  
Snapshot-Baum**

Der Manager stellt jeden Snapshot als Eintrag in einer grafischen Übersicht dar. Sie legen im Manager neue Snapshots an oder löschen sie wieder und wechseln zwischen ihnen mit einem einfachen Doppelklick hin und her. Zu jedem Snapshot können Sie einen Namen und eine Beschreibung hinterlegen. Erfolgt ein Snapshot im laufenden Betrieb des Gastes, zeigt VMware zusätzlich eine Miniatur des Bildschirminhaltes zum Zeitpunkt der Erstellung an.

Ein besonderer Eintrag im Snapshot-Baum ist der Status **YOU ARE HERE**. Er verweist immer auf den momentan aktiven Zustand der VM, Sie sehen daran, an welcher Stelle der Gast aktuell arbeitet.

### Vorbereitungen zum Nachvollziehen des Snapshot-Workshops

Für das folgende Beispiel benötigen Sie eine saubere VM mit funktionierendem Betriebssystem. Die VM darf vorerst noch keinen Snapshot haben. Sie können z.B. eine vorhandene virtuelle Platte kopieren und in eine neue VM einbinden. Für den Test verfügt der Gast idealerweise nur über eine einzige monolithische virtuelle Platte, weil das übersichtlicher ist, das ist die Standardeinstellung bei neuen VMs der VMware Workstation. Bei VMs mit mehreren Platten entstehen auch mehrere Redo-Logs, bei Platten in 2-GB-Segmenten besteht jedes Redo-Log aus mehreren Segmenten – das führt zu sehr vielen Dateien im Verzeichnis der VM.



Weisen Sie der VM zum Testen nicht mehr als 128 MB RAM zu, damit das Erstellen der Snapshots möglichst schnell erfolgt.

Beobachten Sie während des Exkurses folgende Dinge:

- ▶ den Snapshot-Baum im Snapshot Manager
- ▶ die Ordnerstruktur, die Sie im Gast auf der virtuellen Festplatte Schritt für Schritt anlegen
- ▶ die entstehenden Dateien auf dem Host im Verzeichnis der VM, hauptsächlich die Redo-Logs mit dem Namen *meine\_vPlatte-xxxxxx.vmdk*

### Anlegen und Verwalten von mehreren Snapshots Schritt für Schritt am praktischen Beispiel

Sie können den folgenden Workshop mit Ihrer Test-VM Schritt für Schritt nachvollziehen, wir beginnen mit dem einfachen Anlegen einer Reihe von Snapshots:

1. Starten Sie Ihre Test-VM, öffnen Sie im Gast den Windows-Explorer (bzw. in einem Linux-Gast den Konqueror o.Ä.), und legen Sie auf der virtuellen Platte einen Ordner mit dem Namen *Snapshot-Test* an. In diesem Ordner legen Sie zur Verdeutlichung der Snapshot-Funktionen im weiteren Verlauf eine Ordnerstruktur an.
2. Erstellen Sie einen ersten Unterordner GZ-Grundzustand (Abbildung 4.4). Diese Änderungen schreibt der Gast unwiderruflich auf die virtuelle Platte, da Sie noch keinen Snapshot gesetzt haben, wodurch kein Redo-Log existiert. Das Symbol YOU ARE HERE im Snapshot Manager zeigt auf den Grundzustand der VM ohne Snapshot.

**Vor dem ersten Snapshot**

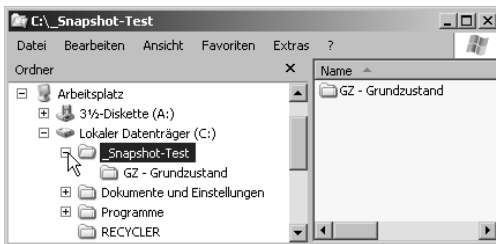


Abbildung 4.4:  
Als Vorbereitung für den Test legen Sie ein Verzeichnis an, in dem Schritt für Schritt weitere Unterordner entstehen werden

3. Setzen Sie jetzt im laufenden Betrieb der VM einen Snapshot, und nennen Sie ihn *Grundzustand* (Abbildung 4.5). Erst in diesem Moment entsteht im Verzeichnis der VM das erste Redo-Log mit der Versionsnummer 00001, z.B. *meine\_vPlatte-000001.vmdk*, in dem VMware ab jetzt alle weiteren Schreibzugriffe auf die virtuelle Platte puffert. YOU ARE HERE zeigt nach dem Snapshot nicht mehr auf die virtuelle Platte, sondern auf dieses aktuelle Redo-Log.

**Der erste Snapshot**

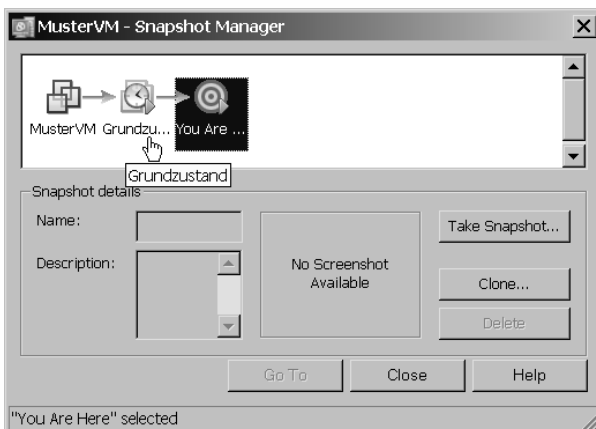


Abbildung 4.5:  
Den erste Snapshot nennen Sie Grundzustand. Erst ab diesem Moment existiert das erste Redo-Log mit der Nummer 00001

Abbildung 4.6:  
Ordner1 ist eine Änderung im Gast-system, die nicht mehr auf die virtuelle Platte, sondern ins Redo-Log 00001 geschrieben wird



#### Weitere Snapshots



4. Legen Sie in der VM einen Ordner mit dem Namen *Ordner1* an (Abbildung 4.6). *Ordner1* wird nicht mehr auf der virtuellen Platte erstellt, sondern in dem aktuell verwendeten Redo-Log mit der Nummer 00001. (Exakter: die veränderten Sektoren, die den Ordner darstellen, befinden sich im Redo-Log.)
5. Setzen Sie einen weiteren Snapshot mit dem Namen *S1* (Abbildung 4.7). VMware hebt das aktuelle Redo-Log 00001 auf und ordnet es diesem Snapshot zu. Zusätzlich entsteht ein neues leeres Redo-Log mit der Versionsnummer 00002. YOU ARE HERE zeigt jetzt auf dieses neue Redo-Log.

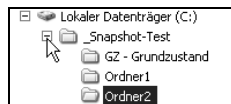
Das ist der Unterschied der VMware Workstation zum VMware Server. Der Server hebt die Redo-Logs nicht auf. Stattdessen überträgt er die Änderungen bei jedem weiteren Snapshot unwiderruflich auf die virtuelle Platte, löscht das Redo-Log und erstellt ein neues.

Abbildung 4.7:  
Snapshot S1 zeigt auf das Redo-Log 00001, in dem sich *Ordner1* befindet. *You Are Here* zeigt auf das Redo-Log 00002



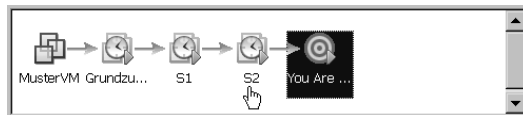
6. Legen Sie in Ihrer VM eine weiteren Ordner mit dem Namen *Ordner2* an (Abbildung 4.8). Dieser Ordner befindet sich damit im gerade aktuellen Redo-Log mit der Versionsnummer 00002 von YOU ARE HERE.

Abbildung 4.8:  
Ordner2 ist eine weitere Änderung im Gastsystem. Er liegt im aktiven Redo-Log 00002



7. Setzen Sie einen weiteren Snapshot mit dem Namen *S2* (Abbildung 4.9). VMware ordnet dem Snapshot *S2* das Redo-Log 00002 zu und erstellt wieder ein neues leeres Log mit der Nummer 00003. YOU ARE HERE zeigt auf dieses neue Log.

Abbildung 4.9:  
Nach dem Snapshot *S2* ist das Redo-Log 00002 diesem Snapshot zugeordnet, *You Are Here* zeigt auf das neue Redo-Log 00003



8. Legen Sie einen weiteren Ordner mit dem Namen *Ordner3* an (Abbildung 4.10), setzen Sie aber noch keinen Snapshot! *Ordner3* befindet sich im aktuellen Redo-Log mit der Versionsnummer 00003, und YOU ARE HERE zeigt weiterhin auf dieses Log, da Sie keinen neuen Snapshot setzen.

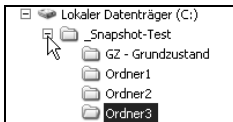


Abbildung 4.10:  
Ordner3 befindet  
sich im Redo-Log  
00003

Zusätzlich zu den Redo-Logs hat jeder Snapshot den RAM-Inhalt und den Status des Gastes in die Dateien *meineVM-SnapshotX.vmem* und *meineVM-SnapshotX.vmsn* gesichert, ersichtlich im Verzeichnis der VM.

**RAM-Inhalt und  
den Status des  
Gastes**

### Der bisher erreichte Zustand im Gastsystem

Die ersten Schritten geben Ihnen bereits einen Überblick, wie VMware seine Snapshots verwaltet und welche Dateien eine Rolle spielen. Anhand der entstandenen Snapshot-Struktur lernen Sie im Anschluss gleich die restlichen Funktionen kennen. Fassen wir vorher kurz zusammen – Sie haben in Ihrer VM folgenden Zustand erreicht:

- ▶ Dem Snapshot mit dem Namen *Grundzustand* sind keine Redo-Logs zugeordnet, er zeigt direkt auf die virtuelle Platte der VM, auf der sich die Ordner *Snapshot-Test* und *GZ* befinden. Da diese Änderungen vor dem ersten Snapshot geschrieben wurden, lassen sie sich nicht mehr verwerfen.
- ▶ Snapshot 1 verweist auf das Redo-Log 00001, das *Ordner1* enthält.
- ▶ Snapshot 2 verweist auf das Redo-Log 00002, das *Ordner2* enthält.
- ▶ YOU ARE HERE verweist auf das Redo-Log 00003, das *Ordner3* enthält. In diesem Redo-Log arbeitet der Gast aktuell. Dieser Zustand ist noch ungesichert, da er keinem Snapshot zugewiesen wurde.

### So verwaltet VMware die Redo-Logs im Gast

Das jeweils aktuelle Redo-Log von YOU ARE HERE (derzeitig Nummer 00003) trägt VMware automatisch als virtuelle Platte in die Konfiguration der virtuellen Maschine ein. Sie können das verfolgen, indem Sie mit einem Texteditor die \*.vmx-Datei öffnen und den Eintrag `ide0:0.fileName`, bzw. `scsi0:0.fileName` suchen. Hier finden Sie den Wert *meine\_vPlatte-000003.vmdk*. Die VM arbeitet also mit dem Redo-Log wie mit einer normalen virtuellen Platte.

**Die Redo-Logs  
benutzt der Gast  
als virtuelle  
Platte**

Die Snapshots setzen aufeinander auf, jedes Redo-Log enthält einen Verweis auf das zugrunde liegende Log. Nummer 00003 verweist auf 00002, dieses wiederum auf 00001. Das erste Redo-Log verweist immer auf die virtuelle Platte. Über diese Verweiskette handelt sich VMware bei einer Leseanforderung des Gastes durch die Dateien, um zu prüfen, ob sich ein Sektor in einem der Logs oder auf der virtuellen Platte befindet (siehe auch Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“).



Sie können sehr gut erkennen, welche Redo-Logs ein Gast aktiv verwendet, indem Sie die Ansicht des Ordners der VM nach der Dateierweiterung (dem Typ) sortieren. Zu jedem verwendeten Redo-Log legt VMware eine Lock-Datei mit der Endung \*.lck an. Arbeiten Sie beispielsweise mit dem Snapshot S2, sehen Sie, dass die Dateien mit der Nummer 00001 und 00002 benutzt werden.

### Verwerfen der aktuellen Änderungen mit Revert

Die jeweils aktuellen Änderungen, dargestellt durch YOU ARE HERE, können Sie mittels REVERT jederzeit verwerfen (Abbildung 4.11). Im aktuellen Falle wäre das der angelegte *Ordner3*, der sich im Redo-Log 00003 befindet. VMware löscht das Log und erstellt automatisch ein neues Log für YOU ARE HERE.



VMware löscht bei einem Revert keine Ordner oder Dateien im Gast, sondern verwirft lediglich geänderte Sektoren in den Redo-Logs. Vom Dateisystem im Gast hat VMware keine Kenntnis.

Abbildung 4.11:  
Mit der Schaltfläche  
Revert verwerfen Sie  
den aktuellen Zu-  
stand der VM, im  
Beispiel das Redo-  
Log 00003 mit  
*Ordner3*



Gleichzeitig stellt VMware bei einem Revert den Status des Gastes zum Zeitpunkt des letzten Snapshots wieder her, im Beispiel von Snapshot S2. Hätten Sie den Snapshot bei ausgeschalteter VM gesetzt, müssten Sie den Gast erst hochfahren. Nach dem Revert sehen Sie in der laufenden VM nur noch die Ordner *GZ*, *Ordner1* und *Ordner2* (Abbildung 4.8). *Ordner3* haben Sie soeben verworfen.

### Wechseln zwischen den einzelnen Snapshots

Legen Sie jetzt im Gast einen Ordner mit dem Namen *Ordner3-neu* an (Abbildung 4.12), setzen Sie aber wieder keinen Snapshot. Sie wissen mittlerweile, dass sich der eben angelegte *Ordner3-neu* in einem Redo-Log befindet, das dem aktuellen Status YOU ARE HERE zugeordnet ist. Sie haben damit wieder den gleichen Zustand wie vor dem eben erfolgten Revert und können den nächsten Test durchführen.

Abbildung 4.12:  
Für den weiteren  
Workshop legen Sie  
einen neuen Ordner3  
an, der sich damit  
wieder im Redo-Log  
00003 befindet



Zwischen den gesicherten Zuständen des Gastes können Sie im Snapshot Manager beliebig wechseln. Dazu genügt ein Doppelklick auf einen Eintrag, beispielsweise auf Snapshot *S1*. Eine Warnmeldung macht Sie darauf aufmerksam, dass ein Wechsel die aktuellen ungesicherten Änderungen verwirft (Abbildung 4.13). Sie lernen damit einen wichtigen Punkt bei der Arbeit mit Snapshots kennen: Die Änderungen in den aktuellen Logs von *YOU ARE HERE*, im Beispiel also der eben angelegte *Ordner3-neu*, sind nicht in einem Snapshot gesichert und werden bei einem Wechsel zu einem anderen Snapshot immer verworfen.

**Aktuelle Änderungen werden verworfen**

Wollen Sie die aktuellen Änderungen von *YOU ARE HERE* erhalten, müssen Sie vor dem Wechsel erst einen neuen Snapshot setzen. In unserem Test tun Sie das aber bewusst nicht, um zu sehen, was bei einem Wechsel zu einem anderen Snapshot passiert.

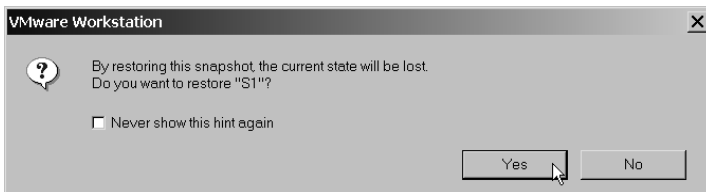


Abbildung 4.13:  
Beim Wechsel zu  
einem anderen Snap-  
shot werden die aktu-  
ellen Änderungen  
von *You Are Here*  
verworfen

Nachdem Sie die Meldung mit *YES* bestätigt haben und zum Snapshot 1 gewechselt sind, sehen Sie im Gastsystem nur noch die Ordner *GZ* und *Ordner1* (Abbildung 4.6). Der *Ordner2* ist erst im Redo-Log von Snapshot 2 enthalten. Sobald Sie mit einem Doppelklick zum Snapshot 2 wechseln, ist *Ordner2* wieder da (Abbildung 4.9 und Abbildung 4.8). *Ordner3-neu* lässt sich dagegen nicht wiederherstellen, da Sie ihn beim Wechsel zum Snapshot 1 verworfen haben.

Die Meldung zum Verwerfen des aktuellen Status erscheint bei jedem Wechsel zwischen den Snapshots. Sie müssen sich entscheiden, ob es sich nur um unwichtige Änderungen handelt oder ob Sie vorher einen Snapshot zur Sicherung setzen.



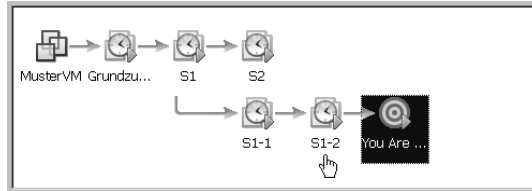
## Eröffnen eines neuen Zweiges im Snapshot-Baum

Wechseln Sie nochmals zum Snapshot *S1*. Sie sehen, *YOU ARE HERE* zweigt immer vom aktuellen Snapshot ab. Weitere Snapshots eröffnen einen neuen parallelen Pfad (Abbildung 4.14). In der Praxis könnten Sie damit eine Applikation in einer bestimmten Versionsnummer installieren und dabei die Snapshots *S1* und *S2* setzen. Parallel dazu installieren Sie in der gleichen VM ab dem Snapshot *S1-1* die Folgeversion der gleichen Applikation oder ein Update. Jetzt wechseln Sie im Manager jederzeit zwischen beiden Versionen hin und her und vergleichen bereinigte Fehler bzw. neue Funktionen der zu testenden Software.

Gehen Sie zum Erstellen eines neuen Zweiges folgendermaßen vor:

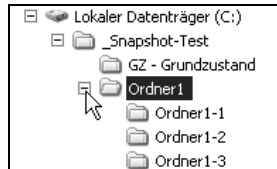
1. Wechseln Sie zum Snapshot *S1*.
2. Legen Sie im Gast als Unterordner von *Ordner1* einen *Ordner1-1* an, und setzen Sie anschließend einen neuen Snapshot mit Namen *S1-1*.
3. Legen Sie im Gast einen weiteren Ordner *Ordner1-2* an, und setzen Sie einen Snapshot mit Namen *S1-2* (Abbildung 4.14).

Abbildung 4.14:  
Jeder parallele Zweig  
im Snapshot-Baum  
kann völlig andere  
Änderungen enthal-  
ten, z.B. unterschied-  
liche Programm-  
versionen



4. Zum Abschluss legen Sie einen Ordner *Ordner1-3* an (Abbildung 4.15), setzen aber keinen Snapshot. Dieser Ordner befindet sich damit wieder im aktuellen ungesicherten Redo-Log von YOU ARE HERE hinter dem Snapshot *S1-2* (Abbildung 4.14).

Abbildung 4.15:  
Die Ordner1-1 bis  
1-3 verdeutlichen in  
unserem Test die  
Änderungen im  
Zweig *S1-1* des  
Snapshot-Baumes



Die Versionsnummern der Redo-Logs lassen sich in diesem Zweig nicht mehr eindeutig den Snapshots zuordnen, da VMware die Nummerierung einfach hochzählt. Dadurch ist es nach Verzweigungen, oder auch bei mehrfachem Zurücksetzen mittels Revert, nicht mehr auf den ersten Blick nachvollziehbar, welches Redo-Log zu welchem Snapshot gehört. Die Zuordnung, die VMware getroffen hat, finden Sie in der Datei *meine\_VM.vmsd*. In dieser Textdatei verwaltet VMware alle Informationen zu den Snapshots.

### Wechsel zwischen verschiedenen Zweigen im Snapshot-Baum

**Aktuellen  
Zustand vorm  
Wechseln sichern**

Wenn Sie vom aktuellen Zustand der VM im Zweig *S1-2* wieder zum Snapshot *S2* wechseln, würden die aktuellen Änderungen von YOU ARE HERE verworfen. Der zuletzt angelegte *Ordner1-3* wäre also wieder verschwunden. Um das zu verhindern, setzen Sie diesmal vor dem Wechsel einen weiteren Snapshot und geben ihm den Namen *S1-3* (Abbildung 4.16). Erst jetzt wechseln Sie zum Snapshot *S2*. Damit ist folgender Zustand erreicht:

- ▶ Sie sehen nach dem Wechsel zum Snapshot 2 im Gast die Ordner GZ, *Ordner1* und *Ordner2*, da Sie sich wieder im oberen Zweig des Snapshot-Baumes befinden.
- ▶ Der aktuelle Zustand YOU ARE HERE hinter Snapshot S2 (Abbildung 4.16) zeigt auf ein neues leeres Redo-Log. Hier werden alle aktuellen Änderungen geschrieben.
- ▶ Der Zweig ab Snapshot S1-1, mit den im Gast angelegten Beispielordnern *Ordner1-1* usw., existiert weiterhin, und Sie können jederzeit dorthin wechseln, um an diesem Stand weiterzuarbeiten.
- ▶ Sie könnten weitere Zweige eröffnen, indem Sie z.B. zum Snapshot S1-2 wechseln und weitere Snapshots anlegen.

Bewegen Sie sich ein wenig in Ihrem Snapshot-Baum, um ein Gefühl für die verschiedenen Snapshots zu bekommen.

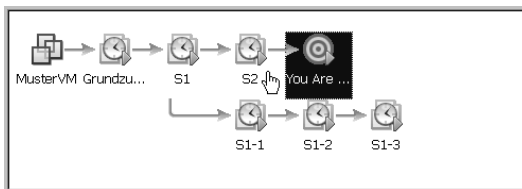


Abbildung 4.16:  
Zwischen den Zweigen können Sie jederzeit wechseln, *You Are Here* zeigt den aktiven Ort im Snapshot-Baum an

### Löschen von einzelnen Snapshots im Snapshot-Baum

Sie sehen, das Anlegen neuer Snapshots und der Wechsel zwischen diesen Sicherungen sind nicht weiter kompliziert. Dagegen sorgt das Löschen von Snapshots regelmäßig für einige Konfusion bei den Anwendern.

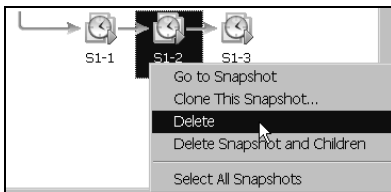


Abbildung 4.17:  
Löschen einzelner Snapshots entfernt und konsolidiert nur die Redo-Logs. Inhalte werden auf den nächstmöglichen Snapshot gerettet

Sie können einen Snapshot mit der rechten Maustaste und DELETE jederzeit entfernen (Abbildung 4.17). Dabei erfolgt allerdings nur ein Ausdünnen und Konsolidieren der Redo-Logs, die enthaltenen Änderungen bleiben bestehen. Wenn Sie z.B. Snapshot S1-2 löschen, rettet VMware vorher den Inhalt auf den nächstmöglichen Snapshot, in diesem Falle auf Snapshot S1-3. Dabei führt VMware die Sektoren der beiden Redo-Logs zusammen. Im Gast ändert sich nichts am Dateisystem, auf dem Host ist dagegen das zugehörige Redo-Log von Snapshot S1-2 verschwunden.

**Konsolidieren der Redo-Logs ohne Löschen der Inhalte**

Eine Ausnahme wäre der Snapshot S1, dessen Redo-Log die Grundlage für den untergeordneten Zweig bildet. Beim Löschen dieses Snapshots bleibt das Redo-Log im Hintergrund erhalten, auch wenn S1 im



Baum verschwindet. Das Erhalten der Inhalte ist notwendig, da Änderungen an Sektoren eines Redo-Logs auch alle nachfolgenden Snapshots beeinflussen würden. Die gesamte Kette von Redo-Logs wäre nicht mehr konsistent und unbrauchbar, wenn VMware mittendrin einfach geänderte Sektoren verwerfen würde.



Der Sinn, einzelne Snapshots zu entfernen, liegt einzig und allein darin, die Anzahl von Redo-Logs zu konsolidieren. Zum einen kommt das der Performance zugute, weil VMware bei Lesevorgängen nicht mehr so viele Dateien durchsuchen muss, zum anderen wird der Snapshot-Baum übersichtlicher. Weiterhin spart die Konsolidierung Platz, weil einige Sektoren in verschiedenen Redo-Logs immer mehrfach vorhanden sein können. Zusätzlich löscht VMware auch die Dateien mit der Sicherung des RAM-Inhaltes, was weiteren Platz spart.

So vollziehen Sie das Löschen eines Snapshots an unserem praktischen Beispiel nach:

1. Löschen Sie den Snapshot *S1-2* mit einem rechten Mausklick und der Funktion DELETE.
2. Wechseln Sie jetzt zum Snapshot *S1-1*. Er enthält nur *Ordner1-1*, wie Sie im Gastsystem sehen können.
3. Wechseln Sie zum Snapshot *S1-3*. Sie sehen *Ordner1-1*, *Ordner1-2* und *Ordner1-3*. Der vorher im Snapshot *S1-2* enthaltene *Ordner1-2* wurde also auf den Snapshot *S1-3* übertragen, bevor VMware das Redo-Log gelöscht hat.



Wenn der gelöschte Snapshot keinen Nachfolger hat, addiert VMware den Inhalt zum Redo-Log von YOU ARE HERE. Sobald Sie allerdings den letzten verbleibenden Snapshot löschen (im Beispiel *Grundzustand*), dann überträgt VMware alle Änderungen unwiderruflich auf die virtuelle Platte – siehe auch „Löschen von bestimmten Snapshots samt Inhalt“.

#### Löschen von bestimmten Snapshots samt Inhalt

##### Änderungen endgültig verwerfen

In einigen Fällen wollen Sie nicht nur die Redo-Logs konsolidieren, sondern die Inhalte der Snapshots verwerfen, z.B. um nach umfangreichen Tests wieder den sauberen Grundzustand der VM herzustellen. Um gesicherte Snapshots samt Inhalt endgültig zu entfernen, sind zwei Schritte notwendig:

1. Zuerst löschen Sie mit der rechten Maustaste und der Funktion DELETE SNAPSHOT AND CHILDREN einen ausgewählte Snapshot im Baum, inklusive aller Nachfolger, aber auf keinen Fall den ersten Snapshot (im Beispiel *Grundzustand*). VMware entfernt die zugeordneten Redo-Logs und überträgt die Inhalte auf YOU ARE HERE.

2. Erst im zweiten Schritt verwerfen Sie diese gesammelten Inhalte mittels REVERT endgültig. Revert löscht die Redo-Logs von YOU ARE HERE.

Sobald Sie Ihren ersten Snapshot des Baumes (im Beispiel *Grundzustand*) mittels DELETE SNAPSHOT AND CHILDREN löschen, überträgt VMware mit einem Schlag sämtliche Änderungen aller nachfolgenden Snapshots auf die virtuelle Platte und verwirft nichts! Dieses Verhalten ist extrem irreführend und vor allem ärgerlich, wenn Sie die Änderungen eigentlich verwerfen wollten, etwa nach ausführlichen Tests in einem Gast. Nur wenn Sie wichtige Änderungen erhalten wollen, ist dieses Verhalten nützlich.

Um virtuelle Platten in Test-VMs sicher vor Veränderungen zu schützen, sollten Sie die Behälterdatei immer mit einem Schreibschutz versehen!

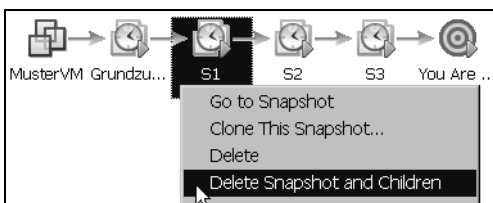


### Entfernen aller Snapshots und Beenden des Snapshot-Status

Wollen Sie Ihre VM wieder in einen Zustand völlig ohne Redo-Logs und Snapshots versetzen, etwa für den produktiven Einsatz einer Muster-VM oder vor dem Weitergeben, existieren zwei Optionen.

Um den sauberen Grundzustand ohne Snapshot herzustellen und alle Änderungen zu verwerfen, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf den zweiten Snapshot Ihres Snapshot-Baumes (im Beispiel S1), und entfernen Sie mittels DELETE SNAPSHOT AND CHILDREN alle nachfolgenden Snapshots (Abbildung 4.18). Stellen Sie sich dazu keinesfalls auf den ersten Snapshot (im Beispiel *Grundzustand*), weil Sie dann alle Änderungen unwiderruflich auf die virtuelle Platte übernehmen würden!



### Änderungen verwerfen

Abbildung 4.18:  
Wird ein Snapshot  
samt Nachfolgern  
gelöscht, dann rettet  
VMware alle Ände-  
rungen auf You Are  
Here

2. Jetzt befinden sich alle Änderungen im Status YOU ARE HERE, und Sie verwerfen diese mittels REVERT. VMware beginnt sofort mit einem leeren Redo-Log.
3. Erst jetzt entfernen Sie den ersten und damit letzten Snapshot (im Beispiel *Grundzustand*) mit rechter Maustaste und DELETE. VMware übernimmt dabei zwar trotzdem den Inhalt des Redo-Logs von YOU ARE HERE auf die virtuelle Platte, dieses Log enthält aber noch keine weiteren Änderungen, da es erst seit dem eben erfolgten REVERT existiert.



Wenn Sie die Schritte im ausgeschalteten Zustand der VM durchführen, entsteht nach dem letzten Revert gar nicht erst ein Redo-Log.

**Änderungen übernehmen**

Wollen Sie dagegen die Änderungen in den Snapshots nicht verwerfen, sondern unwiderruflich auf die virtuellen Platten der VM übernehmen, dann klicken Sie einfach mit der rechten Maustaste auf den ersten Snapshot (im Beispiel *Grundzustand*) und wählen DELETE SNAPSHOT AND CHILDREN. VMware überträgt den Inhalt aller Redo-Logs auf die virtuelle Platte, löscht die Logs und beendet den Snapshot-Status.

**Kein Snapshot mehr**

Unabhängig vom gewählten Vorgehen ist die Schaltfläche SNAPSHOT jetzt wieder ausgegraut, und alle weiteren Änderungen schreibt VMware direkt auf die virtuellen Platten des Gastes. Die VM hat keinen Snapshot mehr. Erst wenn Sie erneut einen Snapshot setzen, entstehen wieder Redo-Logs.

**Die Besonderheit des ersten Snapshots einer VM – der Grundzustand**

Dem ersten Snapshot der VM haben wir nicht ohne Anlass den Namen *Grundzustand* gegeben, ihm kommt eine besondere Rolle zu. Dem ersten Snapshot einer VM sind niemals Redo-Logs zugeordnet, das bedeutet, er enthält keine zu verwerfenden Änderungen. Er verweist immer direkt auf die virtuellen Platten des Gastes. Erst dem Eintrag YOU ARE HERE hinter dem ersten Snapshot ist ein Redo-Log zugeordnet. Darum ist es empfehlenswert, immer gleich zu Beginn einen Snapshot anzulegen, der den Grundzustand der VM sichert.



YOU ARE HERE wird im Snapshot Manager auch dann angezeigt, wenn gar kein Snapshot gesetzt wurde. Das ist z.B. bei einer neu erstellten VM der Fall. Die Anzeige von YOU ARE HERE suggeriert, dass Änderungen wieder verworfen werden können, was aber in diesem Falle nicht stimmt. Ohne Snapshot schreibt VMware alle Änderungen direkt auf die virtuelle Platte.

Eine weitere Besonderheit des ersten Snapshots haben Sie ebenfalls bereits kennen gelernt. Sobald Sie diesen Snapshot mittels DELETE oder DELETE SNAPSHOT AND CHILDREN entfernen, überträgt VMware alle Änderungen automatisch unwiderruflich auf die virtuelle Platte. Das passiert nur beim Löschen des ersten Snapshots. Auch für diesen Fall ist es gut, mit dem eindeutigen Namen *Grundzustand* die Besonderheit dieses Snapshots hervorzuheben.

**Inhalt der Basisplatte dokumentieren**

Weiterhin unterschlägt VMware im Snapshot Manager eine Möglichkeit, den Grundzustand der VM vor dem ersten Snapshot zu dokumentieren. Nicht jede VM wird von Grund auf neu installiert, viele

virtuelle Platten bekommt man auch von Kollegen oder als Mustervorlage aus einem zentralen Archiv. Im Snapshot *Grundzustand* können Sie in diesem Falle dokumentieren, um welche Basisinstallation es sich handelt, bevor Sie eigene Änderungen einbringen.

## **4.5 Tipps zur Arbeit mit Snapshots und einige wichtige Grundsätze**

Für die Arbeit mit Snapshots liefert Ihnen folgende Zusammenfassung einige Hinweise und Tipps.

### **4.5.1 Allgemeine Hinweise zum Umgang mit den Snapshots zu allen VMware-Produkten**

- ▶ Vor dem ersten Snapshot sollten Sie Ihr Betriebssystem samt Patches sowie alle benötigten Tools installieren und die virtuelle Platte im Gastsystem defragmentieren. Wenn Sie zum Testen Versionen des Gastsystems ohne Service-Pack benötigen, können Sie das es auch später installieren.
- ▶ Sobald Sie mit Ihrer sauberen Grundinstallation einer VM zufrieden sind, erstellen Sie sofort einen Snapshot. Erst ab diesem Moment sind Redo-Logs aktiv, und Sie können nachfolgende Änderungen verwerfen. Ohne Snapshot werden alle Änderungen unwiderruflich geschrieben.
- ▶ Erstellen Sie einen Snapshot nicht vor der Betriebssysteminstallation, da sonst die gesamte Grundinstallation in einem Redo-Log und nicht auf der virtuellen Platte abgelegt ist.
- ▶ Ob ein Snapshot in einer VM aktiv ist, erkennen Sie am einfachsten daran, ob die Schaltfläche REVERT ausgegraut ist oder nicht.
- ▶ Um sicherzugehen, dass an wichtigen virtuellen Platten einer VM unter keinen Umständen Änderungen erfolgen, setzen Sie die Behälterdatei der virtuelle Platte im Host-Dateisystem auf den Status Schreibgeschützt.
- ▶ Der VMware Player und der Server arbeiten in VMs, die unter VMware Workstation erstellt wurden, immer mit dem Snapshot, der zuletzt in der Workstation aktiv war. Ein Wechsel zwischen Snapshots ist nicht möglich. Wurde im VMware Server ein neuer Snapshot gesetzt, erscheint dieser nach dem Übertragen der VM zur Workstation im Snapshot-Baum als *VMware Server Undopoint*.

#### 4.5.2 Zusammenfassende Hinweise zur Verwendung von multiplen Snapshots

- ▶ YOU ARE HERE zeigt immer auf das aktuell verwendete Redo-Log, in dem VMware die Schreibzugriffe des Gastes ablegt. Alle anderen Redo-Logs bestehender Snapshots werden nur lesend verwendet.
- ▶ Revert verwirft immer die aktuell benutzten Redo-Logs von YOU ARE HERE, die darin enthaltenen Änderungen gehen dabei unwiderruflich verloren. Es entstehen sofort neue leere Redo-Logs für YOU ARE HERE. Alle anderen Snapshots bleiben erhalten.
- ▶ Ein Wechsel zu einem anderen Snapshot verwirft ebenfalls die aktuell benutzten Redo-Logs von YOU ARE HERE. Um sie zu erhalten, können Sie vorher einen Snapshot setzen.
- ▶ Das Löschen eines Snapshots mit DELETE entfernt nur die Dateien der Redo-Logs. Der Inhalt wird vorher auf den nächstmöglichen Snapshot gerettet. Wenn kein Nachfolger existiert, kopiert VMware die Änderungen auf YOU ARE HERE.
- ▶ Der erste Snapshot einer VM enthält niemals Redo-Logs bzw. zu verwerfende Änderungen. Existiert nur ein einziger Snapshot, dann enthält YOU ARE HERE alle Änderungen.
- ▶ Beim Löschen des letzten verbleibenden Snapshots mit DELETE überträgt VMware alle nachfolgenden Änderungen unwiderruflich auf die virtuelle Platte, es sei denn, Sie haben die Behälterdatei mit einem Schreibschutz versehen.

#### 4.5.3 Virtuelle Platten im Modus *independent persistent* oder *nonpersistent*

Ein Problem bei der Arbeit mit Snapshots kann es sein, wichtige Daten innerhalb der VM bei einem Revert zu erhalten. Nehmen wir an, Sie fertigen zu einer Testinstallation in der VM Screenshots mit einem entsprechenden Tool im Gast an und legen diese auf der virtuellen Platte ab. Wenn Sie den fehlgeschlagenen Test verwerfen, sind auch diese Screenshots verschwunden. Das Gleiche gilt für eingepflegte Daten einer Testdatenbank, dort ist das Problem noch prekärer.

##### **Daten vor Verwerfen schützen**

Sie haben entweder die Möglichkeit, solche Daten gleich außerhalb der VM auf eine Netzwerkfreigabe zu legen. Oder Sie binden in jede VM eine zusätzliche virtuelle Platte im Modus *independent persistent* ein. Zu einer solchen Platte legt VMware niemals Redo-Logs an, sie wird immer unwiderruflich beschrieben. Den gewünschten Modus wählen Sie über die Schaltfläche **ADVANCED** einer virtuellen Platte unter **VM/SETTINGS/HARDWARE**. Auf diesem Datenträger kann der Gast Daten ablegen, die nicht verworfen werden sollen. Leider bringt die Verwendung einer virtuellen Platte in diesem Modus zwei Nachteile mit sich:

- ▶ Der Modus *independent persistent* kann nur eingeschaltet werden, wenn in der VM noch kein Snapshot gesetzt ist.
- ▶ Mit einer Platte im Modus *independent persistent* sind keine Snapshots im laufenden Betrieb möglich. Sie müssen den Gast vor jedem Snapshot erst herunterfahren.

Das Gegenstück ist eine virtuelle Platte im Modus *independent nonpersistent*. Sie hat immer ein Redo-Log, das automatisch beim Beenden verworfen wird. Damit werden VMs immer automatisch zurückgesetzt. Mehr Informationen zu diesen beiden Plattentypen finden Sie in Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“.

#### 4.5.4 Einstellungen zu den Snapshots in jeder VM und global am Host

Folgende wichtige Einstellungen existieren zu den Snapshots. Zu jeder einzelnen VM finden Sie die Optionen unter VM/SETTINGS/OPTIONS/SNAPSHOTS:

- ▶ *Disable Snapshots* – damit schalten Sie die Snapshot-Funktion grundsätzlich ab. Das ist bei produktiven Maschinen empfehlenswert, um versehentliches Setzen und Verwerfen von Snapshots zu verhindern.
- ▶ *When powering off* – hier legen Sie fest, ob VMware beim Abschalten der VM den Snapshot belassen, verwerfen, neu anlegen oder danach fragen soll.
- ▶ *Lock this snapshot* – dieser Punkt existiert nur beim VMware Server. Damit schützen Sie einen vorhandenen Snapshot vor versehentlichem Überschreiben mit einem Folge-Snapshot. In der VM kann kein neuer Snapshot gesetzt werden, solange diese Option gewählt ist.

Die Redo-Logs kann VMware auch an einem anderen Ort als im Verzeichnis der VM speichern. Das kann sinnvoll sein, wenn Sie VMs direkt von einer Netzwerkfreigabe betreiben und die Redo-Logs aus Performancegründen lokal ablegen. Sie ändern das Verzeichnis hier:

**Speicherort der Redo-Logs**

VM/SETTINGS/OPTIONS/GENERAL/WORKING DIRECTORY

#### Snapshot im laufenden Betrieb im Hintergrund erstellen oder Gast kurz einfrieren

Das Abspeichern des Zustandes eines Gastes während des Snapshots erfolgt standardmäßig im Hintergrund, wodurch Sie im Gast sofort weiterarbeiten können. In machen Fällen bremsst die Funktion das Gastsystem während des Vorganges allerdings aus. Schalten Sie die Hintergrundspeicherung ab, können Sie den Fortschritt der Aktion besser verfolgen, was bei mehreren aufeinander folgenden Snapshots praktischer ist. Die Einstellung gilt global für den Host:

EDIT/PREFERENCES (VMware Workstation) oder HOST/SETTINGS (VMware Server) und dort PRIORITY/TAKE AN RESTORE SNAPSHOTS IN THE BACKGROUND.

### 4.5.5 Verwendung von Snapshots in produktiven Umgebungen

#### Gefahr des versehentlichen Zurücksetzens

Snapshots sollten grundsätzlich nur in Testumgebungen oder in Mustervorlagen permanent in einer VM verwendet werden. Produktionsmaschinen können Sie zwar vor einem Update oder vor ähnlichen Änderungen zur Vorsicht ebenfalls mit einem Snapshot sichern. Sobald sich die Änderung als erfolgreich erwiesen hat, sollten Sie den Snapshot aber wieder entfernen und dabei die Änderungen auf die virtuelle Platte übernehmen.

Zum einen kann die Performance unter dem zusätzlichen Redo-Logs leiden, zum anderen stellt das versehentliche Zurücksetzen eines länger aktiven Redo-Logs eine große Gefahr dar. Dabei kommt es zu Datenverlusten und zu inkonsistenten Zuständen von Netzwerkdiensten, z.B. bei mehreren Domänencontrollern, da der Zustand der zurückgesetzten VM weit in der Vergangenheit liegen kann (zu Problemen mit Domänencontrollern siehe auch *Teil 3, Kapitel 5, „Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs“*).

Eine interessante Variante ist die Möglichkeit, nach einem Snapshot die virtuelle Platte als Sicherung wegzukopieren, da durch das Redo-Log kein Schreibzugriff mehr auf die Behälterdatei erfolgt. Siehe dazu ebenfalls *Teil 3, Kapitel 5*.

## 4.6 Linked Clones und Full Clones unter VMware Workstation

#### Linked Clones sparen Zeit und Platz

Eine Erweiterung der Snapshots sind die so genannten linked Clones der VMware Workstation, erreichbar unter VM/CLONE. Im Grunde genommen eröffnet VMware beim Anlegen eines linked Clones einen neuen Snapshot-Zweig. Dieser Snapshot-Zweig wird allerdings einer automatisch erstellten neuen VM zugeordnet. Für diese VM ist der Snapshot-Baum der Mutter-VM nicht mehr sichtbar, der Klon wirkt wie eine eigenständige VM.

Im Verzeichnis des erstellten Klones existiert eine virtuelle Platte *meine\_vPlatte-cl1.vmdk*, die Erweiterung *-cl1* steht für Klon Nummer 1. Diese virtuelle Platte ist nichts weiter als ein Redo-Log, das wiederum auf das Redo-Log des Snapshots der Mutter VM verweist, von dem der linked Clone erstellt wurde, ähnlich wie in einer Verzweigung im Snapshot-Baum.

Sie können mit linked Clones in Sekunden mehrere VMs erstellen, die parallel und unabhängig voneinander laufen. Ein Testnetzwerk ist mit wenigen Mausklicks aufgebaut. Sie sparen Platz, weil die Basisinstallation nur einmal vorhanden sein muss, und Sie sparen Zeit, weil nicht erst die gesamte VM kopiert wird.

Wenn Sie mehrere Testplätze betreiben, können Sie Musterinstallationen auf einer Netzwerkfreigabe ablegen und von dort bei Bedarf linked Clones erstellen. Mehrere Nutzer arbeiten so über ein Gigabit-Netzwerk mit der gleichen Basis-VM, wobei die Redo-Logs der Klone auf den lokalen Testplätzen liegen.

**Testplätze mit  
zentralem  
Musterarchiv**

Ein linked Clone lässt sich nur von einem Snapshot erstellen, der nicht im laufenden Betrieb gesichert wurde. Bei Bedarf können Sie Ihre VM auch herunterfahren und einen linked Clone *from current State* erstellen. Ebenso erlauben VMs mit Platten im Modus *independent* keine linked Clones.



Eine komplette und unabhängige Kopie erstellen Sie dagegen mit einem *full Clone*, wobei VMware die gesamte VM kopiert. Um eine VM weiterzugeben, ist ein full Clone praktischer, bei einem linked Clone dürfen Sie nicht vergessen, die Basis-VM mitzugeben. Ein full Clone sollte immer dann verwendet werden, wenn Sie eine völlig unabhängige Kopie einer VM benötigen.

**Komplette  
Kopien mit  
full Clones**

#### 4.6.1 Templates als geschützte Vorlagen für neue VMs

In Verbindung mit dem Klonen von Gästen ist noch der Template-Modus einer virtuellen Maschine unter VMware Workstation erwähnenswert, Sie schalten ihn über VM/SETTINGS/OPTIONS/ADVANCED mittels ENABLE TEMPLATE MODE ein. Eine Maschine in diesem Modus kann nicht mehr gelöscht werden, und vorhandene Snapshots lassen sich nicht mehr entfernen. Dadurch ist die VM geschützt und kann als Klon-Vorlage für anderen VMs dienen.

Zusätzlich können Sie für diese Templates in den Favoriten einen Ordner *Vorlagen* anlegen und dort für alle benötigten Betriebssysteme jeweils eine fertig eingerichtete VM im Template-Modus erstellen. Jetzt erstellen Sie mittels linked Clones in Sekunden Ihre Testumgebungen immer wieder aus diesen Vorlagen.

**Ordner in den  
Favoriten anlegen**



## 4.7 Multiple Snapshots und linked Clones unter VMware Server und VMware Player

Der VMware Server unterstützt keine multiplen Snapshots und keine linked Clones, was in Testumgebungen jedoch sehr nützlich wäre. Es gibt allerdings einige Tricks, um diese Funktion teilweise nachzubilden. In den Vorgängerversionen GSX Server oder auch Workstation 4 musste man dazu in den Kopfdateien der virtuellen Platten die Verweisketten zwischen den Redo-Logs manuell mit einem Texteditor pflegen. Ohne zusätzliche Tools war der Aufwand zu hoch, um wirklich damit arbeiten zu können. Zum Glück macht es Ihnen der VMware Server wesentlich einfacher.



Wenn Ihnen als Nutzer des VMware Servers die Funktion der Redo-Logs und multipler Snapshots unklar ist, lesen Sie den Workshop zur VMware Workstation unter *Abschnitt 4.4, „Multiple Snapshots von VMware Workstation und ESX Server 3“*, dort sind die multiplen Snapshots mitsamt Grundlagen zu den Redo-Logs ausführlich erklärt.

### 4.7.1 Mehrere Redo-Logs erzeugen mittels Schreibschutz der zugrunde liegenden virtuellen Platte

Bei jedem neuen Snapshot überträgt VMware Server sämtliche Änderungen aus dem aktuellen Redo-Log auf die virtuelle Platte, löscht danach das Log und beginnt mit einem neuen. Es bleiben keine Zwischenstände erhalten wie bei der VMware Workstation.

#### Mehrere Redo-Logs hintereinander erzeugen

**Ein Schreibschutz verhindert das Löschen der Logs**

Es gibt aber eine Möglichkeit, das Löschen der Redo-Logs zu verhindern. Der Trick ist es, die Behälterdatei der virtuellen Platte Ihrer VM mit einem Schreibschutz zu versehen, z.B. im Windows Explorer mittels rechter Maustaste und EIGENSCHAFTEN/SCHREIBGESCHÜTZT. Der Gast hat damit kein Problem, da Schreibzugriffe nach dem ersten Snapshot sowieso ins Redo-Log umgeleitet werden. Der Server kann allerdings bei einem erneuten Snapshot keine Änderungen aus dem aktuellen Redo-Log auf die virtuelle Platte übertragen, bevor er das Log entfernt.

Um Datenverluste zu vermeiden, löscht VMware das Redo-Log vorsichtshalber nicht, sondern erstellt freundlicherweise bei jedem Snapshot ein neues Log mit fortlaufender Versionsnummer – genau wie bei den Snapshots der VMware Workstation. Das bedeutet, Sie

können vor jedem wichtigen Konfigurationsschritt in Ihrem Gastsystem einen Snapshot setzen und erhalten im Hintergrund eine Kette von Redo-Logs mit den Versionsständen Ihres Gastsystems. Eventuell auftretende Fehlermeldungen wie *VMDB failure*, *Insufficient permission to access file* oder *A needed file was not found* können Sie ignorieren, sie haben keine Auswirkung auf die Funktion.

Im Verzeichnis der VM entsteht nach mehreren Snapshots z.B. folgende Kette von Redo-Logs, wobei die Datei ohne Nummer die virtuelle Platte mit der Basisinstallation ist und jedes nummerierte Redo-Log die aufgelaufenen Änderungen zwischen zwei Snapshots enthält:

```
meine_vPlatte.vmdk
meine_vPlatte-000001.vmdk
meine_vPlatte-000002.vmdk
meine_vPlatte-000003.vmdk
usw.
```

### Zu einem Vorgänger-Redo-Log zurückkehren

Die entstandenen Redo-Logs lassen sich beim VMware Server nicht über eine grafische Oberfläche wie beim Snapshot Manager der Workstation verwalten. Um zu einem vorherigen Stand zurückzukehren, entfernen Sie über VM/SETTINGS/HARDWARE mit REMOVE die aktuelle virtuelle Platte (hier hat VMware automatisch das aktuelle Redo-Log eingetragen) und fügen an deren Stelle den Namen des gewünschten Redo-Logs mit ADD/HARDDISK/USE AN EXISTING VIRTUAL DISK ein. Im Grunde genommen macht es VMware Workstation nicht anders, nur eben komfortabler. Die VM ist zum Ändern des Platteneintrages allerdings herunterzufahren und anschließend neu zu starten.

Mit einem Texteditor können Sie die Redo-Logs auch direkt in der Konfigurationsdatei *\*.vmx* der VM als virtuelle Platte eintragen, z.B.:

```
ide0:0.fileName = "meine_idePlatte-000002.vmdk"
scsi0:0.fileName "meine_scsiPlatte-000002.vmdk"
```



Snapshots können Sie zwar weiterhin im laufenden Betrieb setzen, was eine schnelle Sicherung zwischendurch ermöglicht. Allerdings gelangen Sie später zu diesem Laufzeitstatus nicht zurück, da VMware bei dem verwendeten Trick nur die Redo-Logs, nicht aber den RAM-Inhalt pro Snapshot speichert. Dadurch ist der Zustand der Redo-Logs eines Snapshots im laufenden Betrieb nur noch crashkonsistent, als wäre die VM abgestürzt, da der zugehörige Systemstatus nicht wiederhergestellt werden kann. In Testumgebungen ist das aber meistens nicht weiter dramatisch. Konsistente Snapshots können Sie jederzeit im heruntergefahrenen Zustand des Gastes erstellen.

**Snapshots  
im laufenden  
Betrieb**

**Dokumentation  
der Snapshots**

Auch um die Dokumentation, welcher Zustand in welchem Redo-Log enthalten ist, müssen Sie sich selbst kümmern, am besten legen Sie dazu für jeden Gast eine Textdatei in seinem Verzeichnis an, in der Sie die Versionsnummer des Redo-Logs und die getätigten Änderungen im Gastsystem notieren.

**Praktisches Beispiel zum Einsatz mehrere Redo-Logs beim  
VMware Server**

Der beschriebene Trick ist sehr nützlich, um in Testumgebungen mehrere Zwischenstände zu sichern, auch wenn der Umgang damit etwas umständlich ist. Ein Beispiel zeigt Ihnen die Funktion, es ähnelt der ausführlichen Beschreibung unter *Abschnitt 4.4, „Multiple Snapshots von VMware Workstation und ESX Server 3“*:

1. Erstellen Sie eine neue VM mit einem sauberen Gastbetriebssystem, setzen Sie noch keinen Snapshot.
2. Fahren Sie die VM herunter, versehen Sie die virtuelle Platte mit einem Schreibschutz, z.B. im Windows Explorer mittels rechter Maustaste und EIGENSCHAFTEN/SCHREIBGESCHÜTZT.
3. Setzen Sie jetzt den ersten Snapshot, und starten Sie danach die VM. Es entsteht das erste Redo-Log mit der Nummer 000001.
4. Alle Änderungen am Gastsystem werden ins Redo-Log mit der Nummer 000001 geschrieben, z.B. eine installierte Applikation oder Systemeinstellungen.
5. Wollen Sie einen Zwischenstand sichern, z.B. nach der erfolgreichen Installation eines Domänencontrollers in einer Test-VM, setzen Sie einfach einen neuen Snapshot im laufenden Betrieb (crash-konsistent), oder fahren Sie die VM vorher herunter (konsistent). Es entsteht ein Redo-Log mit der Nummer 000002.
6. Weitere Änderungen werden jetzt im Redo-Log mit der Nummer 000002 geschrieben und könnten später verworfen werden.
7. Sie können auf diese Weise weitere Redo-Logs erstellen.

Sie sollten sich alle Änderungen zwischen den Snapshots notieren, um später zu wissen, welcher Stand in welchem Redo-Log gespeichert ist. Sie können bei Bedarf folgendermaßen zu einem zurückliegenden Stand wechseln:

1. Beenden Sie die VM, und ersetzen Sie die virtuelle Platte über VM/SETTINGS mit dem gewünschten Redo-Log, z.B. der Nummer 000001.

**Nachfolger  
verwerfen**

2. Sind Sie zum Redo-Log zurückgekehrt, um die nachfolgenden Änderungen zu verwerfen, können Sie die VM bereits wieder starten und während des Hochfahrens im Verzeichnis manuell die nachfolgenden Redo-Logs und auch die Datei \*.vmsd löschen. Sonst können Sie später keine weiteren Snapshots setzen.

Wollen Sie dagegen später zu den nachfolgenden Redo-Logs wieder zurückkehren, müssen Sie vor dem Start der VM unbedingt einen neuen Snapshot setzen. Den *VMDB* Fehler ignorieren Sie dabei. Ohne erneuten Snapshot verändern Sie das Redo-Log, auf dem die Nachfolger aufsetzen. Die Nachfolger werden dadurch unbrauchbar.

**Nachfolger  
erhalten**

3. Starten Sie die VM neu. Sie arbeiten jetzt mit einem zurückliegenden Stand des Gastes. Das Redo-Log hat allerdings eine höhere Nummer, da VMware die Versionen einfach hochzählt. Das kann etwas unübersichtlich sein.
4. Um wieder zu einem Nachfolger zu gelangen, beenden Sie die VM und ändern die virtuelle Platte unter VM/SETTINGS auf ein anderes Redo-Log der Kette. Merken Sie sich dabei die Nummer des aktuell eingetragenen Redo-Logs, und löschen Sie es zusammen mit der Datei *\*.vmsd*. Das sorgt dafür, dass die Zählung wieder beim letzten Redo-Log ansetzt und nicht völlig durcheinanderkommt.

Theoretisch sind auch kompliziertere Snapshot-Bäume mit Verzweigungen möglich, aber dabei verliert man über die gesamte Verkettung der Redo-Logs zu schnell den Überblick. Beschränken Sie sich deshalb auf die Möglichkeit, in einem Zweig zwischen den gesicherten Zuständen zu wechseln. An den Lock-Dateien (*\*.lck*) im Verzeichnis der VM erkennen Sie deutlich, welche Redo-Logs bei gestarteter VM aktiv verwendet werden.



#### 4.7.2 VMSnap – das Tool von vmaschinen.de zur Verwaltung mehrerer Snapshots

Komfortabler wird die Verwaltung mehrerer Snapshots mit dem Tool VMSnap, das bereits in den früheren Versionen der VMware Workstation 4 und des GSX Servers multiple Snapshots bereitstellte, noch bevor das VMware selbst ermöglichte.

Mittlerweile habe ich das Tool an den VMware Server angepasst. Eine komfortable Integration in die grafische Benutzeroberfläche, wie unter VMware Workstation, kann das Tool allerdings nicht bieten. Es ist beispielsweise sehr nützlich, um bei Tests mehrere Zwischenstände zu erhalten. Einziger Nachteil – es ermöglicht noch keine Snapshots im laufenden Betrieb. Die VM muss bei einem Wechsel zwischen den Zuständen immer neu gestartet werden. Sie finden das Tool auf meiner Website [www.vmaschinen.de](http://www.vmaschinen.de).

**Komfortabel,  
aber nicht im  
laufenden  
Betrieb**

Ein großer Vorteil von VMSnap – es funktioniert auch mit dem VMware Player!



### 4.7.3 Linked Clones unter VMware Server – mehrere VMs auf einer Basisinstallation betreiben

Ebenfalls sehr nützlich ist die Möglichkeit, mehrere gleiche VMs von ein und derselben Basis-VM zu betreiben, ähnlich den linked Clones der VMware Workstation. Dadurch sparen Sie viel Zeit und Platz. Der Weg ähnelt der Verwendung mehrerer Redo-Logs und basiert auf dem gleichen Trick der schreibgeschützten virtuellen Platte:

1. Erstellen Sie eine Basis-VM mit einem sauber installierten Gastsystem und mit allen Einstellungen, Tools, Patches usw. Damit errichten Sie einen sauberen Grundzustand, der als Vorlage für darauf aufsetzende Klone dienen soll.
2. Versetzen Sie die virtuelle Platte dieser Vorlage-VM mit einem Schreibschutz, z.B. im Windows Explorer mittels rechter Maustaste und EIGENSCHAFTEN/SCHREIBGESCHÜTZT. Gegebenenfalls können Sie diese Behälterdatei an einen zentralen Ablageort für Ihre Muster-VMs kopieren. Das kann ein Ordner auf dem Host oder auch eine Netzwerkfreigabe sein.
3. Erstellen Sie eine neue VM im *Custom*-Modus. Legen Sie im Wizard keine neue virtuelle Platte an, sondern binden Sie mit *Use an existing virtual disk* die virtuelle Platte der Basis-VM ein. Sie müssen diese Platte vom zentralen Ablageort nicht kopieren, alle Klone werden gemeinsam darauf zugreifen.
4. Setzen Sie in der neu erstellten VM einen Snapshot, und starten Sie diese VM. Der Snapshot entkoppelt die Schreibzugriffe des Gastes von der zentralen Basisplatte. Dadurch können mehrere VMs die gleiche Vorlage verwenden. Ohne Snapshot könnte die VM mit der schreibgeschützten virtuellen Platte gar nicht starten.
5. Erstellen Sie weitere VMs auf die gleiche Art und Weise. Beachten Sie, dass die Performance darunter leiden kann, wenn sehr viele VMs die gleiche Basisplatte verwenden, vor allem wenn diese auf einer Netzwerkfreigabe liegt. Bis zu fünf Maschinen dürften aber keine Probleme bereiten.

#### Alle Klone funktionieren eigenständig

Alle VMs verwenden die gleiche Basisplatte. Jede VM verhält sich wie ein eigenständiger Gast. Wenn die Gäste in einem Netzwerk eingebunden sind, benötigen sie eigene IP-Adressen und Namen. Diese Anpassung müssen Sie in jedem Gast selbst vornehmen. Eine eigene MAC-Adresse haben sie durch das Neuerstellen der VMs automatisch. Gegebenenfalls sollten Sie NewSID oder Sysprep durchführen (siehe Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“). In jedem Gast funktionieren auch wieder mehrer Snapshots, wie weiter oben beschrieben. Auf diese Weise wurde z.B. die drei Server für die Cluster-Umgebung in Teil 2, Kapitel 8, erzeugt, andere Testumgebungen sind auf diese Weise mit wenigen Mausklicks ohne langwieriges Kopieren hergestellt.

#### 4.7.4 Erstellen einer eigenständigen VM ohne Snapshots aus einem der Redo-Logs

Irgendwann wollen Sie eine der Test-VMs mit mehreren Snapshots als Vorlage für eine produktive Maschine verwenden, oder Sie benötigen den aktuellen Zustand eines Snapshots als neue Basis-VM. Genauso werden Sie früher oder später einen der linked Clones gerne als unabhängige Maschine mit eigener vollständiger virtueller Platte betreiben wollen. Wie konsolidieren Sie die Zwischenstände auf eine einzige virtuelle Platte? Sie haben dazu zwei gängige Möglichkeiten:

- ▶ *Imaging-Tool im Gast* – Sie binden in die VM eine leere virtuelle Platte ein und starten die VM mit dem bootfähigen ISO-Image eines Imaging-Tools, z.B. Acronis oder BartPE mit Drive Snapshot. Jetzt übertragen Sie im Gast den Inhalt der vorhandenen Platte (und damit den Zustand aus allen Redo-Logs und der Basisplatte) auf die neue virtuelle Platte. Diese Platte kann dann unabhängig in einer neuen VM verwendet werden.
- ▶ *vmware-vdiskmanager* – Mit dem Tool *vmware-vdiskmanager.exe*, zu finden auf dem Host im Installationsverzeichnis von VMware, können Sie eine virtuelle Platte in eine andere konvertieren. Wenn Sie dabei als Quelle ein Redo-Log angeben, wird ebenfalls der Inhalt aller Logs und der Basisplatte, also der aktuelle Zustand, auf die neue virtuelle Platte übertragen. Vorteil – Sie benötigen kein Imaging-Tool. Verwenden Sie folgendes Kommando, und geben Sie als Quelle ein beliebiges Redo-Log mit dem gewünschten Zustand an:

```
vmware-vdiskmanager.exe -r meine_vPlatte-
xxxxxx.vmdk -t 0 meine_neue_vPlatte.vmdk
```

#### 4.7.5 Entfernen des Snapshot-Status beim VMware Server

Die im Menü des VMware Servers verfügbare Funktion REMOVE SNAPSHOT entfernt im Normalzustand, also ohne den beschriebenen Trick mit mehreren Redo-Logs, den Snapshot-Status und überführt eine VM wieder in den Zustand ohne Redo-Logs. Dabei überträgt VMware Server alle aufgelaufenen Änderungen des Snapshots immer auf die virtuelle Platte, es sei denn, Sie haben diese Änderungen vorher mittels Revert verworfen oder die virtuelle Platte ist schreibgeschützt.

Sollten Sie den beschriebenen Trick mit der schreibgeschützten virtuellen Platte verwenden, um mehrere Snapshots zu verwalten, dann können Sie den Snapshot nur manuell entfernen und alle Änderun-

gen verwerfen, indem Sie bei abgeschalteter VM folgende Dateien im Verzeichnis der VM löschen:

```
meine_vm.vmsd
meine_vPlatte-000001.vmdk
meine_vPlatte-000002.vmdk
usw.
```

Zusätzlich müssen Sie unter VM/SETTINGS/HARDWARE in der VM die vorhandene Festplatte entfernen (das letzte Redo-Log) und an deren Stelle wieder die Basisplatte eintragen, z.B. `meine_vPlatte.vmdk`. Vorher können Sie die Änderungen in den Redo-Logs bis zu einem gewünschten Stand auf eine andere Platte retten, wie das unter Abschnitt 4.7.4, „Erstellen einer eigenständigen VM ohne Snapshots aus einem der Redo-Logs“, beschrieben ist.

## 4.8 Snapshots per Skript mit vmrun.exe erstellen

VMware bietet die Möglichkeit, Snapshots auch von der Kommandozeile oder mittels Skript zu erstellen oder zu entfernen. Dazu können Sie das Programm `vmrun.exe` verwenden. Sie finden es auf dem Host im Ordner `C:\Programme\VMware\VMware VIX\vmrun.exe` oder bei der VMware Workstation unter `C:\Programme\VMware\VMware Workstation`.

Folgende Befehle setzen einen Snapshot und verwerfen ihn wieder:

```
vmrun.exe snapshot "pfad\zur\vm\config.vmx"
vmrun.exe deleteSnapshot "pfad\zur\vm\config.vmx"
```

Mit `revertToSnapshot` kehren Sie zum letzten Zustand der VM zurück. Die Befehle funktionieren auch über das LAN von einem Client aus:

```
vmrun.exe -h mein_host -u nutzer -p passwort snapshot
"pfad\zur\vm\config.vmx"
```

Weitere Infos zum Scripting finden Sie in Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“.

# 5 Datensicherung, Verfügbarkeit und Rechteverwaltung von VMs

Ein wichtiger Aspekt bei der Arbeit mit virtuellen Maschinen, vor allem im produktiven Bereich, ist die Sicherheit und die Verfügbarkeit der Systeme. Von einer Datensicherung sollten Sie jederzeit einen möglichst aktuellen Stand der Anwendungsdaten und auch der Konfiguration Ihrer Gastsysteme wiederherstellen können. Um es gar nicht erst so weit kommen zu lassen, ist einiges an Vorsorge zur Verfügbarkeit der Hosts und damit auch der virtuellen Maschinen zu treffen. Nicht zuletzt schützen Sie mit einer strukturierten Rechteverwaltung Ihre virtuelle Umgebung gegen Manipulationen und vor allem gegen versehentliches Löschen von VMs samt Inhalten.

## 5.1 Allgemeine Betrachtungen zur Datensicherung und Wiederherstellung

Eine funktionierende Datensicherung benötigt man grundsätzlich in zwei Szenarien, unabhängig davon, ob es sich um eine virtuelle Maschine oder um einen physischen Rechner handelt. Zum einen kann es zum kompletten Ausfall eines Systems durch Hardware-Fehler kommen oder zu Systemfehlern, z.B. Virenbefall oder fehlerhafte Updates. Katastrophen, wie Brände und Wasserschäden, gehören ebenfalls dazu. Weit häufiger ist dagegen ein Fehler an den Inhalten. Das versehentlich gelöschte Word-Dokument oder die Datenbank, die beim letzten Reorganisationslauf kompromittiert wurde, zählen zu dieser Kategorie genauso wie verschwundene E-Mails oder korrupte Exchange-Postfächer.

Die Wiederbelebung eines Komplettsystems, z.B. nach einem Serverausfall, stellt bei physischen Rechnern ein größeres Problem dar, da zuerst neue Hardware beschafft werden muss. Das System ist darauf neu zu installieren, inklusive aller Patches. Danach ist die gesamte Konfiguration wiederherzustellen, samt heikler Komponenten wie Active Directory oder Novell Directory Services. Die handlichste Methode kann ein aktuelles Image auf Sektorenbasis sein, erstellt mit Tools wie Acronis True Image, DriveSnapshot oder Ghost, das die Systempartition des Servers komplett enthält. Doch auch hier sind nach dem Zurückspielen des Images auf einen neuen physischen Rechner Probleme zu erwarten, z.B. mit fehlenden Treibern für die neue Ersatz-Hardware (siehe auch P2V-

**Disaster Recovery oder Wiederherstellung von Dateien**



Workshop in Teil 3, Kapitel 6). Außerdem beherrschen nicht alle Backup-Programme eine regelmäßige Sicherung auf Image-Basis.

Die Rücksicherung von einzelnen Dateien oder Datenbanken in ein laufendes System ist dagegen meist einfacher, vorausgesetzt die Sicherung wurde ordnungsgemäß durchgeführt. Alles in allem unterscheidet man also zwei verschiedene Ansätze der Datensicherung und Wiederherstellung:

- ▶ Die Systemkomplettsicherung mit der Möglichkeit, ein System von null auf wiederherzustellen, auch auf anderer Hardware.
- ▶ Die Sicherung auf Dateisystemebene zur Wiederherstellung einzelner Inhalte bei noch funktionierendem System.

## 5.2 Datensicherung und Wiederherstellung von virtuellen Maschinen

Virtuelle Maschinen unterscheiden sich in der Datensicherung prinzipiell nicht von anderen Computern. Sie können genau die gleiche Vorgehensweise verwenden, die Sie bereits von physischen Servern kennen, etwa die Bandsicherung über das LAN auf Dateisystemebene oder die Sicherung von Datenbanken mit speziellen Agenten in den Gästen.

Im Gegensatz zu physischen Rechnern bieten Ihnen virtuelle Maschinen zusätzlich ein sehr gängiges Mittel für eine Systemkomplettsicherung – das einfache Kopieren der Behälterdateien virtueller Platten. Beide Methoden, die herkömmliche Datensicherung und die Kopie auf Basis virtueller Platten, haben Vor- und Nachteile.

### 5.2.1 Herkömmliche Datensicherung über das LAN mit Agenten in den Gästen

#### Einzelne Dateien im Gast sichern

Die übliche Datensicherung erfolgt über die Installation eines Sicherungsagenten in den Gästen. Reine Dateisicherungen verzichten häufig auf einen Agenten, indem die Sicherungssoftware auf normale Dateifreigaben zugreift. Die Sicherung erfolgt von einem zentralen Backup-Server über das LAN.

#### Vorteile:

- ▶ *Die bewährte Datensicherung wird weiterverwendet* – Vorläufig müssen Sie nichts an der bisherigen Methode verändern. Sie können sich auf die erprobten Konzepte verlassen, bevor Sie mit der virtuellen Infrastruktur vertraut sind. Das ist sehr praktisch nach der Übernahme vorhandener physischer Maschinen in VMs (P2V).
- ▶ *Sicherung auf Dateiebene* – Einzelne Dateien im Gast können wie gewohnt gesichert und später wiederhergestellt werden.

- ▶ *Inkrementelle Sicherung* – Anhand des Archivbits oder der Änderungszeit können Sie nur geänderte Dateien sichern, das Datenaufkommen der Sicherung wird beträchtlich verringert.
- ▶ *Konsistente Onlinesicherung mit Agenten* – Für Exchange Server oder andere Datenbanken können im Gast spezielle Agenten installiert werden, die eine konsistente Online-Sicherung oder den Zugriff auf Inhalte, wie einzelne Postfächer, ermöglichen.

#### Nachteile:

- ▶ *Performanceprobleme* – Bei gleichzeitiger Sicherung vieler VMs auf demselben Host können Performanceprobleme auftreten, da die Netzwerkkarten und die Festplatten von vielen Gästen gemeinsam benutzt werden und bei der Datensicherung markante Lastspitzen auftreten.
- ▶ *Schwierige Komplettsicherung* – Eine Sicherung auf Image-Basis für schnelle und einfache Wiederherstellung des Gesamtsystems ist bei dieser herkömmlichen Sicherung nicht ohne weiteres möglich.

### 5.2.2 Datensicherung mit den speziellen Vorteilen virtueller Maschinen

Zusätzlich zu den bekannten Methoden bietet sich bei virtuellen Maschinen eine Sicherung der Behälterdateien der virtuellen Platten an. Diese können Sie auf dem Host einfach wegekopieren, etwa auf eine LAN-Freigabe, oder mit einer Datensicherungssoftware auf Band schreiben. Diese Art der Sicherung ist eine Besonderheit virtueller Maschinen.

**1:1-Kopie eines  
Gastsystems  
sichern**

#### Vorteile:

- ▶ *Einfacher als Image-Sicherung* – Die Sicherung entspricht dem Image eines physischen Servers, ist aber wesentlich einfacher zu erzeugen und wiederherzustellen. Unter bestimmten Voraussetzungen kann das Kopieren der virtuellen Platten sogar im laufenden Betrieb des Gastes erfolgen.
- ▶ *Komplettsicherung samt Systemkonfiguration* – In der Sicherung ist das lauffähige System samt Applikationen und Konfigurationseinstellungen enthalten.
- ▶ *Einfache Wiederherstellung* – Die gesicherten Dateien können auf jedem Rechner wiederhergestellt werden, auf dem die Virtualisierungssoftware läuft. Die Gäste starten sofort, ohne Treiberprobleme, weil die virtuelle Hardware immer gleich ist.
- ▶ *Sicherung von Systemständen (Wiederanlaufpunkte)* – Vor Patches oder Software-Upgrades können Sie sehr einfach alte Stände sichern. Mittels Snapshots (VMware) oder Differenzplatten (Microsoft) kann das sogar ohne komplettes Kopieren der gesamten virtuellen Platten erfolgen.

### Nachteile:

- ▶ *Keine direkte Rücksicherung einzelner Dateien* – Diese Methode ermöglicht nur eine umständliche Rücksicherung auf Dateiebene, der Inhalt der virtuellen Platte muss erst zugänglich gemacht werden, enthaltene Dateien müssen Sie dann manuell kopieren.
- ▶ *Große monolithische Dateien* – Bei jeder Sicherung müssen teilweise sehr große Dateien der virtuellen Platten am Stück bewegt werden. Ist eine dieser Dateien defekt, dann auch gleich der gesamte Inhalt.
- ▶ *Eingeschränktes inkrementelles Backup* – Es ist nicht ohne weiteres möglich, eine Sicherung anhand veränderter Inhalte im Dateisystem des Gastes anzufertigen, etwa anhand des Archivbits. Nur wenige Tools unter dem ESX Server ermöglichen inkrementelle Backups der virtuellen Platte mit so genannten Delta-Backups oder direktem Zugriff auf die virtuelle Platte (siehe „Besonderheiten beim VMware ESX Server 3 und etablierte Sicherungssoftware“ weiter hinten).

Bei der Methode einer Sicherung virtueller Platten existieren wiederum zwei grundsätzliche Möglichkeiten – das Kopieren kann im laufenden Betrieb einer VM erfolgen, oder der Gast wird vorher heruntergefahren. Auch hier gibt es Vorteile, Nachteile und Mittelwege.

### Cold Backup – konsistente Sicherung der virtuellen Platten bei heruntergefahrener VM

Einen wirklich sauberen Zustand des Gastsystems erhalten Sie mit einem so genannten *Cold Backup*, indem Sie die virtuelle Maschine herunterfahren und erst dann die virtuellen Platten kopieren. Das gewährleistet einen konsistenten Zustand des Inhaltes der Datenträger. Der Nachteil ist die Ausfallzeit der Maschine während des Kopiervorganges.

#### **Cold Backup garantiert Konsistenz**

Eine Methode, um die Ausfallzeit zu minimieren, ist das Anlegen eines Redo-Logs mittels Snapshot (VMware) oder einer Differenzplatte (Microsoft) nach dem Herunterfahren der VM. Die VM kann sofort neu gestartet werden, und die Platte lässt sich dann in Ruhe im laufenden Betrieb des Gastes sichern, weil der Inhalt nicht mehr geändert wird. Der Inhalt entspricht dem heruntergefahrenen Zustand.

Nach erfolgter Sicherung ist allerdings irgendwann das Redo-Log wieder mit der virtuellen Platte zu verschmelzen. Das kann teilweise, z.B. beim ESX Server, im laufenden Betrieb erfolgen, andere Maschinen müssen dazu erst wieder beendet werden. Das Verschmelzen nimmt je nach aufgelaufenen Änderungen längere Zeit in Anspruch. Um den gesamten Vorgang des Herunterfahrens, Snapshot-Setzens usw. zu automatisieren, ist einiges an Skriptarbeit notwendig, siehe dazu auch *Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“*.

## Crashkonsistente Sicherung der VM im laufenden Betrieb, so genannte Hot Backups

Um Ausfallzeiten zu vermeiden, werden die virtuellen Platten in der Praxis häufig kopiert, während das System läuft. Das wird als *Hot Backup* bezeichnet. Der ESX Server bietet spezielle Befehle, um im laufenden Betrieb ein Redo-Log zu erstellen, VMware Server kann einen Snapshot im laufenden Betrieb erstellen und erzeugt dabei ebenfalls ein Redo-Log. Microsoft ermöglicht eine Online-Sicherung mittels Volumenschattenkopien auf dem Host (siehe „Sicherung mit Volumenschattenkopien auf einem Windows Host oder mit SAN Snapshots auf einer LUN“).

Der Zustand der gesicherten virtuellen Platte ist bei einer solchen Online-Sicherung allerdings genau der gleiche wie nach einem Stromausfall eines physischen Rechners. Das liegt daran, dass viele Transaktionen von einem Betriebssystem nicht sofort geschrieben werden, sondern eine Weile im RAM gepuffert sind. Genauso können komplexe Transaktionen in einer Datenbank noch nicht abgeschlossen sein, z.B. wurden einige Sätze bereits mit einem neuen Index aktualisiert, andere abhängige Sätze dagegen noch nicht.

**Zustand des Dateisystems wie nach einem Stromausfall**

Ein Snapshot, bzw. ein im laufenden Betrieb erzeugtes Redo-Log, liefert immer eine Momentaufnahme. Erfolgt der Snapshot beispielsweise während einer Datenbanktransaktion im Gast, dann befinden sich Teile davon noch auf der virtuellen Platte, nachfolgende Teile bereits im neu entstandenen Redo-Log. Mit der virtuellen Platte sichern Sie also einen inkonsistenten Zustand. Greifen Sie später auf die kopierte virtuelle Platte zu, fehlt der dazu passende Laufzeitstatus samt RAM-Inhalt des Systems, als wäre die VM vorher abgestürzt.

Moderne transaktionsorientierte Dateisysteme, wie NTFS und viele Datenbanken mit Transaktionslogs oder Prüfpunktdateien, z.B. Exchange Server, bieten zwar einige Sicherheit bei Abstürzen. In den meisten Fällen wird die gesicherte Platte ohne Datenverlust funktionieren. Garantieren kann Ihnen das aber niemand, ein Restrisiko bleibt immer. Zumindest kann es beim Hochfahren inkonsistenter Datenbanken erst zu längeren Wiederherstellungsläufen kommen.

**Transaktionslogs können helfen**

Hot Backups werden in der Praxis trotzdem vielfach angewendet, auch von kommerziellen Sicherungsprodukten für den ESX Server. Aber es ist wie mit Systemabstürzen – es kann 99 Mal gut gehen, und ein einziges Mal ist die Datenbank kaputt. Dieses Risiko sollten Sie kennen. Letztendlich ist ein crashkonsistentes Hot Backup aber immer besser als gar keine Sicherung, wenn Sie die Server zum sicheren Cold Backup nie herunterfahren konnten.



Beim ESX Server 3 existiert die Möglichkeit, wenigstens das Dateisystem NTFS vor einer Datensicherung der virtuellen Platte durch die VMware Tools kurz anzuhalten und in einen konsistenten Zustand zu versetzen, lesen Sie dazu das Thema *VMware Consolidated Backup* in Teil 2, Kapitel 9. Mit Datenbanken, und genau hier liegt der Knackpunkt, funktioniert das bisher allerdings nur über Fremdherstellerprodukte, z.B. FalconStor Application Snapshot Director for VMware (<http://www.falconstor.com/>) oder mit Funktionen wie Volumenschattenkopien im Gast, wenn die entsprechende Datenbank unterstützt wird, etwa Exchange 2003 oder SQL Server. Eventuell können Sie Datenbanken im Gast vor dem Snapshot auch kurz herunterfahren und danach gleich wieder starten.

### Konsistente Sicherung des virtuellen Systems mit einem Snapshot im laufenden Betrieb

Wirklich konsistente Sicherungen durch Herunterfahren des Gastes sind in der Praxis oftmals nicht möglich, crashkonsistente Sicherungen dagegen immer mit einem Restrisiko behaftet. Eine Erweiterung der Methode gibt Ihnen zusätzliche Sicherheit.

#### **Virtuelle Platte und Laufzeitzustand des Gastes sichern**

Bei einem Snapshot im laufenden Betrieb speichert VMware auch den RAM-Inhalt und den Systemstatus der VM in Dateien. Der VMware Server macht das immer, beim ESX Server können Sie in einem Parameter angeben, ob er nur Redo-Logs erstellt oder auch den RAM-Inhalt sichert.

Dieser eingefrorene Gesamtzustand des Gastes ist in sich konsistent, da Sie die VM nach der Rücksicherung mittels Revert wieder in genau diesen Status versetzen können. Dabei ist es wichtig, die gesamte VM und nicht nur die virtuellen Platten wegzukopieren, um den RAM-Inhalt zum Zeitpunkt des Snapshots zu erhalten.

Diese Methode ist Ihre Rückversicherung für den Fall, dass eine Datenbank oder ein Dateisystem nach dem Wiederherstellen der kopierten virtuellen Platte defekt sein sollte. Wenn das der Fall ist, kopieren Sie die gesicherte VM vollständig zurück (also nicht nur die virtuellen Platten) und vollziehen ein Revert zu dem eingefrorenen Zustand zum Zeitpunkt des Snapshots. Die VM erwacht und beendet offene Transaktionen, als wäre nichts gewesen. Jetzt fahren Sie das System nachträglich geordnet herunter. Sie verschieben damit den Zeitpunkt des Herunterfahrens sozusagen nach hinten. Auf diese Weise erhalten Sie im Notfall einen sauberen Zustand des Dateisystems samt Datenbanken im Gast.

Der Vorteil gegenüber dem Herunterfahren beim Cold Backup ist, dass die VM während der Snapshot-Sicherung ohne Unterbrechung weiterarbeitet. Und der Vorteil gegenüber einer reinen Plattenkopie ohne Systemstatus und RAM ist der zusätzlich eingefrorene konsistente Laufzeitzustand für den Notfall.

Unter Microsoft Virtual Server funktioniert diese Methode nur mit Suspend, dann Schattenkopie, dann Resume – der Gast wird also beim Sichern kurz unterbrochen.

Die Wiederherstellung einer laufenden VM funktioniert auf einem Host mit anderem CPU-Modell nicht immer, da der Status des Gastes dort eventuell nicht wiederhergestellt werden kann. Es bleiben dann aber wenigstens die gesicherten virtuellen Platten, wenn auch nur im crashkonsistenten Zustand.



### **Sicherung mit Volumenschattenkopien auf einem Windows Host oder mit SAN Snapshots auf einer LUN**

Eine Erweiterung der Sicherungsmöglichkeiten bieten die so genannten Volumenschattenkopien mit den *Volume Shadow Copy Services* (VSS) von Windows Server 2003. Diese ermöglichen eine Art Snapshot des Dateisystems NTFS auf einem Windows Server, in unserem Falle auf dem Host. Dabei wird der momentane Zustand eingefroren und vor nachfolgenden Änderungen geschützt. Das Prinzip ist ähnlich wie bei den Redo-Logs oder Differenzplatten einer VM. Windows verwaltet verschiedene Versionen des Dateisystems, indem es geänderte Sektoren überwacht und in spezielle reservierte Bereiche schreibt. Zurückliegende Versionen einer Datei lassen sich einfach wiederherstellen. Damit können Sie auf einem Windows-Host beispielsweise folgende Sicherungsmethode verwenden:

1. Herunterfahren oder schnelleres Suspend der virtuellen Maschine, damit die virtuellen Platten nicht mehr in Verwendung sind und der RAM in eine Datei gespeichert wird.
2. Anlegen einer Volumenschattenkopie des NTFS-Dateisystems auf dem Host. Das geschieht innerhalb von Sekunden.
3. Neustart oder Resume der virtuellen Maschine.
4. Die virtuellen Platten, gegebenenfalls das gesamte Verzeichnis der VM mitsamt Suspend-Status und RAM-Inhalt, können jetzt gesichert werden, da der Zustand vor dem Zeitpunkt der Schattenkopie nicht mehr verändert wird.

Die Schattenkopie funktioniert im Prinzip auch ohne das Herunterfahren des Gastes direkt im laufenden Betrieb. Das geht in den meisten Fällen gut, es bleibt aber wieder das erwähnte Restrisiko von crashkonsistenten Sicherungen. Bei kritischen Datenbanken im Gast sollten diese vor der Schattenkopie dann wenigstens kurz beendet werden, das kann durch Skripte erfolgen.



Im *Volume Shadow Copy Service SDK 7.2* existiert eine Datei *vshadow.exe*, mit der sich das Anlegen der Schattenkopie in einem Skript automatisieren lässt (siehe Linkliste in *Teil 3, Kapitel 7*).

Mit einem Skript könnte die Schattenkopie sogar in einem Windows-Gastsystem vor der Sicherung der VM ausgelöst werden. Der Vorteil darin ist, dass die Volumenschattenkopien mit einigen Anwendungen kompatibel sind und einen konsistenten Zustand gewährleisten können, z.B. bei NTFS, Exchange Server 2003 oder Microsoft SQL Server. Das Programm *psexec.exe* von *www.sysinternals.com*, zum Starten von Skripten auf fernen Rechnern, also auch in VMs, finden Sie ebenfalls in der Linkliste von *Teil 3, Kapitel 7*.

#### **SAN-Snapshots auf LUN-Basis**

Viele SAN-Speichergeräte bieten als Zusatzoptionen ähnliche Funktionen zum Einfrieren von Versionen des Dateisystems auf einer LUN an. Diese werden je nach Hersteller auch *SAN-Snapshots*, *Flash Copy* o.Ä. genannt. Der Effekt ist der gleiche wie bei einer Schattenkopie, allerdings ist die Funktion unabhängig vom Betriebssystem bzw. vom Dateisystem, das auf der LUN untergebracht ist, es funktioniert also auch mit älteren Windows-Versionen, Linux oder VMFS vom ESX Server.

### **5.2.3 Konzepte zur Sicherung virtueller Maschinen – Hot, Cold oder Agenten?**

#### **Hot Backup, Cold Backup oder Agenten in den Gästen?**

Sie sehen, die Sicherung virtueller Maschinen wirft bei genauer Betrachtung einige Probleme auf. Aus den bisherigen Überlegungen lassen sich Aussagen ableiten, wie Sie Ihre virtuellen Maschinen am besten sichern sollten. Ein pauschales Konzept gibt es nicht, es hängt stark von Ihren Anwendungen ab. Betreiben Sie in virtuellen Maschinen nur Dienste-Server ohne großes Datenaufkommen, etwa Lizenzserver, Intranetserver o.Ä., dann ist eine tägliche Sicherung der kompletten virtuellen Systemplatten als Dateien praktisch, dadurch sichern Sie neben den Daten auch die aktuelle Konfiguration immer mit. Kommen dagegen auch virtuelle Dateiserver oder Datenbankserver dazu, ist eine Kombination aus allen Methoden der beste Weg.

#### **Wichtige Grundsätze für die Datensicherung**

Einige wichtige Grundsätze sollten Sie beachten:

- ▶ Trennen Sie Systemdatenträger und Datenplatten der Gäste. Die Behälterdateien der Systemplatten lassen sich dadurch einfacher sichern, da sie meist unter 10 GB bleiben.
- ▶ Sichern Sie regelmäßig, mindestens wöchentlich, die virtuellen Platten mit dem Gastbetriebssystem für den Fall der kompletten Systemwiederherstellung einer VM. Vor der Sicherung sollten Sie die VM skriptgesteuert herunterfahren, z.B. am Wochenende, um einen wirklich konsistenten Zustand zu erhalten.

In der Praxis ist selbst ein crashkonsistentes Backup besser als gar keines. Wenn Sie keine Gelegenheit finden, die VMs zu beenden, erstellen Sie wenigstens Kopien der virtuellen Platten im laufenden Betrieb mit Redo-Logs oder mit Volumenschattenkopien. In den meisten Fällen funktionieren die Sicherungen nach dem Zurückspielen.



- ▶ Wollen Sie ganz sichergehen, dann erstellen Sie täglich (oder auch häufiger) Sicherungen auf Dateiebene in den Gastsystemen über das Netzwerk mit den üblichen Methoden. Im Gastsystem können Sie alle Sicherungsmethoden nutzen wie auf einem physischen Rechner. Vor allem das Zurückspielen einzelner Dateien ist mit der gewohnten Sicherungssoftware unkompliziert möglich.
- ▶ Kritische Anwendungen, wie Datenbanken, Exchange Server usw., können nur durch spezielle Agenten oder unterstützte Methoden in den Gastsystemen in einem garantiert konsistenten Zustand gesichert werden. Oder Sie fahren die Anwendung im Gast herunter. In der Praxis werden trotzdem sehr häufig Hot Backups durchgeführt, da transaktionsorientierte Datenbanken nicht mehr so sensibel auf Abstürze reagieren wie eine Access-Datenbank. Sie sollten das Risiko aber kennen.
- ▶ Wenn Sie Ihre gesamte VM ausschließlich auf Basis der Behälterdateien virtueller Platten sichern wollen und auf Agenten in den Gästen verzichten, dann können Sie das Risiko minimieren, indem Sie Datenbankanwendungen im Gast vor dem Kopieren der virtuellen Platten bzw. vor dem Anlegen eines Redo-Logs kurz beenden. Das kann beispielsweise mit dem Befehl *net stop* im Gast erfolgen. Beispiele für Skripte finden Sie in *Teil 3, Kapitel 7*. Dateisysteme wie NTFS oder ext3 kommen sehr gut auch ohne Herunterfahren aus.
- ▶ Als Notfallversicherung können Sie den Systemstatus und RAM Inhalt der VM mitsichern, um die VM nach der Wiederherstellung nachträglich sauber herunterfahren zu können, sollten Datenbanken oder Dateisysteme auf den kopierten Platten defekt sein.
- ▶ Der Sicherungsserver mit der Sicherungshardware (Bandlaufwerke usw.) sollte ein separates Gerät sein. Damit sind Sie bei Wiederherstellungsvorgängen unabhängig von der Host-Hardware. Verwenden Sie deshalb möglichst keine Streamer auf dem Host oder etwa in den Gästen (obwohl das mit *Raw Device Mapping* möglich wäre – siehe *Teil 3, Kapitel 3*).

Testen Sie unbedingt Ihr Sicherungskonzept! Gerade in virtuellen Umgebungen ist es besonders einfach, eine Sicherung in einer Testumgebung zurückzuspielen und das Ergebnis zu begutachten. Nur so sind Sie auf den Ernstfall gut vorbereitet.





### Besondere Probleme bei virtuellen Domänencontrollern

Ein besonderes Problem stellen mehrere Domänencontroller dar. Haben Sie nur einen Domänencontroller, dann können Sie einen alten Stand problemlos von einer Kopie der VM wiederherstellen. Bei mehreren Controllern führt das aber zu Fehlern in der Synchronisation.

#### Systemstatus separat sichern

Sichern Sie immer den Systemstatus mit einem Sicherungsprogramm im Gast, im einfachsten Falle mit NTBackup. Haben Sie einen Domänencontroller von einer älteren Kopie der VM wiederhergestellt, spielen Sie erst die aktuellste Sicherung des Systemstatus wieder auf, bevor Sie ihn ans Netzwerk anschließen, ansonsten ist er mit den anderen Domänencontrollern im Netzwerk nicht mehr synchron. Siehe auch folgende Artikel in der Microsoft Knowlegedbase:

*Considerations when hosting domain controller in virtual environments:*

<http://support.microsoft.com/kb/888794/en-us>

*How to detect and recover from a USN rollback:*

<http://support.microsoft.com/default.aspx?scid=kb;en-us;885875>

<http://support.microsoft.com/default.aspx?scid=kb;en-us;875495>

Auf einem Domänencontroller sollte übrigens grundsätzlich keine Anwendungssoftware laufen. Das ist in virtuellen Umgebungen, in denen es auf eine Maschine mehr oder weniger nicht so sehr ankommt, auch nicht notwendig. Damit wäre das neue Aufsetzen eines Domänencontrollers, anstelle einer Rücksicherung, ebenfalls kein Problem, wenn mehrere vorhanden sind.

### 5.2.4 Beispiele zur Sicherung und Wiederherstellung unter VMware Server

In diesem Abschnitt finden Sie ein paar Anregungen, um VMs komplett auf Basis der virtuellen Platten auf dem VMware Server zu sichern. Beispiele zum Scripting, z.B. Beenden und Starten von VMs oder Setzen von Snapshots, finden Sie imn *Teil 3, Kapitel 7*, und auf der Buch-CD.

#### ESX Server und Virtual Server

Für den ESX Server empfiehlt sich professionelle Software (siehe „Besonderheiten beim VMware ESX Server 3 und etablierte Sicherungssoftware“).

Für Microsoft Virtual Server eignen sich die beschriebenen Volumenschattenkopien (siehe „Sicherung mit Volumenschattenkopien auf einem Windows Host oder mit SAN Snapshots auf einer LUN“).

### Als Vorbereitung Snapshots im Hintergrund einschalten

Als Vorbemerkung muss ich Sie gleich auf ein Problem aufmerksam machen – VMware Server kann keine Redo-Logs im laufenden Betrieb konsolidieren, also deren Inhalt wieder mit der Basisplatte

verschmelzen (siehe „Redo-Logs wieder entfernen und konsolidieren“ weiter hinten). Die VM muss dazu kurz heruntergefahren bzw. in den Suspend-Modus gebracht werden.

Die Ausfallzeit zum Entfernen der Redo-Logs, meist wenige Minuten, müssen Sie allerdings in Bezug auf die Sicherungszeit betrachten. Das Kopieren einer 5 Gigabyte großen VM über Gigabit Ethernet dauert nur ein paar Minuten. Die VM kann also kurz heruntergefahren werden, Sie sparen sich das kompliziertere Hot Backup. Dagegen dauert das Kopieren von 100 GB großen Datenplatten eines Servers wesentlich länger als das erforderliche Konsolidieren der Redo-Logs nach dem Backup. Hier lohnt sich also das Hot Backup.

Die hier vorgestellten Methoden eignen sich beispielsweise auch dazu, um von einem produktiven System im laufenden Betrieb eine Kopie für die Pilotumgebung zu erstellen.



Schalten Sie als Vorbereitung auf dem VMware Server Host die Funktion zur Hintergrundisierung von Snapshots ein, zu finden unter HOST/SETTINGS/PRIORITY/TAKE AND RESTORE SNAPSHOTS IN THE BACKGROUND. Jede VM, für welche die Einstellung wirken soll, muss danach einmal neu gestartet werden. Ab jetzt erfolgt das Sichern eines Snapshots, vor allem des RAM-Inhaltes, ohne Unterbrechung des Gastes im Hintergrund, es kann aber eine Zeit lang die Leistung etwas beeinträchtigen.

### Crashkonsistente Sicherung mit Snapshot beim VMware Server

Leider funktioniert bei der folgenden einfachen Methode das Wiederherstellen des Systemstatus nicht, wenn Sie die VM im laufenden Betrieb kopieren. Das liegt daran, dass VMware eine Datei im Zugriff hat, die sich dadurch nicht richtig kopieren und später beim Revert nicht wiederherstellen lässt.

**Einfaches Kopieren der Platten ohne RAM**

Also können Sie nur die virtuellen Platten sichern, und die sind dann crashkonsistent. Wenn Sie allerdings vor dem Snapshot Datenbankdienste im Gast kurz beenden, genügt diese Sicherung vollauf:

1. Sie können im Gast gegebenenfalls über ein Skript Dienste wie Exchange Server kurz beenden. Dazu kann beispielsweise das Tool *psexec.exe* von <http://www.sysinternals.com/> dienen. Sie können die VM natürlich auch ganz herunterfahren.
2. Setzen Sie einen Snapshot im laufenden Betrieb. Das Erstellen des Redo-Logs geht sehr schnell, der Gast arbeitet sofort weiter. Der RAM-Inhalt wird im Hintergrund gesichert. Der Snapshot kann mittels *vmrun.exe* aus dem Verzeichnis *C:\Programme\VMware\VMware VIX* des Hosts automatisiert erfolgen.

3. Sie können sofort, noch während der Hintergrundicherung des RAM, die Dienste im Gast wieder starten, die Sie eventuell vor dem Snapshot beendet haben, beispielsweise Exchange Server. Der Gast schreibt ja bereits in die Redo-Logs. Das minimiert die Ausfallzeit.
4. Jetzt können Sie die virtuellen Platten wegkopieren. Das Dateisystem im Gast ist crashkonsistent, was meist keine Probleme bereitet. Haben Sie Datenbanken vor dem Snapshot kurz heruntergefahren, sind diese konsistent.

### Konsistente Sicherung mit Snapshot beim VMware Server

#### Sicherung mit Systemstatus und RAM

Mit einem kleinen Trick können Sie das Manko der oben beschriebenen Methode umgehen und auch einen wiederherstellbaren Systemstatus sichern. In diesem Falle müssen Datenbanken nicht unbedingt beendet werden, weil Sie als Rückversicherung den Systemstatus der VM haben:

1. Setzen Sie einen Snapshot im laufenden Betrieb. Die VM arbeitet weiter, eventuell mit etwas eingeschränkter Leistung. Warten Sie, bis der RAM im Hintergrund gespeichert ist. Das ist nur unten in der Statusleiste zu sehen, warten Sie in Skripten einfach 15 Minuten. Die Zeitdauer hängt von der Menge des zugewiesenen Speichers ab.
2. Bringen Sie die VM kurz in den Suspend-Modus. Das ist der Trick, damit die Snapshot-Datei \*.vmsn einmal ordentlich geschlossen wird. Dadurch lässt sich die Kopie später und mit einem Revert der Systemstatus wiederherstellen.
3. Starten Sie die VM aus dem Suspend-Modus sofort wieder mittels Resume. Suspend und Resume gehen sehr schnell, mit minimaler Ausfallzeit des Gastes. LAN-Clients bemerken meistens keinen Ausfall. Kopieren müssen Sie noch nichts, es genügt das kurze Suspend.
4. Jetzt können Sie bei laufendem Gast das Verzeichnis der VM kopieren. Diese Kopie lässt sich später mittels Revert wieder auf den Zeitpunkt der Sicherung zurücksetzen, sie hat einen konsistenten Zustand. Der Systemstatus ist eine zusätzliche Absicherung für den Fall, dass die einfache Kopie der virtuellen Platte später nicht funktionieren sollte.

Kopieren Sie mindestens folgende Dateien:

```
meine_vm.vmx
meine_vm.vmsd
meine_vm-SnapshotXX.vmsn
meine_vm-SnapshotXX.vmem
meine_vm_plattel.vmdk
meine_vm_plattel-XXXXXX.vmdk
```

Folgende Dateien benötigen Sie nicht:

```
*.lck
meine_vm.vmsx (Suspend-Datei)
meine_vm.vmem (Suspend-Datei)
```

Dateien in folgendem Format sind geöffnet und führen eventuell zum Abbruch der Kopieraktion. Um das gesamte Verzeichnis zu kopieren, verwenden Sie deshalb z.B. *xcopy* mit dem Schalter */c*. Die Dateien (eine pro VM) können folgendermaßen aussehen:

```
564d3538-a6f7-8173-0cac-9a08ba1ff8e7.vmem
(Beispiel)
```

### Redo-Logs wieder entfernen und konsolidieren

Ein Problem bei beiden Sicherungsmethoden ist die schon erwähnte Konsolidierung des Redo-Log nach erfolgtem Kopiervorgang. Beim VMware Server funktioniert das leider nicht ohne Unterbrechung des Gastsystems, gehen Sie folgendermaßen vor:

1. Bringen Sie die VM in den Suspend-Modus, eventuell mit einem Skript.
2. Führen Sie REMOVE SNAPSHOT aus. Das geht leider nicht im laufenden Betrieb. Sie können *vmrun.exe* verwenden.
3. Jetzt werden die Änderungen im Redo-Log zur virtuellen Platte addiert. Die Zeitdauer dieser Aktion ist abhängig vom Inhalt des Logs. Das ist das größte Problem der Snapshot-Sicherung beim VMware Server, der ESX Server kann das im laufenden Betrieb. Trotzdem ist die Ausfallzeit geringer als wenn man eine komplette Kopie der VM im abgeschalteten Zustand erstellen würde.

Wenn der Pfad der Redo-Logs auf einem anderen Datenträger liegt als die virtuelle Platte, geht der Vorgang schneller. Einstellen können Sie das im Gast unter VM/SETTINGS/OPTIONS/GENERAL/WORKING DIRECTORY.



4. Nach dem Vorgang können Sie den Gast sofort wieder starten (Resume). Er arbeitet jetzt wieder direkt auf der virtuellen Platte bis zur nächsten Snapshot-Sicherung.

Sie können das Redo-Log auch bis zur nächsten Sicherung belassen. Der Snapshot der nächsten Sicherung würde es dann konsolidieren und ein neues Log anlegen. Allerdings dauert das wesentlich länger, weil sich das Log mittlerweile gefüllt hat.

### Eine Snapshot-Sicherung oder Schattenkopie wiederherstellen

**VM vorerst nicht  
ans Netzwerk  
anschießen**

Bei der Rücksicherung genügt es oft, die kopierte virtuelle Platte wieder in eine VM einzubinden. Sind Datenbanken oder Dateisysteme durch das Hot Backup defekt, ist folgende Vorgehensweise Ihre Versicherung. Beachten Sie, dass die VM nach dem Erwachen durch Revert in einem Zustand läuft, der lange zurückliegen kann. Die VM sollte vorläufig keinen Kontakt zum Netzwerk haben. Sehr kritisch sind hier Domänencontroller. Folgende Vorgehensweise bietet sich an:

1. Stellen Sie das komplette Verzeichnis der gesicherten VM von der Datensicherung auf einem Host wieder her.
2. Sorgen Sie dafür, dass die VM nach dem Erwachen keinen Kontakt zum Netzwerk hat. Entweder ziehen Sie am Host das LAN-Kabel ab oder isolieren das virtuelle Netzwerk, an dem der Host bei der Sicherung hing und in dem er wieder erwachen wird.
3. Setzen Sie die zurückkopierte VM mit einem Revert auf den aktuellen Zustand zum Zeitpunkt der Sicherung zurück. Der Gast erwacht, beendet alle Transaktionen und bemerkt nur, dass er plötzlich den Kontakt zum LAN verloren hat.
4. Sie können die Maschine herunterfahren, das Dateisystem im Gast befindet sich dadurch nachträglich in einem konsistenten Zustand. Sie können auch gleich die wiederherzustellenden Dateien aus dem laufenden Gast kopieren.
5. Wollen Sie die gesamte VM wiederherstellen (Disaster Recovery) und die Sicherung der virtuellen Platten liegt länger zurück, dann spielen Sie nach dem Revert gegebenenfalls die aktuellsten Datensicherungen auf Dateibasis in den Gast zurück, bevor Sie ihn wieder ans Netz nehmen.

### Einzelne Dateien aus gesicherten virtuellen Platten wiederherstellen

Um einzelne Dateien aus einer kopierten virtuellen Platte wiederherzustellen, haben Sie mehrere Möglichkeiten:

- Binden Sie eine gesicherte Platte in eine vorhandene VM ein, und kopieren Sie die benötigten Inhalte aus diesem Gast über das Netzwerk zum Ziel.
- Binden Sie die virtuelle Platte mittels *VMware DiskMount* (VMware) oder *WinImage* (Microsoft) am Host ein, und kopieren Sie die benötigten Inhalte (siehe auch Teil 3, Kapitel 3).
- Bei einer Snapshot-Sicherung der gesamten VM haben Sie sofort Zugriff auf den Inhalt der virtuellen Platte, sobald die wiederhergestellte VM nach dem Revert läuft.

## Komplette VMs aus einzelnen gesicherten Platten wiederherstellen

Wenn Sie nur die virtuellen Platten einer VM sichern, dann genügt das auch für den Fall einer kompletten Wiederherstellung. Sie konfigurieren einfach eine neue VM und binden die gesicherten Platten ein, anstelle eine neue leere Platte zu erstellen. Die Konfigurationsdatei ist für einen Gast relativ unwichtig und kann neu erstellt werden, das Herzstück ist die virtuelle Platte.

## Besonderheiten beim VMware ESX Server 3 und etablierte Sicherungssoftware

Der VMware ESX Server 3 bietet eine ganze Reihe Besonderheiten in Sachen Datensicherung. Zum einen existieren Befehle, um Redo-Logs im laufenden Betrieb zu erstellen und wieder mit der virtuellen Platte zu verschmelzen, z.B. *vmsnap.pl* beim ESX Server 2 bzw. *vmware-cmd* bei ESX Server 3 (siehe *Teil 2, Kapitel 9*). Zusätzlich können Sie mit *VMware Consolidated Backup* im laufenden Betrieb einer VM eine konsistente Datensicherung sogar auf Dateiebene des Gastsystems durchführen, die nicht über das LAN, sondern direkt über das Speichernetzwerk abläuft (siehe Abschnitt *VMware Consolidated Backup* in *Teil 2, Kapitel 9*).

**Redo-Logs im laufenden Betrieb anlegen und entfernen**

Zur Sicherung von VMs auf dem ESX Server existiert einiges an Fremdanbieter-Software, die es ermöglicht, über die Service-Konsole automatisch komplette VMs zu sichern. Alle Lösungen machen Gebrauch von Redo-Logs, um Sicherungen im laufenden Betrieb zu erstellen. Folgende Produkte sind für den ESX Server etabliert:

- ▶ Von der Firma Vizioncore stammen u.a. die Programme *esxRanger* zu komfortablen Sicherung virtueller Maschinen und *esxReplicator* zur Replikation laufender VMs auf einem anderen Host. Das kostenlose Paket *esxBasics* enthält eine abgespeckte Version von *esxRanger*:  
<http://www.vizioncore.com/>
- ▶ Die Firma PHD Consulting stellt *esXpress* bereit, das ebenfalls eine komfortable Sicherung virtueller Maschinen im laufenden Betrieb ermöglicht. Es existiert auch eine kostenlose Variante. Sehr interessant ist die Abhandlung zum Thema Hot Backup auf der Webseite:  
<http://www.esxpress.com/hottest.php>
- ▶ Die Firma aeXia bietet mit Ihrer *Virtual Solution Box (VSB)* umfangreiche Datensicherung und Replikation virtueller Maschinen:  
[http://www.aexia.ch/produkte\\_vsb.htm](http://www.aexia.ch/produkte_vsb.htm)
- ▶ Weiterhin stellt Massimiliano Daneri auf seiner Webseite ein kostenloses Backup-Skript bereit, das den Vorgang der Redo-Log-Erstellung und Verschmelzung sowie des Kopierens der VMs auf dem ESX Server 2 automatisiert:  
<http://www.vmts.net/vmbk.htm>

### 5.2.5 Archivierung von Testsystemen oder Legacy-VMs als Teilaspekt der Datensicherung

Ein Teilaspekt der Datensicherung ist die Archivierung virtueller Maschinen. Vor allem in Testumgebungen wollen Sie Ihre Vorlagen, aber auch Kundenkonfigurationen längere Zeit abrufbar aufheben. Ebenso kann es sehr nützlich sein, den alten Fibu Server zu virtualisieren und als VM zu archivieren. So steht er auch später auf beliebiger Hardware als lauffähiges System bereit, etwa um Daten zu überprüfen, die eventuell nicht ordnungsgemäß ins neue System übernommen wurden.

#### Platzsparen in archivierten VMs

Einige Vorbereitung der Gäste auf das Archivieren spart Ihnen Platz und Zeit beim Kopieren. Die Liste reicht vom Aufräumen des Dateisystems im Gast bis zum Aufteilen virtueller Platten in handliche 2-GB-Streifen. Diese Vorgehensweise ist beim Klonen, Weitergeben und Archivieren immer die gleiche, Sie finden sie in *Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“*.

### 5.2.6 Sicherung des Host-Systems

Neben der Sicherung der virtuellen Maschinen kann auch das Host-System gesichert werden, etwa um es bei einem Hardware-Ausfall wiederherzustellen. Diese Sicherung ist allerdings wesentlich unkritischer als die Sicherung der Gäste. Natürlich sollte die Systempartition immer von der Partition für die virtuellen Maschinen getrennt sein. Bei externem Speicher und mehreren Hosts ist ein Host-Ausfall noch unproblematischer.

#### Schnelle Neuinstallation

Auf dem Host sollten grundsätzlich keine Anwendungen laufen. Das System dient ausschließlich als Basis für die Virtualisierungssoftware. Beim ESX Server ist das systembedingt nicht anders möglich. Ein ESX Server kann in wenigen Minuten wieder neu installiert werden, die meisten Einstellungen liegen im Virtual Center. Auch die Windows-Basis samt Virtualisierungssoftware von VMware Server oder Microsoft Virtual Server ist recht schnell wieder erstellt. Ein wichtiger Punkt ist die Dokumentation von Einstellungen wie Netzwerkkonfigurationen oder Rechten. Empfehlenswert ist eine regelmäßige Sicherung der Systemplatte des Hosts mit einem Image.

#### Wiederherstellung eines ausgefallenen Hosts

Beim Totalausfall eines Hosts würden Sie dann folgendermaßen vorgehen:

1. Wiederherstellung des Host-Systems auf neuer Hardware durch Neuinstallation oder durch Zurückspielen des Images. Gegebenenfalls Neuinstallation der Virtualisierungssoftware.

2. Zurückspielen der gesicherten virtuellen Maschinen, zumindest der virtuellen Systemplatten der Gäste. Andere Möglichkeiten sind Umbau des Plattenstapels aus dem defekten Gerät oder Anbindung an die gleiche LUN im externen Speicher.
3. Gegebenenfalls Neuerstellung virtueller Maschinen und Einbinden der vorhandenen virtuellen Platten oder einfaches Aufnehmen der komplett gesicherten VMs in die Favoriten, Inventory usw. des Virtualisierers.
4. Eventuell zusätzliche Datenrücksicherung in die wiederhergestellten Gastsysteme von der aktuellsten Sicherung auf Dateisystemebene mit Agenten. Das ist nur notwendig, wenn die VMs von älteren Sicherungen wiederhergestellt wurden.

Verwenden Sie externen Speicher, z.B. ein SAN oder NAS, dann ist beim Ausfall eines Hosts keinerlei Rücksicherung virtueller Maschinen notwendig, sie können sofort auf einem anderen Host neu gestartet werden. Jede virtuelle Maschine ist zwar durch den Ausfall des Hosts abgestürzt, enthält aber den aktuellsten Datenbestand.

In produktiven Umgebungen sollten Sie die Wirtsrechner auf jeden Fall redundant auslegen, so dass im Notfall andere Hosts alle VMs des ausgefallenen Gerätes übernehmen können. Auch wenn kurzzeitig die Leistung darunter leidet, ist doch wenigstens der Betrieb gewährleistet – das ist gleich eine schöne Überleitung zum nächsten Thema.



## 5.3 Verfügbarkeit virtueller Maschinen und der Host-Systeme

Vorbeugen ist besser als Wiederherstellen! Trotz ausgeklügelter Datensicherung und mehrfach erprobter Rücksicherung – am schönsten ist es doch, wenn alles läuft. Ausfallsicherheit ist eines der wichtigsten Themen im produktiven Betrieb virtueller Maschinen.

### 5.3.1 Allgemeine Betrachtungen zur Ausfallsicherheit

Wie bereits die Datensicherung, so kann das Thema Verfügbarkeit und Ausfallsicherheit in mehrere Teilaspekte gegliedert werden:

- *Hardware-Ausfall des Hosts* – Der Host kann durch eine kaputte Komponente unvorhergesehen ausfallen. Bereits der Ausfall einzelner Komponenten, etwa Netzkarten oder Host Bus Adapter, können fatale Folgen haben. Aber auch geplante Wartungsarbeiten werden zum Problem, da es in vielen Umgebungen heute



kaum noch möglich ist, einen Server für eine Stunde außer Betrieb zu nehmen. Da auf einem Host gleich mehrere Serverinstanzen laufen, verschärft sich das Problem.

- ▶ *Hardware-Ausfall beteiligter Komponenten* – Selbst wenn der Host ordnungsgemäß arbeitet, nützt das wenig, wenn eine wichtige zentrale Komponente ausfällt, etwa der LAN-Switch oder gar der externe Speicher. Zentrale Komponenten sind hier LAN- und Fibre-Channel-Switches sowie die Speichersysteme, etwa SAN oder NAS und natürlich die Stromversorgung.
- ▶ *Ausfall einer kompletten VM* – Neben der Hardware können auch einzelne Gäste ausfallen. Eine VM kann beispielsweise versehentlich komplett gelöscht oder heruntergefahren werden. Genauso kann das Betriebssystem in der VM abstürzen.
- ▶ *Ausfall einer Applikation in einer VM* – Am Ende kann auch nur eine bestimmte Applikation in einem Gast ausfallen, etwa der Informationsspeicher eines Exchange Servers durch Platzmangel oder eine Datenbankapplikation durch Absturz.

**Cluster automatisieren das Fail-over**

Der Ausfall von Applikationen kann durch Cluster-Konfigurationen abgefangen werden, die spezielle Anwendungen in den Gästen überwachen und bei Bedarf auf andere Gäste übertragen. Der Ausfall einzelner VMs kann ebenfalls durch Cluster-Lösungen abgefangen werden, die entweder einzelne Applikationen oder nur den Gast als Einheit überwachen, etwa mittels Heartbeat-Signalen der VMware Tools. Letztendlich können so genannte Host-Cluster den Host überwachen und alle VMs bei Bedarf auf anderen Maschinen neu starten.

Das Thema Cluster-Lösungen wird von *Teil 2, Kapitel 8*, sehr praxisorientiert behandelt. Beachten Sie auch das *Teil 2, Kapitel 9*, in dem die ausgeprägten Cluster-Funktionen von VMware ESX Server 3 beschrieben sind.

In diesem Kapitel geht es nicht um die Behebung der Folgen, also das Failover bei einem Ausfall, sondern eher um die Vorbeugung – die Methoden, um Ausfälle zu verhindern. Bei aller Virtualisierung bildet Hardware immer die Basis der gesamten virtuellen Infrastruktur. Also sollten Sie auf deren Verfügbarkeit besonders Ihr Augenmerk richten.

### **5.3.2 Redundanz – der Weg zum störungsfreien Betrieb**

Ausfallsicherheit bedeutet neben zuverlässiger Hardware vor allem die Absicherung wichtiger Bauteile durch Ersatzkomponenten. Denn auch das Netzteil eines Markenherstellers kann kaputt gehen. Auf folgende Komponenten sollten Sie achten:

## Stromversorgung und USV-Steuerung

Ohne Strom geht gar nichts. Eine unterbrechungsfreie Stromversorgung (USV) sollte kurze Ausfälle komplett überbrücken und bei längeren Ausfällen dafür sorgen, dass die Hosts inkl. aller Gäste genügend Zeit haben, um sauber herunterzufahren. Für hochverfügbare Lösungen können auch Notstromaggregate in Frage kommen, die das Rechenzentrum unabhängig vom öffentlichen Netz machen. Die Laufzeit einer USV ist abhängig von der Last der angeschlossenen Geräte und sollte entsprechend dimensioniert sein.

Redundant ausgelegte USVs stellen die Stromversorgung auch beim Defekt eines Gerätes sicher, eine so genannte Multicast-Konfigurationen mit Netzwerkanbindung der USVs sorgt für die gegenseitige Überwachung. In fast allen modernen Servern kommen bereits redundante Netzteile zum Einsatz. Verteilen Sie die Anschlüsse auf verschiedene USVs, damit auch beim Ausfall einer USV alle Server weiterlaufen.

Besonderes Augenmerk ist auf eine funktionierende USV-Steuerung zu richten. Es nützt nichts, wenn die Batterien bei längerem Stromausfall leer sind und alle Server dann doch hart abschalten. Eine USV-Steuerung muss anhand der Restkapazität rechtzeitig das Herunterfahren der Hosts inklusive VMs auslösen. Dazu sind spezielle Agenten des jeweiligen Hersteller im Hostsystem zu installieren. Beim ESX Server müssen Sie in der Service-Konsole die Linux-Version der Steuerungssoftware einrichten, z.B. *PowerChute Network Shutdown für Linux*.

**USV-Steuerung  
zum geordneten  
Herunterfahren**

Das Host-System ist wiederum dafür zuständig, die Gäste ordentlich herunterzufahren. Unter VMware stellen Sie das beispielsweise ein unter VM/SETTINGS/OPTIONS/STARTUP/SHUTDOWN bei ON HOST STARTUP bzw. ON HOST SHUTDOWN.

Unter Microsoft Virtual Server finden Sie die Konfiguration unter ALLGEMEINE EIGENSCHAFTEN einer VM bei AKTION BEIM BEENDEN VON VIRTUAL SERVER.

## Server-Hardware und Überwachung

Lüfter und Netzteile sollten in einem Server mehrfach vorhanden sein und sich vor allem im laufenden Betrieb wechseln lassen. Dazu gehört auch der Einbau des Gerätes in einen Serverschrank, möglichst auf Gleitschienen, um an die Komponenten im Wartungsfalle auch heranzukommen.

Wenn ein Bauteil ausfällt, muss man das erst einmal merken, sonst nützt die beste redundante Ausstattung nichts. Ein Überwachungsagent sollte auf jedem Host installiert sein, um erhöhte Temperaturen, defekte Lüfter, Netzteile oder Festplatten sofort zu erkennen. Beim ESX Server wird dieser Agent in der Linux-basierten Service-Konsole installiert.

**Mehrere Server  
zur Ausfall-  
sicherheit**

Grundsätzlich sind zwei leistungsschwächere Maschinen besser als eine leistungsstarke. Das bietet zwar für mehr Geld nur die gleiche Leistung, ist aber redundant (siehe Abbildung 5.1). Die Hardware sollte immer so ausgelegt sein, dass zur Not ein Host längere Zeit ausfallen kann. Die verbleibenden Maschinen tragen dann alle Gäste. Mit zentralem Speicher ist ein schnelles Übertragen virtueller Maschinen von einem Host zum anderen möglich (siehe dazu auch den Cluster-Workshop in Teil 2, Kapitel 8).

**Netzwerkkarten und Switches**

**Redundanter  
Backbone mit  
XRN**

Netzwerkkarten im Host und die LAN-Switches sollten ebenfalls redundant ausgelegt sein. Mittels Teaming können dann bestimmte Adapter den Datenverkehr ausgefallener Netzwerkkarten übernehmen. Die Hosted-Produkte unterstützen Teaming nur mit Hersteller-treibern für die Netzwerkkarten. Der ESX Server hat sehr ausgefeilte Methoden zum Teaming und zum Load Balancing von Netzwerk-adaptoren (siehe Teil 2, Kapitel 9). Switches sollten gegebenenfalls mit Protokollen wie XRN (*Expandable Resilient Networking*) untereinander verbunden sein und so einen logischen redundanten Backbone bilden.

**Interner oder externer Festplattenspeicher**

Der Plattenspeicher, auf dem Ihre VMs liegen, nimmt eine zentrale Rolle im Verfügbarkeitskonzept ein. Der Ausfall eines Hosts lässt sich bei mehreren vorhandenen Servern recht einfach kompensieren, wo eine VM läuft, ist relativ nebensächlich. Der Massenspeicher bleibt dagegen die kritische Komponente, da hier die Gastsysteme mitsamt der Anwendungsdaten liegen.

RAID-Systeme sind unersetzlich zur Vorsorge bei einem Plattenausfall. Fällt ein ganzer Host mit internem Plattenspeicher aus, dann ist es sehr vorteilhaft, wenn der gesamte Plattenstapel in einem Gerät mit kompatiblen Controller sofort weiterverwendet werden kann. Damit sparen Sie sich die Datenrücksicherung.

**Externer Speicher  
im SAN hat einige  
Vorteile bei Host-  
Ausfällen**

Ein zentraler Datenspeicher, etwa ein SAN, bietet gegenüber lokalen Festplatten sehr viele Vorteile, auch bei einem Ausfall des Hosts. Die Maschinen können auf einem anderen Host einfach neu gestartet werden, teilweise durch Host-Cluster sogar automatisiert. Dieser Speicher wird aber gleichzeitig zur Achillesferse des gesamten Konzeptes. Das Speichernetzwerk muss redundant ausgelegt sein. Doppelte Fibre-Channel-Switches oder Ethernet-Switches bei iSCSI bzw. NAS-Anbindung. Auch die Host Bus Adapter (HBA) in den Wirtsrechnern sollten doppelt vorhanden sein, damit ein Ausfall mittels Multipathing kompensiert werden kann (Abbildung 5.1). Das Speichergerät selbst verfügt möglichst über mehrere Speicherprozessoren (*Storage Processor* bzw. *Controller*).

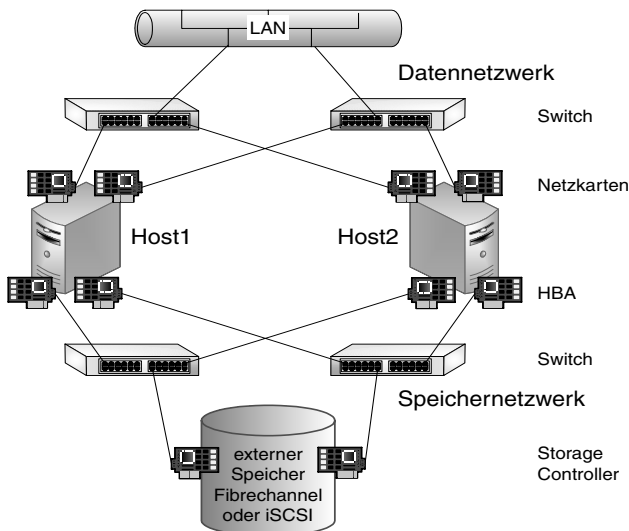


Abbildung 5.1:  
Eine gebräuchliche  
Konfiguration  
zweier ESX Server  
mit redundanter  
Anbindung an den  
externen Speicher  
und an das LAN

Speichernetzwerk und LAN sind physisch zu trennen. Bei Fibre-Channel ist das sowieso gegeben, bei iSCSI sollten Sie nicht den Verkehr über die vorhandene LAN-Struktur leiten, sondern separate Switches anschaffen, um Performanceproblemen aus dem Wege zu gehen.

Dass der externe Speicher über ausfallsichere RAID-Konfigurationen verfügt, ist selbstverständlich. Eine weitere interessante, aber auch sehr teure Methode ist die Spiegelung des Speichersystems auf ein weiteres Gerät, eventuell sogar an einem entfernten Standort, zur Katastrophenvorsorge. Herstellerspezifische Zusatzsoftware sorgt bei diesen Lösungen dafür, dass vom Speichersystem an den Client (in unserem Falle der Host) erst dann ein erfolgreicher Schreibvorgang zurückgemeldet wird, wenn die gleichen Daten auf einem zweiten System im Hintergrund ebenfalls geschrieben wurden. So steht nach einem Komplettausfall des Primär-Speichers ein gespiegeltes System mit einer aktuellen 1:1-Kopie zur Verfügung. Allerdings ist erst ein manueller Eingriff notwendig, um die gespiegelten LUNs des Standby-Systems wieder dem Host unter den gleichen Nummern, wie die des ausgefallenen Systems zuzuordnen.

### SAN-Spiegelung

Eine Alternative ist die Verwendung von Software-Raid innerhalb der Gastsysteme. So können Sie beispielsweise zwei virtuelle Platten auf räumlich getrennte SAN-Systeme ablegen und in Windows-Gästen als Dynamische Datenträger in einem Spiegelsatz verwenden. Teure Optionen zur direkten SAN-Spiegelung entfallen und wenn ein SAN ausfällt, dann wirkt das für den Gast nur wie der Ausfall einer Festplatte des Spiegelsatzes. Mit den folgenden Parametern in der \*.vmx-Datei arbeitet die VM auf einem ESX-Server trotz Ausfall eines SANs ohne Unterbrechung weiter:

### Software-Raid

```
scsi0.returnBusyOnNoConnectStatus = "FALSE"
```

```
disk.powerOnWithDisabledDisk = "TRUE"
```

Das Gast-System erkennt einen Plattenausfall und benutzt die verbleibende virtuelle Platte. Der Nachteil ist die geringere Leistung des Software-Raid.



Einige Sicherungsprodukte, z.B. der ESX Replicator der Firma Vizioncore, sind eine preiswerte Minimallösung, um komplette VMs auf einen zweiten Host zu spiegeln (siehe unter *Abschnitt 5.2.4, „Besonderheiten beim VMware ESX Server 3 und etablierte Sicherungssoftware“*).

## 5.4 Rechteverwaltung auf dem Host

Eine Gefahr bei der Arbeit mit virtuellen Maschinen ist das versehentliche oder mutwillige Löschen von virtuellen Platten und dem damit verbundenen Datenverlust. Gerade in Mischumgebungen, in denen auch die interne Testumgebung der IT-Abteilung neben produktiven Maschinen auf dem gleichen Host läuft, kann durch Unachtsamkeiten schnell ein Missgeschick passieren, vor allem auf einfach zu bedienenden Windows-Hosts.

### 5.4.1 Eine Verzeichnisstruktur auf dem Host mit Berechtigungen versehen

Sehr wirkungsvoll ist die Einrichtung einiger Gruppen und Nutzer, die auf eine Verzeichnisstruktur Rechte zugewiesen bekommen. Diese effektive Lösung funktioniert vor allem ohne Zusatzprodukte auf jedem Host. Folgendes Beispiel eignet sich für den VMware Server genauso wie für Microsoft Virtual Server oder sogar VMware Workstation in einer zentralen Testumgebung. Der ESX Server verfügt über eine eigene Rechteverwaltung, wo Sie sehr detailliert Zugriffsberechtigungen festlegen können (siehe *Teil 2, Kapitel 9*).

1. Legen Sie getrennte Ordner an für *Muster-VMs*, *Testumgebung* und *Produktion*.
2. Legen Sie zugehörige Gruppen an, etwa *muster*, *test* und *prod*. Ordnen Sie diesen Gruppen die entsprechenden Benutzer zu.
3. Geben Sie den Gruppen folgende Rechte:

*Tabelle 5.1:  
Mögliche Gruppen  
und Verzeich-  
nisstruktur auf  
dem Host-Rechner  
mit zugehörigen  
Dateirechten*

|                      | Muster-VMs  | Testumgebung | Produktion   |
|----------------------|-------------|--------------|--------------|
| <b>Gruppe test</b>   | Lesen       | Vollzugriff  | kein Zugriff |
| <b>Gruppe muster</b> | Vollzugriff | Vollzugriff  | kein Zugriff |
| <b>Gruppe prod</b>   | Lesen       | Vollzugriff  | Vollzugriff  |

4. Legen Sie zusätzlich einen Nutzer mit dem Namen *vm\_run\_prod* an. Dieser Nutzer ist ebenfalls Mitglied der Gruppe *prod* und wird in allen produktiven VMs als Dienstkonto eingetragen, damit die Gäste selbst Zugriff auf die Produktionsumgebung haben. Unter Linux laufen Gäste immer unter dem Besitzer der *vmx*-Datei.
5. Zum Schluss ist es sinnvoll, einen Nutzer *host\_down* anzulegen, der das Recht hat, den Host herunterzufahren. Allen anderen Nutzern entziehen Sie das Recht, z.B. über die Systemrichtlinien von Windows. Eine Remote Session versehentlich mit *Herunterfahren* anstelle *Abmelden* zu beenden, dürfte wohl schon so manchem Admin einmal passiert sein.

#### 5.4.2 Notwendige Rechte auf die Konfigurationsdatei unter VMware

Unter VMware können Sie Dateirechte auf die Konfigurationsdatei (\*.vmx) einer VM vergeben. Sie bestimmen damit, was der aktuelle Nutzer, der in der Remote-Konsole angemeldet ist, mit der VM für Aktionen ausführen darf. Der Nutzer kann sich in einer der oben genannten Gruppen befinden, dieser Gruppe geben Sie auf die Konfigurationsdatei folgende Rechte:

##### Windows:

- ▶ *Keine Rechte* – Die VM wird im Inventory nicht angezeigt, es sei denn, der an der VMware Console angemeldete Benutzer ist Administrator.
- ▶ *Lesen* – Es ist nur der Power-Status sichtbar, aber kein PowerOff, PowerOn, Suspend usw. möglich. Der Bildschirm der VM bleibt schwarz, und Sie haben keinerlei Rechte, die Konfiguration zu ändern.
- ▶ *Lesen, ausführen* – Sie können die VM steuern, z.B. PowerOff, und der Bildschirm ist sichtbar. Sie können allerdings keine Änderung an der Konfiguration vornehmen und die VM auch nicht vom Inventory entfernen. Einschalten lässt sich die VM in dieser Berechtigungsstufe nur dann, wenn als Dienstkonto ein Benutzer mit Schreibrechten hinterlegt ist.
- ▶ *Ändern* – Sie haben volle Rechte.

Wenn Sie in den Sicherheitseinstellungen im Host-Dateisystem für die virtuellen Platten unter ERWEITERT/BEARBEITEN das Recht zum Löschen für alle Nutzer entfernen, verhindern Sie in jedem Falle das Entfernen der Datenträger samt Inhalt. Das kann z.B. ganz einfach versehentlich über das Inventory passieren, mittels rechter Maustaste und DELETE FROM DISK.



Leider ist eine Trennung von der Berechtigung zum Ein- und Ausschalten der VM (PowerOn, PowerOff) und der Sichtbarkeit der Bildschirmausgabe nicht möglich. Entweder Sie sehen den Bildschirminhalt und dürfen die VM auch abschalten, oder Sie dürfen die VM nicht abschalten, sehen dann aber auch keinen Bildschirminhalt. Hier hilft nur eine Remotesteuerung wie VNC oder Remotedesktop, um einem eingeschränkten Benutzer die Arbeit im Gastsystem zu erlauben.

#### Linux:

Unter Linux ist die Wirkung der Berechtigungen etwas anders. Sie benötigen auf das übergeordnete Verzeichnis der VM auf jeden Fall das Recht *Execute* (+x), damit die VM überhaupt im Inventory erscheint. Den Rest steuern Sie wieder über die *vmx*-Datei:

- ▶ *r* – Der Bildschirm bleibt schwarz, und die meisten Funktionen sind gesperrt, allerdings ist PowerOff/PowerOn möglich.
- ▶ *rw* – Ändern der Konfiguration und auch PowerOff/PowerOn, aber kein Bildschirminhalt sichtbar.
- ▶ *xr* – Volle Steuerung, aber keine Änderung an der Konfiguration möglich.
- ▶ *xrw* – Volle Rechte.

### 5.4.3 Notwendige Rechte auf die Konfigurationsdatei unter Virtual Server 2003 R2

Auf die Konfigurationsdatei (\*.vmc) eines Gastes unter Virtual Server werden mindestens folgende Rechte benötigt:

- ▶ *Ordner auflisten/Daten lesen* – Anzeigen der Einstellungen und des Bildschirmes der VM.
- ▶ *Dateien erstellen/Daten schreiben* – Ändern der Konfiguration.
- ▶ *Ordner durchsuchen/Datei ausführen* – Steuern der VM (PowerOn usw.)

# 6 P2V – physische Rechner in virtuelle Maschinen übernehmen

Sie können ein System von einem physischen Rechner 1:1 in eine virtuelle Maschine übernehmen, dieser Vorgang wird auch als *P2V (Physical to Virtual)* bezeichnet. Ein produktiver Server lässt sich damit genauso virtualisieren wie ein Client-PC. Was ist die grundsätzliche Vorgehensweise, wo lauern Stolpersteine bei diesem Umzug? Wie muss das Quellsystem vorbereitet werden, und welche Treiberprobleme sind zu erwarten?

## 6.1 Einleitung

Der alte NT-Server mit der Datenbank, die für bestimmte Auswertungen von Zeit zu Zeit noch benötigt wird, bereitet Ihnen schon lange Kopfschmerzen? Keiner mehr da, der die Anwendungen damals installiert hat und sich damit noch auskennt? Hoffentlich macht die betagte Hardware nicht irgendwann schlapp!

**Server virtualisieren**

Ähnliche Systeme finden sich in fast jedem Serverraum. Eine ideale Methode, solche potenziellen Gefahren zu entschärfen, ist Virtualisierung. Die alte Hardware verschwindet durch die Umsetzung des Systems auf eine virtuelle Maschine, und in Zukunft ist ein Umzug der VMs auf aktuellere Technik kein Problem mehr, da die virtuelle Hardware weitestgehend unabhängig vom Host-System ist. Zusätzlich lässt sich das System für immer konservieren und sichern mittels einer einfachen Kopie der virtuellen Systemplatte auf DVD oder Band, da diese virtuelle Platte die komplette Konfiguration und alle lauffähigen Applikationen der Maschine enthält. Nebenbei sieht es im Serverschrank wieder richtig aufgeräumt aus.

LAN-Clients können Sie ebenso wie Server in eine VM transferieren, um dort umfangreiche Tests mit neuen Patches oder aktueller Software vor einem Rollout zu unternehmen. Durch verschiedene Funktionen virtueller Maschinen, wie Snapshots zur Sicherung von Systemzuständen und Wiederanlaufpunkten, kann das wesentlich komfortabler sein als auf echter Hardware. Genauso können Sie als Privatanwender Ihr ausgedientes Windows 98-System auf den neu erworbenen XP-Boliden mitnehmen, um im VMware Player hin und wieder eine alte Anwendung zu benutzen oder um Konfigurationseinstellungen abzuschauen.

**Privat-PC oder LAN-Client**



### 6.1.1 Gründe für eine Virtualisierung

Eine Virtualisierung von physischen Maschinen kommt aus verschiedenen Gründen in Frage:

- ▶ *Aufbau einer Testumgebung* – Eine Kopie des realen produktiven Netzwerks samt Servern, Clients, Anwendungen und Daten bildet eine virtuelle Pilotumgebung. Darin können neue Applikationen, Migrationen oder Patches an einem Abbild der realen Zustände getestet werden.
- ▶ *Konsolidierung des physischen Serverparks* – Mehrere produktive Maschinen lassen sich auf wenige leistungsfähige Hosts konsolidieren. Vorhandene physische Server können anstatt auf neue Hardware in VMs umgesetzt werden. Damit nutzen Sie die Vorteile virtueller Maschinen, z.B. Hardware-, Strom- und Platzersparnis, einfachere Disaster Recovery sowie Hardware-Unabhängigkeit.
- ▶ *Übernehmen von Legacy-Anwendungen auf neue Hardware* – Anwendungen auf alter unzuverlässiger Hardware können samt Betriebssystem und Konfigurationseinstellungen 1:1 ohne Neuinstallation in eine VM auf moderner Hardware übernommen werden.
- ▶ *Konservierung alter Systeme und Anwendungen* – Nach einer Übernahme in eine VM kann ein altes System, z.B. eine Fibu-Anwendung samt Datenbank, archiviert werden und lässt sich jederzeit auf einem beliebigen Host wieder zum Leben erwecken, ohne alte Hardware aufheben zu müssen.

### 6.1.2 Cloning oder Neuinstallation einer VM?

Grundsätzlich gibt es zwei Möglichkeiten, um eine virtuelle Maschine mit Leben zu erfüllen. Sie können ein vorhandenes System über einen Klonvorgang in eine virtuelle Maschinen übernehmen oder in einer VM ein sauberes System aufsetzen und alle Applikationen neu installieren. Jeder Weg hat seine Vorteile und Nachteile.

#### Neuinstallation des Gastsystems anstelle P2V

Der sauberste Weg ist die Neuinstallation eines Betriebssystems in der VM. Leider ist diese Vorgehensweise in der Praxis nicht immer möglich, weil die neue Einrichtung aller Applikationen sehr aufwändig ist, vor allem bei vielen zu migrierenden Servern.

**Sauberer, neu  
installiertes  
System**

Trotzdem – eine Überlegung ist es wert, ob Sie die Gelegenheit nicht gleich zu einer Bereinigung Ihres Systems nutzen wollen. Sie können Ihre Server in einer virtuellen Testumgebung parallel zum Produktivbetrieb völlig ungestört aufsetzen und alle Applikationen von Grund auf neu installieren. Das befreit vom Ballast jahrelang aufgelaufener Fehlinstallationen, übrig gebliebener DLLs, alter Treiber oder unnötiger Platzfresser. Und ein Upgrade des Betriebssystems auf eine aktu-

elle Version ist bei dieser Gelegenheit auch gleich möglich. Mit einer neu installierten und gepatchten Maschine legen Sie eine gute Grundlage für Ihre weitere Arbeit.

### **Virtualisierung durch Cloning eines vorhandenen Systems**

Wenn Sie allerdings den Aufwand einer kompletten Neuinstallation scheuen, und da sind Sie nicht allein, dann kommt nur die zweite Möglichkeit in Frage – die 1:1-Übertragung des Systems vom physischen Rechner auf eine neue virtuelle Maschine. Genau darum geht es in diesem Workshop.

#### **6.1.3 Grundsätzliche Vorgehensweise einer 1:1-Virtualisierung**

Im Grunde unterscheidet sich die Virtualisierung einer physischen Maschine nicht von einem Austausch der Hardware bei einem echten Rechnerwechsel. Alle Probleme, die beim Umzug des Betriebssystems auf neue physischen Hardware auftauchen würden, entstehen auch bei der Virtualisierung. Die Vorgehensweise kann in folgende Schritte aufgeteilt werden:

- ▶ Vorüberlegungen zur Machbarkeit
- ▶ Vorbereiten des Quellsystems
- ▶ System-Image erstellen und auf eine virtuelle Platte übertragen
- ▶ Vorbereitungen vor dem ersten Start der VM und Beheben von Boot-Problemen (Treiber, Einstellungen usw.)
- ▶ Nacharbeiten am System in der VM (Treiber bereinigen, VMware Tools bzw. Virtual Machine Additions installieren usw.)
- ▶ Daten mittels Sicherungssoftware zurückspielen

#### **P2V-Assistenten und Tools zur automatisierten Virtualisierung**

Wer die Investition machen will, findet im Profi-Bereich von verschiedenen Anbietern Tools, die das Übernehmen physischer Maschinen in eine VM automatisieren. Es existieren mittlerweile auch einfachere kostenlose Alternativen. Besonders hervorzuheben ist dabei der *VMware Virtual Machine Importer*. Zu den Zusatztools erfahren Sie mehr unter Abschnitt 6.8, „Produkte und Tools zur automatisierten Virtualisierung“.

Aber auch mit P2V-Tools ist teilweise manuelle Arbeit notwendig, und einige der hier geschilderten Probleme sind grundsätzlicher Natur. Es spricht nichts gegen eine manuelle Übertragung des Systems, außer es handelt sich um sehr viele Rechner. Vor allem lernen Sie das Konzept und die Fehlerquellen auf diese Weise am besten kennen. Viele Überlegungen aus diesem Workshop sollten Sie auch dann beachten, wenn Sie mit einem der Werkzeuge zur automatisierten Virtualisierung arbeiten. Nicht zuletzt ermöglicht Ihnen eine

manuelle Vorgehensweise unter Umständen sogar, einen laufenden Produktionsserver ohne Ausfallzeit als virtuelle Kopie in eine Testumgebung zu übernehmen.

## 6.2 Vorüberlegungen zur Virtualisierung

Einige Überlegungen vor der Virtualisierung eines physischen Rechners können Ihnen während des Vorganges selbst und auch später im laufenden Betrieb der neuen VMs viel Ärger ersparen. Diese Vorüberlegungen gelten auch für den Fall, dass Sie ein P2V-Tool zur Übernahme verwenden.

### 6.2.1 Problematische Hardware in der virtuellen Maschine

Zuerst ist auf dem Quellsystem zu prüfen, welche Hardware in der virtuellen Welt Probleme bereiten könnte und ob man diese umgehen kann. So können FireWire-Geräte, Geräte an der USB2.0-Schnittstelle oder die Notwendigkeit spezieller VGA-Karten bereits das vorzeitige Aus für ein Virtualisierungsvorhaben bedeuten. Ich reiße hier alle wichtigen Probleme kurz an, ausführlichere Informationen zu den Voraussetzungen für virtuelle Maschinen finden Sie in *Teil 1, Kapitel 1, „Grundlagen virtueller Maschinen und Hinweise zur Hardware“*. Sie sollten sich dieses Kapitel als Vorbereitung auf eine Virtualisierung zusätzlich durcharbeiten.

#### Nutzung von ISDN in einem Gast

**LAN-CAPI** Ein häufiges Problem virtueller Server ist die fehlende Unterstützung für ISDN-Karten, z.B. für die zentrale Faxlösung. Hier kann ein so genannter LAN-CAPI eines ISDN-Routers helfen. Dieser Router ist direkt am ISDN angeschlossen und reicht den Verkehr über TCP/IP an eine emulierte CAPI-Schnittstelle auf den Servern durch. Achten Sie dabei auf eine eventuell benötigte FAX-G3-Option, und testen Sie Ihre Anwendung unbedingt vorher in einer Pilot-VM. Anbieter solcher LAN-CAPIs finden Sie in *Teil 1, Kapitel 1*.

#### Dongles an verschiedenen Schnittstellen

Auch die Kompatibilität bestimmter USB-Geräte, vor allem Dongles, sollte vorher in einer Test-VM geprüft werden. USB-Dongles haben unter VMware das Problem, dass sie bei einem Neustart des Hosts oder der VM nicht immer automatisch dem richtigen Gast zugewiesen werden. Microsoft-Gäste unterstützen überhaupt kein USB. Auch hier existieren Lösungen, um USB 2.0 über TCP/IP in die Gäste durchzuschleifen (siehe *Teil 1, Kapitel 1*). Dongles in Form von inter-

nen PCI-Steckkarten können in einer VM grundsätzlich nicht verwendet werden, Dongles am LPT-Port funktionieren dagegen meist problemlos.

### Netzwerkarten in den virtuellen Maschinen

Ist die Quell-VM an verschiedenen Netzwerken angeschlossen, dann benötigt der Host ebenfalls mehrere physische Netzwerkkarten. Eine virtuelle Firewall belegt eventuell eine dedizierte Netzwerkkarte zum Router nur für sich allein. Ansonsten können sich mehrere VMs problemlos eine physische Netzwerkkarte teilen, wenn das die benötigte Bandbreite zulässt. Detaillierte Informationen zu den Netzwerken finden Sie in *Teil 3, Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“*.

### Virtuelle Platten der Gäste

Planen Sie auch eine Struktur für die virtuellen Festplatten. Es ist besser, mehrere virtuelle Platten für einen Gast zu verwenden anstatt nur eine einzige. System, Auslagerungsdatei und Daten sollten unbedingt getrennt werden, genauso können Datenbanken oder Exchange-Daten-speicher auf verschiedene virtuelle Datenträger verteilt werden. Das ermöglicht später eine unkomplizierte Umlagerung dieser Bereiche auf unterschiedliche physische Datenträger für eine bessere Performance. Detaillierte Informationen zu den virtuellen Festplatten finden Sie in *Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“*.

### Platten aufteilen

### Auslastung und Speicherbedarf der Gastsysteme

Bei stark frequentierten Servern müssen im Vorfeld der Virtualisierung Lastmessungen erfolgen. Die Virtualisierung eines unter Volllast laufenden Dual-CPU-Servers auf einem Host, der ebenfalls nur über zwei CPUs ähnlicher Leistung verfügt, ist nicht sehr sinnvoll, weil dann diese eine VM den Host bereits voll auslasten würde. Arbeiten dagegen alle Quellserver nur bei 5–10%, steht einem einfachen Dual-CPU-Host nichts im Wege. Ansonsten muss für den Host zu Mehrwegesystemen und leistungsstärkeren CPUs gegriffen werden. Die Netzwerkbandbreite und die benötigte Plattenperformance müssen ebenfalls im Vorfeld abgeschätzt werden.

Weiterhin sollten Sie beim Speicherbedarf für die Gäste daran denken, dass alle Virtualisierer den Gästen maximal 3,6 GByte RAM zuteilen können; bis auf den ESX-Server 3, der 16 GB pro VM bereitstellen kann. Virtuelle Dual-CPU-s bieten nur die VMware-Produkte, Microsoft-VM-s reichen immer nur eine CPU an die Gäste durch. Virtuelle 4-Wege-Systeme kann nur der VMware ESX-Server 3 virtualisieren. Details zu den Unterschieden der Produkte finden Sie ebenfalls in *Teil 1* des Buches.

### 6.2.2 Problematische Software in der virtuellen Maschine

#### Hardware-Prüfsummen

Auch bei der Software lauern Fallen. Ein Beispiel ist die Lizenzierung einer Anwendung mittels Hardware-Prüfsummen. So etwas fällt einem oft erst am Ende des Vorhabens, nachts halb drei auf die Füße. Um diese Zeit kann beim Support des Herstellers garantiert niemand einen neuen Lizenz-Key passend zur neuen virtuellen Hardware bereitstellen, was zu einem Abbruch und zu einer späteren Wiederholung des gesamten Vorhabens führt. Eine Neuregistrierung von Betriebssystemen, wie Windows-XP, wird nach dem Umzug des Systems ebenfalls fällig.

Verschiedene Anwendungen, wie Multimedia, oder grafikintensive Applikationen müssen ebenfalls im Vorfeld in einer Testumgebung auf ihre Tauglichkeit geprüft werden. Vor allem Grafik- und Soundausgabe können zum Problem werden.

### 6.2.3 Pilotmigration auf eine Testmaschine – unbedingt empfohlen!

#### Pilot-Image vom laufenden System

Böse Überraschungen lassen sich am einfachsten ausschließen, indem man ein Image der Systemplatte des Quellsystems erstellt und als Pilot-Versuch in eine VM migriert. Mit manchen Imaging-Programmen lässt sich ein Image im laufenden Betrieb des Rechners erstellen, das genügt oftmals für eine Testmigration. Die Alternative ist das Anfertigen eines Images in einer Wartungsphase bei heruntergefahrenem Rechner, was meistens nicht länger als eine halbe Stunden dauert. Ein Image der Systempartition genügt.

Die eigentliche Migration führen Sie später in Ruhe in einer abgeschotteten Test-VM durch, parallel zum laufenden Betrieb des Originals. Sie haben bei der Testmigration keinen Zeitdruck und können mehrere Versuche durchspielen, bis das System in einer VM läuft. So schaffen Sie viele Probleme aus dem Wege, bevor die heiße Umstellung beginnt.

### 6.2.4 Sicherheit während der Migration und die Möglichkeit zur Umkehr

#### Datensicherung!

Sind alle Punkte geklärt und ein Wochenende oder eine lange Nacht ist reserviert, steht dem eigentlichen Vorhaben nichts mehr im Wege. Vorher sollten Sie sich aber noch ein paar Gedanken zur Sicherheit machen.

Erstellen Sie gleich als Erstes ein Image des Systemdatenträgers des Quellsystems, das Sie notfalls wieder zurückspielen können! Es ist unbedingt notwendig, jederzeit wieder den originalen Server in Betrieb nehmen zu können, sollten bei der Virtualisierung Probleme auftauchen. Notieren Sie sich als Alternative zu einem Image wenigstens jede Änderung am Quellsystem, und vermeiden Sie größere Eingriffe.



Eine komplette Datensicherung vor der Umstellung sollte selbstverständlich sein. Wenn Sie bisher nur einfache Komplettsicherungen auf Band gemacht haben, dann können Sie in der Nacht vor der Umstellung eine Komplettsicherung mit Rücksetzen des Archivbits laufen lassen. So müssen am Tag X nur noch die geänderten Files per Differenz-Backup gesichert werden. Das spart wichtige Zeit für die eigentliche Tätigkeit der Virtualisierung.

Entfernen Sie zur Sicherheit nach dem Anfertigen und Übertragen der Image-Datei unbedingt das LAN-Kabel vom Quellsystem! So vermeiden Sie Kollisionen mit dem geklonten Double, wenn die Quelle nach dem Kopieren versehentlich oder absichtlich eingeschaltet wird, während das Zielsystem schon läuft. Außerdem verhindern Sie dadurch am Quellsystem ungewollte nachträgliche Änderungen, etwa an Postfächern bzw. Datenbanken, die somit im Image und im Zielsystem fehlen würden.

**Quelle vom Netzwerk trennen!**

Nehmen Sie auch das Zielsystem erst dann ans Netz, sobald Sie sicher sind, dass alles funktioniert. Wenn Sie die Virtualisierungsaktion doch abbrechen sollten und das virtuelle System hat bereits Datenbank-Updates, neue PPS-Daten oder Mails empfangen, dann fehlen diese Daten im physischen System, wenn Sie dieses wieder in Betrieb nehmen müssen.

Aktivieren Sie kritische Dienste wie Exchange oder Datenbanken erst ganz zum Schluss wieder im Zielsystem.



## 6.3 Quellsystem auf den Umzug vorbereiten

Vor der Übertragung des Quellsystems in die virtuelle Maschine sind einige Vorbereitungen notwendig; zum einen, um Platz und damit Zeit zu sparen, zum anderen, damit die Ziel-VM nach dem Klonen beim ersten Start nicht gleich in einen BlueScreen läuft.

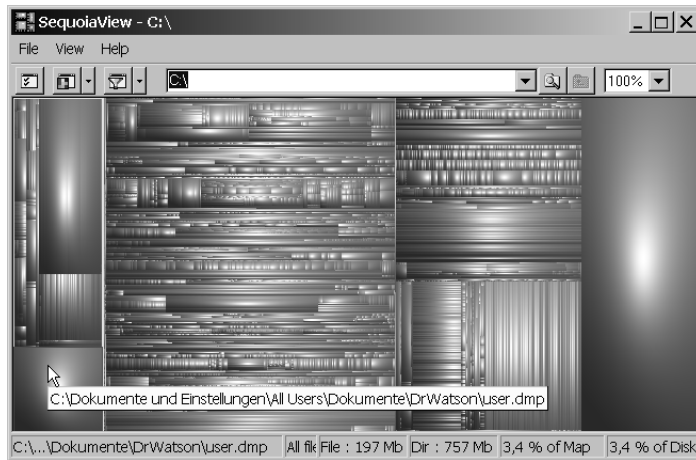
### 6.3.1 Allgemeine Vorbereitungen des Quellsystems vor der Übertragung

#### Platzverschwen- der finden

Vor der Virtualisierung sollten Sie das Quellsystem gründlich aufräumen und ausdünnen, um keinen unnötigen Ballast mitzuschleppen. Dazu gehört das Leeren des Temp-Ordners sowie des Papierkorbes und das Aufspüren großer Dateien wie Dump-Files. Ausgezeichnete Dienste leistet dazu das Programm *SequoiaView*, das sehr anschaulich auf einen Blick die Platzsituation auf der Festplatte visualisiert (Abbildung 6.1).

[www.win.tue.nl/sequoiaview](http://www.win.tue.nl/sequoiaview)

Abbildung 6.1:  
*SequoiaView* ist  
ein nützliches Pro-  
gramm zur Visia-  
lisierung der Platz-  
belegung eines  
Datenträgers



#### Dienste im Quellsystem deaktivieren

Als Nächstes sollten Sie alle Dienste auf *Deaktiviert* stellen und beenden, die sehr viel Zeit zum Starten benötigen oder die z.B. auf Datenbanken zugreifen. Dazu gehören Exchange, Datenbankserver oder Virens Scanner. Änderungen an Daten durch laufende Programme werden so verhindert, und außerdem sparen Sie später eine Menge Zeit bei den Startvorgängen in der Testphase. Konfigurations- und Monitoring-Programme (Intel- oder Compaq-Servermanagement usw.) können schon deinstalliert werden, wenn ein Sicherungs-Image des Servers vorhanden ist.

#### IP Konfiguration und Laufwerkszuordnungen des Quellsystems notieren

Schließlich sollten Sie sich unbedingt die IP-Konfiguration notieren. Diese ist im Zielsystem neu einzutragen, weil dort andere Netzwerkkarten erkannt werden. Folgender Befehl schreibt unter Windows die notwendigen Daten in eine Datei *ip.txt* auf Laufwerk C:, die dann gleich im Image liegt:

```
ipconfig /all > c:\ip.txt
```

Auch die Laufwerkszuordnungen sollten Sie sich notieren, weil alle Datenträger in der Ziel-VM als neue virtuelle Platten angelegt werden müssen.

### Automatisches Neustarten verhindern, um BlueScreens lesen zu können

Im Quellsystem sollten Sie unter SYSTEMSTEUERUNG/SYSTEM/ERWEITERT/STARTEN UND WIEDERHERSTELLEN den Haken an AUTOMATISCH NEU STARTEN entfernen. Sollte ein Fehler auftreten, bleibt das System später in einem BlueScreen stehen und versucht nicht sofort, neu zu starten. Sie haben dadurch Gelegenheit, die Fehlermeldung in Ruhe zu lesen.

### 6.3.2 Treiber für den virtuellen Festplattencontroller in der Quelle vorinstallieren

Großes Augenmerk ist schon im Vorfeld auf die notwendigen Treiber der Festplattencontroller zu legen. Vor dem Image müssen auf der Quellmaschine die später benötigten Treiber für die virtuelle Hardware der Ziel-VM vorinstalliert werden. Das übernommene Betriebssystem findet sonst in der VM ohne den richtigen Treiber die eigene Systemplatte nicht und bricht mit einem BlueScreen ab (Abbildung 6.2).

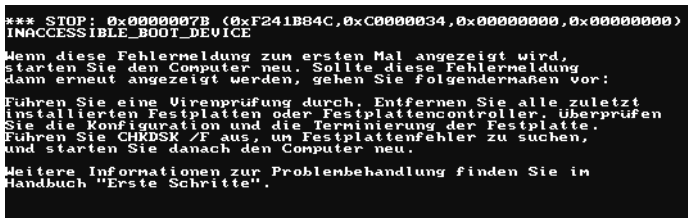


Abbildung 6.2:  
*Fehlende Treiber für die emulierten Festplattencontroller sind eine häufige Fehlerursache bei einer Virtualisierung*

Bei der Vorinstallation des Treibers müssen Sie sich entschieden, welchen emulierten Festplattencontroller Ihre Ziel-VM verwenden wird. Es stehen IDE- oder SCSI-Controller zur Verfügung. Bei SCSI bieten die Virtualisierungsprodukte verschiedene Modelle an, die teilweise vom Gastbetriebssystem abhängig sind. Grundsätzlich haben virtuelle SCSI-Platten eine bessere Performance.

#### IDE oder SCSI?

Alle Grundlagen zu den virtuellen Platten und Controllertypen finden Sie bereits in Teil 3, Kapitel 3, „Die virtuellen Platten als Herzstück der Gastsysteme“, so dass ich hier nicht nochmals darauf eingehen werde. Um den Workshop schnell und unkompliziert nachvollziehen zu können, virtualisieren Sie am besten vorerst auf eine IDE-Platte. Das funktioniert, bis auf den ESX-Server, mit allen im Buch vorgestellten Produkten und ist vom Treiber her unkompliziert. Eine spätere Umstellung der IDE-Platte auf SCSI ist möglich.



Wenn Sie sofort virtuelle SCSI-Platten verwenden wollen, dann sollten Sie unbedingt in *Teil 3, Kapitel 3* unter 5.7.1, *SCSI-Controllertypen und die passenden Treiber in den Gästen unter VMware* nachlesen, welchen Treiber Sie benötigen. Nutzer des ESX-Servers haben keine andere Möglichkeit, da dort IDE-Platten nicht unterstützt werden.



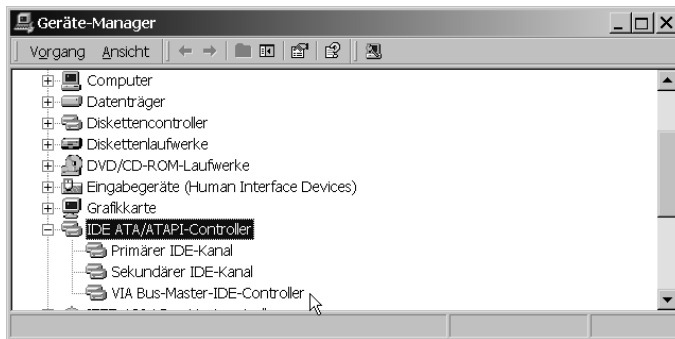
### Hat die Art der Quellplatte (IDE, SCSI oder SAN) einen Einfluss auf die Wahl der Zielplatte?

Nein – es ist nicht relevant, ob Ihr Quellsystem auf SCSI-Platten bzw. auf einem RAID-Array liegt oder gar vom SAN startet. Die Ziel-VM bootet nach dem Zurückspielen des Images ohne Probleme unter jedem Virtualisierungsprodukt von einer virtuellen IDE- oder SCSI-Platte. Voraussetzung ist, dass vorher im Quellsystem der richtige Treiber vorinstalliert wurde. Alte RAID- oder SCSI-Treiber können im Gerätemanager der Ziel-VM später entfernt werden.

### Standard-IDE-Treiber im Quellsystem vorinstallieren

Schauen Sie im Gerätemanager der Quellmaschine nach dem Eintrag *IDE-Controller* (Abbildung 6.3). Ist hier ein herstellerspezifischer Treiber installiert, kann das im Quellsystem zu Problemen führen. Wenn der *Standard-IDE-Treiber* im System vorher noch nie installiert war, produziert die Ziel-VM einen BlueScreen, da das System nicht auf den Boot-Datenträger zugreifen kann.

Abbildung 6.3:  
Andere Treiber als  
der Standard-PCI-  
Controller können  
später in der VM zu  
einem BlueScreen  
führen



Ändern Sie den vorhandenen Treiber im Gerätemanager der Quellmaschine in einen *Standard-Zweikanal-PCI-IDE-Controller*. Unter Windows erledigen Sie das folgendermaßen:

1. Starten Sie den Gerätemanager mit SYSTEMSTEUERUNG/SYSTEM/HARDWARE/GERÄTEMANAGER.
2. Klappen Sie den Eintrag *IDE-Controller* auf, und wählen Sie mit der rechten Maustaste auf den Treiber die EIGENSCHAFTEN.
3. Wählen Sie TREIBER/TREIBER AKTUALISIEREN.

4. Folgen Sie dem Dialog, wobei Sie den Treiber nicht automatisch suchen lassen, sondern unbedingt selbst wählen.
5. Sie können aus der angebotenen Liste den *Standard-Zweikanal-PCI-IDE-Controller* auswählen.

Der IDE-Treiber kann notfalls auch nachträglich durch Änderungen an der Registry der Ziel-VM installiert werden, siehe dazu *Abschnitt 6.5.10, „Registry des Zielsystems nachträglich ändern“*.



## **6.4 Image des Quellsystems erstellen und in eine VM klonen**

Sind alle Vorbereitungen getroffen, können Sie vom Quellsystem ein Image der Systempartition erstellen. Hierzu gibt es eine Vielzahl von Programmen. Sehr gute Erfahrungen habe ich mit dem Tool Acronis True Image gemacht. Es kommt auch mit Systempartitionen auf dynamischen Datenträgern zurecht, und es lässt sich eine Boot-CD mit GUI, vollem Funktionsumfang und sicher funktionierendem Netzwerk erstellen.

<http://www.acronis.com>

Eine gute Alternative zu den teuren Kandidaten, wie Ghost, Drive-Image oder Acronis, ist das preiswerte Drive SnapShot. Der große Vorteil dieses Tools ist das Format als einfache EXE-Datei, die ohne Installation oder Neustart, direkt im laufenden System, ausgeführt werden kann. Das ist sehr praktisch, um noch im Produktionsbetrieb ein Image für die Testmigration zu ziehen, ohne den Server herunterfahren zu müssen.

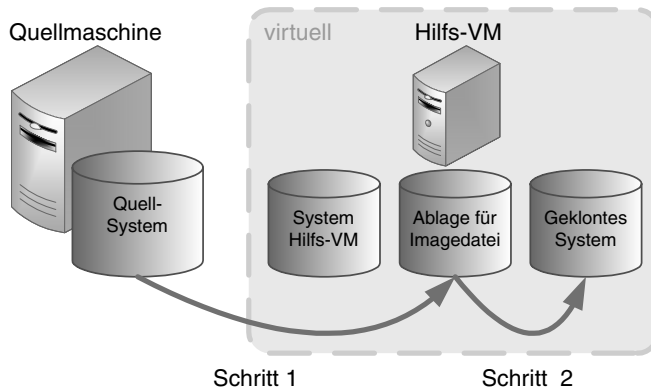
<http://www.drivesnapshot.de>

Das eigentliche Problem ist nicht die Wahl des richtigen Tools, sondern die Übertragung des Images auf eine virtuelle Platte und der Zugriff auf den Inhalt dieser Platte, um eventuelle Boot-Probleme zu beheben. Dazu hat sich das Erstellen einer Hilfs-VM bewährt.

### **6.4.1 Hilfs-VM zur Übertragung des Images und zur Problembehebung einrichten**

Ihre Hilfs-VM wird das Werkzeug sein, um das Image vom physischen Quellrechner auf eine virtuelle Platte zurückzuspielen und später einige Nacharbeiten am geklonten System zu machen. Die Hilfs-VM ist nichts weiter als eine lauffähige virtuelle Maschine mit einem Betriebssystem Ihrer Wahl sowie allen benötigten Tools und einer Bridged-Netzwerkkarte zur Kommunikation mit dem physischen LAN.

Abbildung 6.4:  
Für das Übertragen  
des Images und  
für die Nacharbei-  
ten eignet sich am  
besten eine virtuelle  
Maschine als Hilfs-  
maschine als Hilfs-  
werkzeug



Erstellen Sie für die Hilfs-VM einen neuen Gast mit drei virtuellen Platten (Abbildung 6.4):

**Alternative:  
Boot-CD mit  
BartPE**

- *Platte 1* enthält das gewünschte Betriebssystem für die Hilfs-VM, z.B. Windows XP. Dieses System kann frei gewählt werden und hat nichts mit dem physischen Quellsystem zu tun. Sie können dafür eine vorhandene VM kopieren oder das System neu aufsetzen. Installieren Sie Ihr Imaging-Tool der Wahl in dieser VM. Alternativ zu Platte 1 kann auch eine Boot-CD wie BartPE verwendet werden.

**Alternative:  
Netzwerkfreigabe**

- *Platte 2* ist eine ausreichend dimensionierte, leere virtuelle Platte, auf der Sie die Image-Datei des originalen physischen Rechners zwischenlagern werden. Platte 2 muss formatiert und im LAN freigegeben sein, damit das Image dort abgelegt werden kann (Schritt 1). Alternativ dazu kann auch eine beliebige Netzwerkfreigabe im LAN dienen.
- *Platte 3* wird später die Systemplatte der virtualisierten Maschine, indem Sie das Image darauf zurückspielen (Schritt 2). Diese Platte muss den Klon der bootfähigen Systempartition des Quellsystems aufnehmen und ist entsprechend zu dimensionieren.



Die Zielplatte *Platte 3* muss vom richtigen Typ sein, je nachdem, welchen Treiber Sie im Quellsystem vor dem Klonen vorinstalliert haben. Wenn Sie SCSI verwenden wollen, lesen Sie bitte erst *Teil 3, Kapitel 3*.

**Funktion der  
Platten**

Im Schritt 1 fertigen Sie vom Quellsystem ein Image an und legen die dabei entstehende Image-Datei über das Netzwerk auf die Platte 2 der Hilfs-VM ab. Als Alternative können Sie das Image auch auf CD brennen und in der Hilfs-VM einlegen. Im Schritt 2 spielen Sie in der Hilfs-VM das Image, das auf Platte 2 lagert, auf die Platte 3 zurück. Danach kann die Platte 3 als Systemplatte in eine neue VM, die eigentliche Ziel-VM, eingebunden werden (siehe *Abschnitt 6.4.3, „Schritt 1 der Übertragung – Image erstellen“*).

## 6.4.2 Alternative Methoden zum Übertragen des Images in die VM

Der Weg über die Hilfs-VM ist eine Methode, die in den meisten Anwendungsfällen sicher funktioniert. Es gibt auch andere Möglichkeiten, die teilweise einfacher zu handhaben sind, die aber mehr Vorbereitungsarbeit und spezielle Tools erfordern.

### Übertragen des Images direkt mit einer Boot-CD

Anstelle einer Hilfs-VM mit einem Betriebssystem auf einer virtuellen Festplatte kann auch eine so genannte Live-CD verwendet werden. Das sind CDs, von denen ein Notfallbetriebssystem startet. Hier bietet sich BartPE für die Windows-Welt oder Knoppix für Linux an (siehe auch *Teil 3, Kapitel 7, „Nützliche Zusatzprodukte, Tools, Links und Tipps“*). Viele Imaging-Tools bieten ebenfalls die Möglichkeit, eine bootfähige CD mit Netzwerkunterstützung zu erstellen. Diese CDs können Sie gleich als ISO-Datei in die Hilfs-VM einbinden, Sie sparen sich damit das Einlegen einer physischen CD (Abbildung 6.5).

**BartPE und Knoppix**

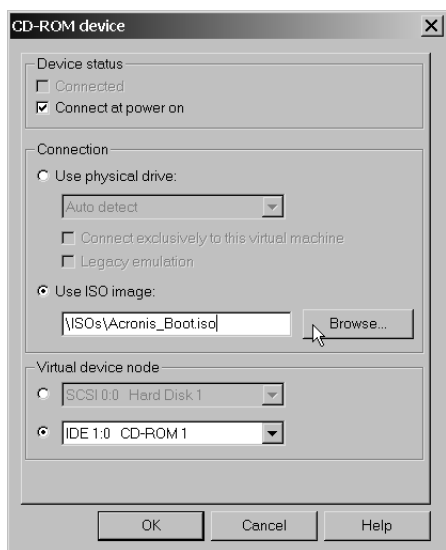
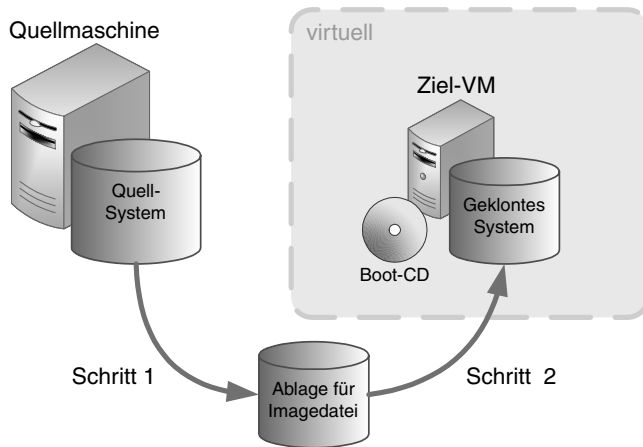


Abbildung 6.5:  
Bootfähige CDs mit  
Imaging-Program-  
men oder Notfall-  
systemen können  
einfach als ISO-  
Image eingebunden  
werden

Wenn Sie eine solche bootfähige CD verwenden und die Image-Datei auf einer LAN-Freigabe, anstelle auf der Platte 2, zwischenspeichern (Schritt 1), dann benötigen Sie keine Hilfs-VM mehr (Abbildung 6.6). Sie können in dieser Konstellation das Image ohne Umwege direkt in der Ziel-VM mittels Boot-CD vom LAN auf die virtuelle Systemplatte übertragen (Schritt 2).

Abbildung 6.6:  
Als Alternative  
können auch Boot-  
CDs und Netzwerk-  
freigaben für das  
Übertragen des  
Images dienen



### Was spricht trotzdem für den Umweg über die Hilfs-VM?

Der Umgang mit Live-CDs wie BartPE ist nicht jedermanns Sache. Wer lieber mit seinem gewohnten System arbeitet, ist mit der Hilfs-VM auf der sicheren Seite, vor allem wenn nach dem Übertragen des Images noch Nacharbeiten am Inhalt der virtuellen Platte der Ziel-VM zu erledigen sind.

Außerdem ist nicht jedes Imaging-Programm netzwerkfähig bzw. erkennt nicht die Netzwerkkartentreiber der Quellmaschine oder der VM. Für diesen Fall kann die Image-Datei in einem Zwischenschritt auf eine USB-Platte oder auf einen Datenträger im Quellsystem abgelegt werden. Von dort kann diese Datei über die funktionierende LAN-Verbindung des wieder gestarteten Quellsystems auf die Platte 2 der Hilfs-VM abgelegt werden. Dadurch muss beim Zurückspielen das Image-Programm in der VM ebenfalls keinen Zugriff auf das Netzwerk haben. Dieser Weg ist etwas umständlich, aber in manchen Fällen nicht anders möglich.

### VMware DiskMount zum direkten Zugriff auf den Inhalt einer virtuellen Platte

#### Platteninhalt direkt bearbeiten

Als weitere Alternative zur Hilfs-VM kann unter VMware das Tool *VMware-DiskMount* dienen (siehe Teil 3, Kapitel 3). Es ermöglicht das Einbinden (*Mounten*) virtueller Platten unter einem Laufwerksbuchstaben am Host. Sie haben damit vom Host direkten Zugriff auf den Platteninhalt. Das ist sehr nützlich, um z.B. nachträglich Einträge in der *Boot.ini* anzupassen oder um auf die Registry des geklonten Systems zuzugreifen. Verwenden Sie keine Hilfs-VM, sondern nur eine bootfähige CD Ihres Imaging-Programms, ist VMware-DiskMount eine komfortable Möglichkeit, um nachträglich den Inhalt der geklonten virtuellen Platte zu bearbeiten.

## **Physische Platte aus dem Quellsystem umbauen oder auf ein SAN zugreifen**

Sie können auch ganz auf ein Image verzichten, indem Sie die Festplatte des Quellsystems einfach in den Host einbauen und in die Ziel-VM als physische Platte einbinden. Die Platte lässt sich direkt verwenden oder der Inhalt innerhalb der VM mittels Boot-CD auf eine virtuelle Platte übertragen. Diese Methode eignet sich allerdings nur für Einzelplatten, weniger für RAID-Systeme. Wenn die Quelle und der Host allerdings auf das gleiche SAN Zugriff haben, kann diese Methode von Interesse sein.

### **6.4.3 Schritt 1 der Übertragung – Image erstellen**

Wenn Sie sich für einen Weg entschieden haben, können Sie von der vorbereiteten physischen Maschine das Image erstellen. Es genügt ein Image der Systempartition, wenn die Datenpartitionen und die Systempartition getrennt sind. So dürfte das Image in den wenigsten Fällen 10 GB überschreiten. Die Nutzdaten werden später per Backup-Software übertragen. Zum Erstellen des Images gibt es zwei grundsätzliche Möglichkeiten:

#### **Image im laufenden Betrieb der Quelle anfertigen**

Bei laufender Quellmaschine ist es mit einigen Imaging-Tools (z.B. DriveSnapshot) möglich, die Systempartition des Systems zu sichern, ohne den Rechner herunterzufahren. Damit können Sie ohne Unterbrechung des Betriebes eine Testmigration durchführen oder einen Klon für eine Pilotumgebung anfertigen. Der Zustand des Images entspricht aber dem einer Platte nach einem plötzlichen Stromausfall oder Absturz, weil offene Dateien und gepufferte Transaktionen im RAM teilweise nicht auf die Platte geschrieben wurden und im Image fehlen.

#### **Konsistentes Image im ausgeschalteten Zustand der Quelle**

Für eine endgültige Virtualisierung eines Produktivsystems ist es sicherer, das Image nur im ausgeschalteten Zustand zu ziehen. Nur so gelangen Sie zu einem wirklich konsistenten Stand des Systems. Moderne Imaging-Tools haben oft eine Boot-CD mit funktionierender Netzwerkunterstützung. Das Image-File kann damit über das Netzwerk auf der freigegebene virtuelle Platte 2 der Hilfs-VM abgelegt werden.

### 6.4.4 Schritt 2 – Image auf die virtuelle Ziellplatte zurückspielen

Nach erfolgreichem Erstellen des Images wechseln Sie zur Hilfs-VM. Wenn das Image-File dort ordentlich auf der virtuellen Platte 2 angekommen ist, können Sie es mit dem Imaging Tool auf die virtuelle Platte 3 zurückspielen. Platte 3 wird damit die geklonte Systemplatte des Quellsystems und kann anschließend in eine neue VM (die Ziel-VM) als Systemplatte eingebunden werden.

*Fertig – Sie haben einen 1:1-Klon Ihres physischen Rechners!*



Machen Sie in der Hilfs-VM unter VMware keinen Snapshot. Sonst landen alle Aktionen, z.B. das Image-Zurückspielen, erst in den Redo-Logs der virtuellen Platten. Die Inhalte dieser Logs müssen dann, mittels Remove Snapshot, erst noch auf die eigentliche virtuelle Platte übertragen werden. Das kann, je nach Größe des Images, sehr zeitaufwändig sein.

#### Den Klon ausprobieren

Sie können die Ziel-VM mit dem geklonten System bereits booten. Mit etwas Glück, mit funktionierendem Plug&Play und vor allem mit IDE als Plattentyp läuft Ihre virtualisierte Maschine problemlos hoch. Mit etwas Pech werden Sie dagegen einen BlueScreen zu Gesicht bekommen mit verschiedenen Fehlermeldungen. Und genau hier beginnt der knifflige Teil der Arbeit.

## 6.5 Vorbereiten des ersten Startvorganges der VM und Beheben von Boot-Fehlern

Wenn Sie bei Ihrem ersten Startversuch des übertragenen Systems in der Ziel-VM kein Glück hatten und ein BlueScreen oder andere Fehler erscheinen, dann sind verschiedene Anpassungen am Gastsystem zu machen. Dazu müssen Sie auf den Inhalt der geklonten Systemplatte zugreifen können, um z.B. die Datei *Boot.ini* anzupassen oder um bestimmte Systemdateien zu ersetzen.

Sie können die geklonte Systemplatte vorläufig in der Hilfs-VM und parallel dazu in der Ziel-VM einbinden, wobei beide VMs aber nicht gleichzeitig laufen können (Abbildung 6.7). Stoßen Sie auf einen Boot-Fehler, schalten Sie die Ziel-VM einfach ab und starten die Hilfs-VM. Dort können Sie auf den Inhalt der virtuellen Platte zugreifen, die das geklonte System enthält. Wenn Sie den Fehler behoben haben, fahren Sie die Hilfs-VM wieder herunter und starten die Ziel-VM, um zu sehen, ob diese jetzt fehlerfrei bootet.

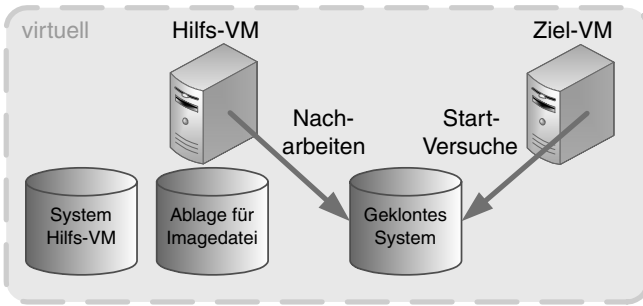


Abbildung 6.7:  
In der Hilfs-VM werden so lange Fehler korrigiert, bis die Ziel-VM mit der virtuellen Systemplatte bootet

Der Zugriff auf die geklonte virtuelle Systemplatte funktioniert auch mit BartPE oder Knoppix in der Ziel-VM bzw. mit VMware DiskMount direkt vom Host aus.



Für die häufigsten Probleme, die bei einer Virtualisierung lauern und die Sie in der Hilfs-VM beheben können, finden Sie im Folgenden eine Lösung.

### 6.5.1 Keine aktive Partition auf der Zielplatte festgelegt

Wenn die Boot-Partition der Ziel-VM nicht auf *aktiv* gesetzt wurde, dann kann das System nicht starten und bleibt mit einer Fehlermeldung noch im schwarzen Bildschirm gleich nach den BIOS-Meldungen stehen. Nicht alle Imaging-Tools aktivieren die übertragene Partition automatisch. Nachträglich geht das Aktivieren der Systempartition am einfachsten über die Datenträgerverwaltung in der Hilfs-VM (Abbildung 6.8). Aber auch mittels FDISK auf einer MS-DOS-Boot-Diskette oder über diverse Tools wie z.B. PowerQuest ServerMagic können Sie die Partition aktivieren.

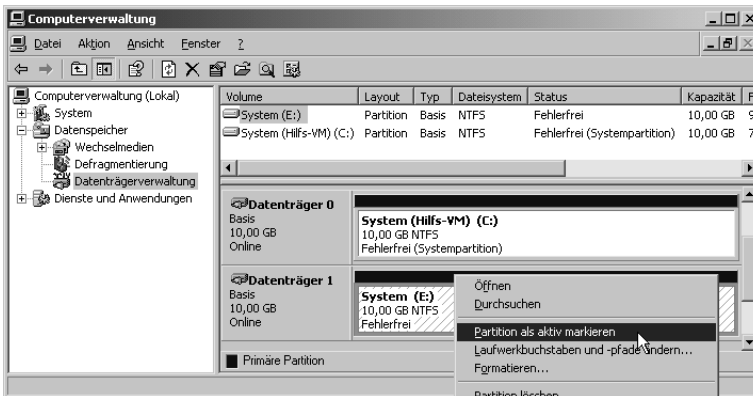


Abbildung 6.8:  
Eine bootfähige Partition muss aktiviert werden



## 6.5.2 Fehlender MBR auf der virtuellen Platte

Wurde die neue leere Zielplatte nach dem Erstellen nicht mit einem Master-Boot-Record (MBR) versehen, dann kann von dieser Platte ebenfalls nicht gebootet werden, wenn das Imaging-Tool nicht selbst den MBR vom Quellsystem überträgt. Nachträglich können Sie z.B. mit der Windows-CD booten und mittels *R* wie *Recovery* (Abbildung 6.9) die Wiederherstellungskonsole starten. An der Kommandozeile der Wiederherstellungskonsole lassen sich mittels der Kommandos `fixmbr` und `fixboot C:` der Master-Boot-Record und der Startsektor neu schreiben. Eine bootfähige DOS-Diskette und der Befehl `fdisk /mbr` führen ebenfalls zum Ziel, genauso das Tool `testdisk` (siehe Abschnitt 6.5.3, „Ziel-VM bootet nicht durch eine falsche CHS-Geometrie“).

Abbildung 6.9:  
Mit der Windows-  
Boot-CD und der  
Taste *R* gelangt man  
in die Kommando-  
zeile der Wiederher-  
stellungskonsole von  
Windows



## 6.5.3 Ziel-VM bootet nicht durch eine falsche CHS-Geometrie

Wenn beim ersten Boot-Versuch gleich nach den BIOS-Meldungen in der Ziel-VM Fehler wie *Ntldr is missing*, *A disk read error occurred* oder nur ein blinkender Cursor auf schwarzem Bildschirm erscheinen, dann kann die Ursache eine andere Plattengeometrie der virtuellen Zielplatte als die des physischen Originals sein. Da Windows den Einsprungpunkt seines Bootloaders (*Ntldr*) direkt per CHS (*Cylinder, Head, Sector*) angibt, wird eine falsche Stelle angesprungen, sobald die neue Platte bzw. das BIOS der VM andere Geometriedaten liefert als die Quellmaschine, auf der Windows installiert wurde.

Manchmal hilft auch bei diesem Fehler `fixmbr` von der Wiederherstellungskonsole. Bleibt der Fehler trotzdem bestehen, dann können Sie mit dem Tool `Testdisk` den richtigen CHS-Wert ermitteln lassen und korrekt neu setzen. Das Tool können Sie entweder unter Windows in der Hilfs-VM starten oder auch unter DOS von einer Boot-Diskette. Nachdem Sie die richtige Festplatte im Hauptmenü von `Testdisk` ausgewählt haben, lassen Sie über den Menüpunkt `ADVANCED/BOOT/REBUILD BS/WRITE` den Boot-Sektor neu berechnen und schreiben (Abbildung 6.10). Den Download finden Sie hier:

<http://www.cgsecurity.org>

```
TestDisk 6.2-WIP, Data Recovery Utility, October 2005
Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org

Disk 00 - 2047 MB - CHS 1040 64 63
Partition Start End Size in sectors
1 * HPFS - NTFS 0 1 1 1037 63 63 4185153
Boot sector
check_NTFS: Incorrect number of heads/cylinder 128 (NTFS) != 64 (HD)
OK
Backup boot sector
check_NTFS: Incorrect number of heads/cylinder 128 (NTFS) != 64 (HD)
OK
Sectors are identical.

[Quit] [Rebuild BS] [Dump]

Rebuild boot sector
```

Abbildung 6.10:  
Unterschiedliche  
CHS-Geometrie-  
daten können mit  
einem Tool wie Test-  
disk korrigiert  
werden

## 6.5.4 Boot.ini anpassen

Wenn im Quellsystem die Systempartition nicht die erste Partition auf der Platte war, dann führt das zu einem BlueScreen in der Ziel-VM mit der Meldung *Inaccessible Boot Device*. Markengeräte der Serverhersteller haben z.B. oftmals eine kleine Wartungspartition an erster Stelle, die beim Klonvorgang nicht mit kopiert wurde. Also muss die Datei *boot.ini* auf der Zielplatte angepasst werden, weil dort die Position der Systempartition vermerkt ist. Da wir in der neuen VM eine separate Platte (disk0) mit nur einer Partition (partition1) als System verwenden, sollte die *boot.ini* etwa so aussehen:

**Position der  
Startpartition**

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Windows
2000 Server" /fastdetect
```

Beachten Sie die Zählweise! Platten beginnen bei Nummer 0, Partitionen bei Nummer 1.

Um die *boot.ini* komplett neu aufzubauen, können Sie an der Wiederherstellungskonsole auch den Befehl `bootcfg /rebuild` eingeben.



## 6.5.5 Alte Treiber verursachen einen BlueScreen

Seltener verursachen alte Treiber oder DLLs beim Start der Ziel-VM einen BlueScreen. Die fehlerhafte Treiberdatei ist aus der BlueScreen-Meldung ersichtlich und wird am einfachsten über die Hilfs-VM auf der geklonten virtuellen Systemplatte umbenannt oder gelöscht. Die Ziel-VM müsste nach dem Entschärfen der Datei starten, und der

Treiber oder die Anwendung kann bei laufender VM später sauber deinstalliert werden.



Normalerweise können Sie im Quellsystem unter SYSTEMSTEUERUNG/SYSTEM/ERWEITERTE STARTEN UND WIEDERHERSTELLEN den Haken an AUTOMATISCH NEU STARTEN entfernen, um BlueScreens in Ruhe lesen zu können. Haben Sie das verpasst und die Fehlermeldung verschwindet zu schnell, um den Treibernamen zu lesen, kann unter VMware der BlueScreen mittels *Suspend* eingefroren werden. Dann lässt sich im Verzeichnis der VM die \*.png-Datei mit einem Bildbetrachter öffnen. Unter Virtual PC/Server hilft der Pausenmodus. Windows XP und 2003 ermöglichen mittels **F8** ein nachträgliches Abschalten der automatischen Startoption. Und mittels Registry-Key kann der Autostart auch nachträglich abgeschaltet werden:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\
Control\CrashControl
```

```
Autoreboot=0
```

([support.microsoft.com/kb/q174630/](http://support.microsoft.com/kb/q174630/))

### 6.5.6 Startprotokollierung und abgesicherter Modus zur Fehlersuche

Eine weitere Möglichkeit, um Startproblemen und fehlerhaften Treibern auf die Spur zu kommen, ist die Startprotokollierung oder der abgesicherte Modus von Windows. Wenn Sie gleich zu Beginn des Windows-Startvorganges in der Ziel-VM die Taste **F8** drücken, dann gelangen Sie in ein Menü, in dem Sie die Startprotokollierung einschalten können (Abbildung 6.11). Windows schreibt dann während des Bootvorganges eine Datei *Ntbtlog.txt* ins Windows-Verzeichnis. In dieser Datei ist der Name des Treibers zu erkennen, der vor dem Absturz als letzter geladen wurde.

Abbildung 6.11:  
Mit der Taste F8  
gelangt man zu den  
erweiterten Start-  
optionen

```
Erweiterte Windows-Startoptionen
Wählen Sie eine Option aus:

 Abgesicherter Modus
 Abgesicherter Modus mit Netzwerktreibern
 Abgesicherter Modus mit Eingabeaufforderung
 Startprotokollierung aktivieren
 UGA-Modus aktivieren
 Letzte als funktionierend bekannte Konfiguration
 Verzeichnisdienstwiederherstellung (Windows-Domänencontroller)
 Debugmodus
 Automatischen Neustart bei Systemfehler deaktivieren

 Windows normal starten
 Neustarten
 Zum Betriebssystemauswahlmenü zurückkehren

Verwenden Sie Pfeil nach oben bzw. unten, um einen Eintrag zu markieren.
```

Weiterhin können Sie versuchen, die Ziel-VM im abgesicherten Modus zu starten, wobei nur die notwendigsten Treiber geladen werden. Sollte der Start gelingen, können Sie im System verdächtige Software deinstallieren und anschließend einen erneuten Versuch unternehmen, um den Gast normal zu booten. Außerdem lässt sich an dieser Stelle unter Windows XP und 2003 auch nachträglich der automatische Neustart bei Systemfehler deaktivieren, wodurch ein BlueScreen stehen bleibt, um die Fehlermeldungen zu lesen.

### 6.5.7 Die Quelle ist ein Multiprozessorsystem

Wenn die fertig geklonte Ziel-VM eine hohe CPU-Last des Hosts verursacht, obwohl in der VM keinerlei Last im Task-Manager zu sehen ist, dann war die Quelle wahrscheinlich ein Multiprozessorsystem. Beim älteren VMware GSX Server, beim VMware Player und bei den Microsoft-Produkten stürzen Multiprozessor-VMs beim Start entweder ab (NT4 als Gastsystem) oder verursachen zumindest eine hohe Last auf dem Host.

**Hohe CPU-Last  
oder BlueScreen**

Bei den aktuellen VMware-Produkten stürzen Dualprozessorsysteme in einer VM nicht mehr ab, wenn als Anzahl der virtuellen Prozessoren 2 eingestellt wird. Das kann die Übernahme in eine VM deutlich vereinfachen. Allerdings ist es nicht sinnvoll, alle virtuellen Maschinen auf Dauer mit zwei virtuellen CPUs zu betreiben, weswegen eine Umstellung auf eine Single-CPU empfehlenswert ist. Die Verwaltung mehrerer virtueller CPUs in den Gästen erzeugt nämlich einen Overhead, der nur dann wieder wettgemacht wird, wenn Applikationen in der VM auch wirklich mehrere Prozessoren ausnutzen. Ansonsten verbraucht die zweite virtuelle CPU mehr Ressourcen, als sie nützt.

### Multiprozessor in Singleprozessor ändern unter Windows 2000 und höher

Ein Multiprozessor-PC kann ab Windows 2000 auch nach dem Klonen im GERÄTEMANAGER über den Punkt COMPUTER in einen Single-CPU-PC geändert werden. Dazu öffnen Sie im Gerätemanager den Eintrag COMPUTER (Abbildung 6.12) und öffnen dort mit einem Rechtsklick, im Beispiel auf den *MPS Multiprozessor PC*, die Eigenschaften. Über TREIBER AKTUALISIEREN können Sie den passenden Eintrag anhand der Tabelle 6.1 herausuchen und installieren (Abbildung 6.13).

**ACPI oder  
Standard**

Wichtig beim Wechsel des Computertyps ist es, innerhalb der Klasse zu bleiben. Ein Wechsel zwischen ACPI oder Nicht-ACPI führt bei dieser Methode zu einem BlueScreen beim nächsten Start des Gastes. Die Typen *ACPI Uniprocessor PC* bzw. *MPS Uniprocessor PC* adressieren übrigens ein Dual-Board mit nur einer CPU bestückt. Das wäre in einer VM falsch.

Abbildung 6.12:  
Der Computertyp  
kann im Gerätema-  
nager angepasst  
werden



Wollen Sie unbedingt von Nicht-ACPI auf ACPI wechseln, dann folgen Sie der weiter unten erläuterten Vorgehensweise für einen NT4-Gast. Das dort beschriebene manuelle Ersetzen der Systemdateien funktioniert auch unter Windows 2000, XP oder 2003.

Abbildung 6.13:  
Der ausgewählte  
Treiber muss zur  
Architektur des  
Quellsystems, ACPI  
oder Nicht-ACPI,  
passen

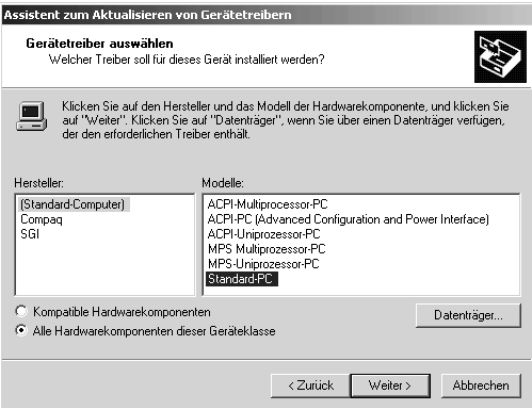


Tabelle 6.1:  
Welcher Computertyp  
muss beim Klonen  
ersetzt werden?

|                 | ACPI                                                 | Nicht-ACPI            |
|-----------------|------------------------------------------------------|-----------------------|
| Quellsystem     | ACPI Multiprozessor PC                               | MPS Multiprozessor PC |
| Ziel-VM         | Advanced Configuration and Power Interface (ACPI) PC | Standard PC           |
| NICHT verwenden | ACPI Uniprozessor PC                                 | MPS Uniprozessor PC   |

Multiprozessor in Singleprozessor ändern unter NT4

**HAL manuell ersetzen** Unter NT4 funktioniert der Wechsel von Multi- zu Single-CPU nur durch direktes Ersetzen des HAL (*Hardware Abstraction Layer*). Booten lässt sich NT4 mit Multiprozessor-HAL in einer VM mit einer CPU

nicht, es läuft sofort in einen BlueScreen. Hier müssen Sie vor dem ersten Start einige Dateien manuell kopieren. Dieses Vorgehen wird von Microsoft nicht empfohlen, es funktioniert aber.

Zuerst benötigen Sie einige Systemdateien, die sie am einfachsten aus einer sauberen Installation des Betriebssystems kopieren. Installieren Sie in einer neuen VM ein gleiches System mit gleichem Service-Pack und Patch-Stand wie Ihr Quellsystem. Von diesem System kopieren Sie aus dem Verzeichnis *System32* folgende Dateien und ersetzen diese in der geklonten virtuellen Zielplatte, danach können Sie Ihren NT4-Gast wieder starten, er arbeitet nur noch mit einer CPU:

*Ntoskrnl.exe*

*Hal.dll*

*Kernel32.dll*

*Ntdll.dll*

*Winsrv.dll*

*Win32k.sys*

### 6.5.8 Probleme bei der Verwendung von Systemplatten größer als 8 GB

Unter NT4 gibt es eine grundsätzliche Beschränkung der Größe der Boot-Platte. Dazu existieren folgende Microsoft-Artikel:

- ▶ Die Größe der Boot-Partition ist auf 4 GigaByte begrenzt (das gilt nur für eine Neuinstallation):

*[support.microsoft.com/kb/119497/DE](http://support.microsoft.com/kb/119497/DE)*

- ▶ Windows NT 4.0 unterstützt eine Systempartition von maximal 7,8 GB (das gilt immer):

*[support.microsoft.com/kb/224526/DE](http://support.microsoft.com/kb/224526/DE)*

Grundsätzlich hat die SCSI-Emulation von VMware hier und da Probleme mit Partitionen > 8 GB. In der Praxis fällt das z.B. beim Bootloader Grub unter Linux auf (nicht bei LILO) und bei einigen Partitionierungstools, die nur eine 8-GB-Platte erkennen, obwohl mehr Platz zur Verfügung steht. Das gilt nicht bei virtuellen IDE-Platten. Bei Problemen dieser Art sollten Sie immer versuchen, mit einer Systemplatte kleiner als 8 GB auszukommen, wenn es eine virtuelle SCSI-Platte ist. Nicht umsonst ist das die Standardgröße einer neu erstellten virtuellen Platte unter VMware.

Bei Datenplatten spielt die 8-GB-Grenze keine Rolle, weil es nur beim Boot-Vorgang Probleme mit dem so genannten *Int13* gibt. Läuft das System einmal, übernehmen die Windows-Treiber die korrekte Ansteuerung der Festplatten.



### 6.5.9 Keine Anmeldung am geklonten DC möglich durch verschobene Active Directory-Dateien

Ein eher seltener Fehler ist beim Übertragen eines Domänencontrollers ab Windows 2000 möglich. Nach dem Klonen startet der Domänencontroller in der VM zwar durch, aber es ist keine Anmeldung möglich. Es erscheint ein Fehler *0xc000000f*. Das deutet darauf hin, dass aus Performancegründen in der Quellmaschine die Protokoll-dateien bzw. die Datenbank des Active Directory auf eine andere Partition verschoben wurde, die jetzt im Klon fehlt, oder einen anderen Laufwerksbuchstaben hat. Normalerweise liegen die Dateien im Windows-Verzeichnis im Ordner *NTDS*.

#### Wiederherstellungskonsolle

Eine Möglichkeit ist es, die Dateien schon in der Quelle mittels Wiederherstellungskonsolle wieder zurück auf Laufwerk C: zu verschieben. Wer das nicht kann (z.B. bei einer Testmigration mit Image vom laufenden System), erreicht dies auch nachträglich durch Patchen der Registry der Ziel-VM und zusätzliches Kopieren der Dateien vom Quellsystem. Die Vorgehensweise über die Wiederherstellungskonsolle, bzw. die benötigten Registry-Keys für eine nachträgliche Änderung, erfahren Sie bei Microsoft:

[support.microsoft.com/kb/257420/de](http://support.microsoft.com/kb/257420/de)

[support.microsoft.com/kb/280364/de](http://support.microsoft.com/kb/280364/de)

### 6.5.10 Registry des Zielsystems nachträglich ändern

Bei Fehlern im Zielsystem, die nachträgliche Änderungen an der Registry notwendig machen, steht man vor dem Problem, dass ohne laufendes Betriebssystem kein Zugriff auf die Registry erfolgen kann. Es existiert aber eine Möglichkeit, die Registry eines fremden Systems als externe Registry direkt in der Hilfs-VM zu bearbeiten. Eigentlich sollten solche Nacharbeiten eher die Ausnahme sein, vor allem wenn man schon in der Quelle vor dem Klonvorgang die benötigten Controllertreiber vorinstalliert hat. Bei einigen Fehlern kann es aber nützlich sein, Anpassungen nachträglich am Klon machen zu können.

#### Fremde Registry manuell editieren

Sie benötigen zum Ändern der Registry aus der Hilfs-VM heraus Zugriff auf den Ordner *system32* der virtuellen Systemplatte der Ziel-VM. Die Registry eines Windows-Systems befindet sich in verschiedenen Dateien. Im Ordner *%SystemRoot%\system32\config* finden Sie die Datei *system*, die *HKEY\_LOCAL\_MACHINE\System* enthält, sowie die Datei *software* mit dem Zweig *HKEY\_LOCAL\_MACHINE\Software*. Mit dem Programm *regedt32.exe* können Sie die fremde Registry in diesen Dateien folgendermaßen bearbeiten:

1. Starten Sie in der Hilfs-VM *regedt32* über START/AUSFÜHREN.
2. Wählen Sie die Struktur *HKEY\_LOCAL\_MACHINE*.
3. Laden Sie eine Datei der fremden Registry über das Menü REGISTRIERUNG/STRUKTUR LADEN von der Festplatte der Ziel-VM. *regedt32* fragt dabei nach einem Schlüsselnamen, unter dem die fremde Registry eingebunden werden soll. Sie können einen beliebigen Namen festlegen, z.B. *system\_vm*.
4. Unter diesem Key kann die Registry der Ziel-VM nun in der Hilfs-VM bearbeitet werden.
5. Nachdem die Änderungen ausgeführt wurden, können Sie die fremde Registry wieder mittels REGISTRIERUNG/STRUKTUR ENTLADEN freigeben.

Alle Änderungen werden immer sofort in die geladene Registry-Datei geschrieben, es erfolgt kein nachträgliches Speichern. Achten Sie auch darauf, Ihre lokale Registry nicht mit dem geladenen fremden Zweig zu verwechseln und dadurch die Änderungen versehentlich am System der Hilfs-VM zu machen.



### Mehrere Einträge in eine fremde Registry automatisch importieren

Um ganze \*.reg-Dateien in eine fremde Registry zu importieren, wird das Programm *reg.exe* benötigt. Es ist bei Windows XP/2003 schon dabei, bei Windows 2000 befindet es sich auf der Windows-CD im Verzeichnis *support\tools*. Mit diesem Programm können Sie eine fremde Registry aus der Hilfs-VM heraus über die Kommandozeile oder eine Batch-Datei mittels *reg load* öffnen und mittels *reg unload* wieder entladen. In die geöffnete Registry kann mittels *regedit /s* der Inhalt einer \*.reg-Datei importiert werden.

Folgendes Beispielskript fügt den gesamten Inhalt einer \*.reg-Datei mit dem Namen *regdatei.reg* in eine fremde Registry ein. Dabei ist *system\_vm* ein beliebig festzulegender Name, unter dem die Registry geladen wird, und *%SystemRoot\_fremd%* ist der Pfad des Windows-Verzeichnisses auf der fremden Festplatte.

```
reg load HKLM\system_vm %SystemRoot_fremd%\system32\
config\system
regedit /s regdatei.reg
reg unload HKLM\system_vm
```

Eine passende *regdatei.reg*, um z.B. den Standard-IDE-Treiber nachträglich zu installieren, sieht dann folgendermaßen aus, Sie finden die Datei auch auf der Buch-CD:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\system_vm\ControlSet001\Services\
PCIIde]
```

**Registry  
„impfen“**

**Beispiel IDE-  
Treiber**



```
"ErrorControl"=dword:00000001
"Group"="System Bus Extender"
"Start"=dword:00000000
"Tag"=dword:00000003
"Type"=dword:00000001
"ImagePath"=hex(2):53,00,79,00,73,00,74,00,65,00,6d,0
0,33,00,32,00,5c,00,44,00,\
52,00,49,00,56,00,45,00,52,00,53,00,5c,00,70,00,63,00
,69,00,69,00,64,00,65,\
00,2e,00,73,00,79,00,73,00,00,00
[HKEY_LOCAL_MACHINE\system_vm\ControlSet001\Control\
CriticalDeviceDatabase\pci#cc_0101]
"Service"="pciide"
"ClassGUID"="{4D36E96A-E325-11CE-BFC1-08002BE10318}"
```

Zusätzlich müssen die zwei Treiberdateien *pciide.sys* und *pciidx.sys* ins Verzeichnis *%SystemRoot\_femd%\system32\drivers* kopiert werden. Diese können Sie aus der Datei *%SystemRoot\_fremd%\DriverCache\I386\Driver.cab* extrahieren oder aus einer installierten VM mit IDE-Unterstützung kopieren. Weitere Informationen zur nachträglichen Installation der IDE-Treiber liefern folgende Microsoft-Dokumente:

[support.microsoft.com/kb/314082/de](http://support.microsoft.com/kb/314082/de)

[support.microsoft.com/kb/822052/de](http://support.microsoft.com/kb/822052/de)

Auf diese Weise lassen sich übrigens auch die Treiber der gängigen SCSI-Controller in einer geklonten VM nachinstallieren. Die P2V-Tools DDChanger und Ultimate-P2V arbeiten nach genau diesem Prinzip (siehe Abschnitt 6.8, „Produkte und Tools zur automatisierten Virtualisierung“). Das ist aber nur dann notwendig, wenn Sie die Treiber in der Quellmaschine nicht vorinstalliert haben.

## 6.5.11 Reparaturinstallation als letzter Notnagel

Zum Abschluss möchte ich noch auf die Möglichkeit einer Reparaturinstallation mit der Windows-Installations-CD mit nachträglichem Aufspielen aller Service-Packs und Patches hinweisen. Diese etwas langwierige Methode kann ebenfalls viele Fehler bereinigen, sollte die Ziel-VM nicht starten. Allerdings werden dadurch auch manche Systemeinstellungen zurückgesetzt. Eine so genannte Slipstream-CD, also eine Installations-CD, die schon alle Service-Packs und Patches enthält, macht den Vorgang vom Zeitaufwand her erträglicher. Diese Methode kann ein letzter Ausweg sein, um ein Virtualisierungsvorhaben noch zu retten, dass Sie diesen Weg einmal beschreiten müssen, ist eher unwahrscheinlich.

## 6.6 Nacharbeiten an der lauffähigen VM

Haben Sie alle Fehler bereinigt und die Kopie des physischen Rechners startet in einer VM, dann sind noch einige Nacharbeiten nötig, um den Virtualisierungsvorgang abzuschließen.

### 6.6.1 Tools und Additions im Zielsystem installieren

Als Erstes sollten Sie die VMware Tools bzw. die Virtual Machine Additions installieren, um vernünftig mit der VM arbeiten zu können. Dabei werden unter anderem optimierte Treiber für Maus, VGA und Netzwerkkarten installiert. Hinweise zu den Tools finden Sie in *Teil 1, Kapitel 4, „Bedienung der Produkte – wichtige Funktionen und Tipps“*.

### 6.6.2 Alte Treiber im Zielsystem entfernen

Ein Blick ins Ereignisprotokoll hilft Ihnen, fehlerhafte Treiber oder Programme aufzuspüren. Überflüssige Programme (Software für Grafikkarten, Hardware-Monitore usw.) können deinstalliert werden, ebenso nicht mehr benötigte Treiber des Quellsystems. Alte Gerätetreiber der Quellmaschine sind im Gerätemanager oftmals nicht mehr sichtbar. An sich ist das kein Problem, diese Geräte stören meist nicht und können auch unangetastet bleiben. Nur bei Netzwerkkarten kommt es immer wieder zu lästigen Fehlermeldungen über schon vergebene IP-Adressen. Das liegt daran, dass der alte Treiber der Quellmaschine noch die originale IP-Adresse hat, die Sie jetzt auch dem neuen virtuellen Adapter des Gastes geben wollen. So spüren Sie solche verborgenen Geräte auf:

**Ereignisprotokoll**

1. Starten Sie eine Kommandozeile, und geben Sie dort ein (unbedingt in der gleichen DOS-Box):

**Verborgene Treiber aufspüren**

```
set devmgr_show_nonpresent_devices=1
start DEVMGMT.MSC
```

2. Im so gestarteten Gerätemanager aktivieren Sie:

ANSICHT/AUSGEBLENDETE GERÄTE ANZEIGEN

3. Jetzt werden zusätzlich alle verborgenen Geräte als ausgegraute Einträge aufgelistet. Alte Controller oder Netzwerkkarten lassen sich deinstallieren.

### 6.6.3 Netzwerkkarten in der Ziel-VM konfigurieren

Die Netzwerkkarten sind im Zielsystem neu zu konfigurieren, da die virtuellen Adapter als neue Hardware erkannt wurden. Die alte Konfiguration steht in der Datei *IP.txt*, die Sie in der Vorbereitungsphase am Quellsystem erstellt haben. In seltenen Fällen müssen Sie die alte MAC-Adresse des Quellrechners übernehmen, wenn diese z.B. bei

**MAC- und IP-Adressen**

einem Provider zur Authentifizierung eingetragen ist. Ausführliche Hinweise zum Thema Netzwerke finden Sie in *Teil 3, Kapitel 2, „Virtuelle Netzwerke Teil 2 – die ganze Wahrheit“*.



Das Konfigurieren der Netzwerkkarten sollte erst ganz zum Schluss geschehen, da durch jede neu hinzugefügte virtuelle Hardware oder durch die Installation der VMware Tools im geklonten System immer wieder neue Netzwerkkarten erkannt werden, die Sie dann jedes Mal neu konfigurieren müssten.

#### 6.6.4 Festplatten anlegen und Daten zurückspielen

Eine Defragmentierung des Laufwerkes C: in der VM kann die Performance des Systems verbessern, wenn die Quelle stark fragmentiert war. Optional können Sie noch eine zusätzliche virtuelle Platte für die Auslagerungsdatei einrichten.

Auf jeden Fall sollten Sie für die Daten eine oder mehrere separate virtuelle Platten, eventuell auf verschiedenen physischen Datenträgern, erstellen. Achten Sie darauf, wieder die alten Laufwerksbezeichner zu verwenden, die schon das Quellsystem verwendet hat. Die Daten spielen Sie mittels der üblichen Datensicherung zurück. Die notwendigen Sicherungs-Agenten sind im Zielsystem noch installiert, wenn sie in der Quelle bereits vorhanden waren.



Vergessen Sie nicht, zum Abschluss alle deaktivierten Dienste, wie Exchange oder Datenbanken, wieder zu aktivieren.

**Fertig!** Ihr Rechner wurde in eine virtuelle Maschine übertragen. Das physische Original darf jetzt auf keinen Fall mehr ans LAN angeschlossen werden. Zur Vorsicht sollten Sie ihn aber noch ein paar Tage aufheben, um bei Fehlern Einstellungen zu vergleichen bzw. um zu testen, ob bestimmte Probleme auch schon am Original aufgetreten sind oder erst seit der Virtualisierung existieren. Den gesamten Vorgang der Virtualisierung zeigt folgender Kasten nochmals auf einen Blick:

## P2V auf einen Blick

### Vorüberlegungen zur Virtualisierung

- ▶ Welche Hardware kann Probleme bereiten (z.B. ISDN-Karten, Dongles, FireWire)?
- ▶ Prüfen von CPU-Auslastung, Speicherbedarf, Netzwerkbandbreite der Quelle.
- ▶ Planen der Plattenaufteilung und der Netzwerkstruktur.

- ▶ Welche Software kann Probleme bereiten (z.B. hardwareabhängige Registrierung und Lizenzierung)?
- ▶ Testmigration des Quellsystems in eine VM durchführen.

### **Vorbereitung des Quellsystems**

- ▶ Sicherheits-Image der Systempartition und Datensicherung durchführen!
- ▶ Verzeichnisse und Dateien ausdünnen und aufräumen.
- ▶ Kritische Dienste deaktivieren (z.B. Exchange, Datenbanken).
- ▶ IP-Konfiguration und Laufwerksbezeichner notieren.
- ▶ IDE- oder SCSI-Treiber für virtuelle Hardware vorinstallieren.

### **Quellsystem in Ziel-VM übertragen**

- ▶ Image der vorbereiteten Systempartition erstellen.
- ▶ Image auf neue virtuelle Platte übertragen.
- ▶ Alten Server zur Sicherheit vom Netzwerk trennen!

### **Boot-Fehlerbehebung in der Ziel-VM**

- ▶ Boot-Partition aktivieren.
- ▶ MBR neu schreiben.
- ▶ CHS-Geometrie aktualisieren.
- ▶ Boot.ini anpassen.
- ▶ Alte Treiber und DLLs umbenennen und entfernen.
- ▶ HAL auf Single-CPU ändern oder als vorläufige Alternative eine VM mit zwei virtuellen CPUs erstellen (nur VMware).

### **Nacharbeiten in der Ziel-VM**

- ▶ VMware Tools installieren.
- ▶ Ereignisprotokoll auf Fehler kontrollieren.
- ▶ Alte Treiber und Programme entfernen.
- ▶ Netzwerkkarten neu konfigurieren.
- ▶ Laufwerk C: defragmentieren.
- ▶ Optional eine zusätzliche virtuelle Platte für die Auslagerungsdatei einrichten und die Auslagerungsdatei verschieben.
- ▶ Daten mittels Datensicherung und Agenten auf zusätzliche leere virtuelle Platten zurückspielen.
- ▶ Deaktivierte Dienste wieder starten und aktivieren.

## **6.7 V2P – Gast wieder zurück auf physische Hardware verschieben**

Es kann Situationen geben, in denen es notwendig ist, das System aus einer VM wieder auf eine physische Maschine umzusetzen, z.B. bei Performanceproblemen oder bei neuer benötigter Hardware, die nicht in einer VM unterstützt wird (z.B. PCI-Dongles für bestimmte

Software). Der häufigste Fall für einen V2P-Vorgang dürfte eintreten, um Mustersysteme, die in einer VM erstellt wurden, auf die endgültige Hardware umzusetzen. So kann es sehr praktisch sein, in einer VM ein Client-Rollout vorzubereiten oder einen Musterserver für eine Terminalserverfarm Schritt für Schritt aufzubauen. Erst wenn alle Funktionen und Applikationen ausreichend getestet wurden, erfolgt die Übertragung auf die Ziel-Hardware.

Der V2P-Vorgang unterscheidet sich nicht von dem im Workshop beschriebenen Ablauf einer P2V-Migration. Der wichtigste Schritt ist wieder die Vorinstallation des Controllertreibers im Gastsystem der VM, bevor ein Image erstellt und übertragen wird. Diesmal muss natürlich der Controllertreiber der Ziel-Hardware installiert werden. Das gelingt nicht immer, weil sich viele Treiber nicht installieren lassen, wenn die entsprechende Hardware noch gar nicht eingebaut wurde. Wie Sie das Treiber-Setup überlisten können, erfahren Sie im Festplatten-Workshop von *Teil 3, Kapitel 3*.

## 6.8 Produkte und Tools zur automatisierten Virtualisierung

Mittlerweise gibt es am Markt einige Produkte, die den gesamten Vorgang der Virtualisierung, also des Übernehmens einer physischen Maschine in eine VM, automatisieren. Dabei werden auch wichtige Anpassungen am System in der VM vorgenommen, z.B. das Ändern des HAL auf eine Single-CPU oder auch die Installation der richtigen Treiber für den virtuellen Festplattencontroller. Mit dem Wissen aus diesem Workshop wird es Ihnen problemlos gelingen, die meisten Ihrer physischen Maschinen auch manuell zu migrieren. Sollten Sie aber vorhaben, viele Systeme zu virtualisieren, dann kann sich die Anschaffung eines P2V-Tools lohnen.

### 6.8.1 Kostenpflichtige P2V-Produkte

Nicht alle kostenpflichtigen Tools sind reine P2V-Produkte. Einige, wie z.B. DDChanger, sind dafür ausgelegt, Systeme von einer Hardware auf eine andere umzusetzen. Dabei wird nebenbei auch die „Hardware“ virtueller Maschinen mit unterstützt. Auch der umgekehrte Vorgang (V2P) ist möglich, also das Umsetzen einer virtuellen Maschinen wieder zurück auf physische Hardware.

#### VMware P2V Assistant

<http://www.vmware.com/products/p2v>

Der P2V Assistant von VMware überträgt mit Hilfe einer Boot-CD im Quellrechner und einer Hilfs-VM (kann auch ein physischer Rechner sein) das System auf eine virtuelle Platte und übernimmt auch das Ersetzen von Controllertreibern und HAL. Im Prinzip ist die Vorge-

hensweise genau die gleiche wie im Workshop, nur dass die Anpassung des Zielsystems automatisch erfolgt. Es können auch Images von Fremdherstellern verwendet werden. Das Tool kann separat erworben werden oder ist im Abo des VMware Technology Networks (VTN) mit enthalten: <http://www.vmware.com/products/vmtn/>.

Der P2V Assistant wird vom VMware Converter 3.0 abgelöst. Mehr dazufinden Sie in Teil 3, Kapitel 8.



### **Platespin PowerConvert**

<http://www.PlateSpin.com>

PowerConvert ist ein sehr mächtiges Tool zur automatischen Massmigration von Systemen in allen Richtungen, also P2V, V2P und auch P2P. Es bietet auch die direkte Verwendung von vorhandenen Image-Dateien anderer Hersteller, etwa Acronis oder Symantec (Ghost und LiveState). Weiterhin wird die Migration von RedHat-Linux unterstützt.

### **Leostream P>V Direct**

<http://www.Leostream.com>

P>V Direct ist ebenfalls ein vollautomatisches Tool zur Migration von Systemen auf physischen Maschinen in eine VM. Es bietet die sehr interessante Funktion, das System im laufenden Betrieb der Quellmaschine zu migrieren, ähnlich wie Sie es im Workshop für eine Testmigration mit dem Tool DriveSnapshot kennen gelernt haben. Datenbankapplikationen müssen dazu allerdings für die Dauer der Migration eingefroren werden.

### **Acronis Universal Restore**

<http://www.acronis.de/enterprise/>

Acronis Universal Restore dient eigentlich dazu, erstellte Images auch auf anderer Hardware wieder herzustellen, als auf dem gesicherten System. Dabei werden Controllertreiber und HAL im Zielsystem angepasst. Damit ist das Produkt in Verbindung mit Acronis True Image zum Erstellen des Images vom Quellsystem und zum späteren Übertragen und Anpassen in der VM eine sehr interessante Option für die Übertragung einzelner Server ohne viel Vorarbeit und manuelle Treiberanpassung.

### **DDChanger**

<http://www.helperapps.com>

DDChanger macht nichts anderes, als in Windows-Systemen offline die verschiedensten Controllertreiber unterschiedlicher Hersteller zu installieren. Dazu muss eine BartPE-CD vorbereitet werden, von wel-

cher der zu aktualisierende Rechner zu starten ist. Das ist notwendig, weil das eigentliche System ohne die richtigen Treiber nicht booten kann. Dann können Sie die gewünschten Treiber direkt auf der Systemplatte des Zielsystems einrichten. Um das Klonen und Übertragen des Systems müssen Sie sich allerdings mit einer Imaging-Software Ihrer Wahl selbst kümmern.

### **Verschiedene Disaster-Recovery-Tools**

Verschiedenste Anbieter von Sicherungssoftware haben mittlerweile eine Disaster-Recovery-Option, die es ermöglicht, ein Betriebssystem auch auf anderer Hardware als der gesicherten wiederherzustellen. Bei diesem Vorgang werden ebenfalls die Controllertreiber ersetzt, damit das wiederhergestellte System auf der neuen Hardware booten kann. Ein Beispiel ist Acronis Universal Restore, aber auch einige reine Backup-Lösungen beherrschen diese Funktion.

## **6.8.2 Kostenlose P2V-Tools**

Die kostenlosen Tools haben nicht den Funktionsumfang wie die kostenpflichtigen Produkte, können aber als Ergänzung zur manuellen Migration dienen. Eine Ausnahme ist der VMware Virtual Machine Importer, der bereits als Standardtool für eine kostenlose Virtualisierung bezeichnet werden kann.

### **VMware Virtual Machine Importer 2**

<http://www.vmware.com/products/vmimporter>

Der Virtual Machine Importer 2 war ursprünglich als Hilfe gedacht, um virtuelle Maschinen zwischen den VMware-Produkten zu migrieren bzw. um Microsoft VMs zu importieren. Er eignet sich aber mittlerweile auch sehr gut als Tool für die Virtualisierung. Beim Migrieren einer VM ersetzt der Importer nämlich automatisch in den virtuellen Systemplatten die Controllertreiber mit dem passenden Modell für die Ziel-VM. Mit dem Menüpunkt ADAPT steht diese Funktion sogar zum nachträglichen Anpassen einer VM zur Verfügung. Sie können diesen Menüpunkt auf eine geklonte VM anwenden, die beim Bootvorgang in einen Stopp-Fehler 00007b läuft.

Ein weiteres Highlight ist der direkte Import von Images, die mit Symantec Lifestate erstellt wurden. Weitere Formate sind nach Aussagen von VMware geplant, so dass sich der Virtual Machine Importer 2 zum ultimativen kostenlosen P2V-Tool entwickeln könnte. Vom Quellsystem ist nur noch ein Image anzufertigen, das direkt importiert und als VM exportiert werden kann. Um die eine oder andere Anpassung werden Sie zwar trotzdem nicht herumkommen, und es ist gut, die Grundlagen zu kennen, aber dieses Tool kann die Virtualisierung stark vereinfachen.

## Virtual Server Migration Toolkit (VSMT)

<http://www.microsoft.com/germany/virtualserver/downloads/vsmt.mspx>

VSMT ist keine automatisierte Lösung. Vielmehr bietet es die Möglichkeit, mittels Skripten und einiger Microsoft-Tools eigene automatisierte Lösungen für P2V-Vorgänge zu konfigurieren. Dazu sind allerdings die Windows Server 2003 ADS (Automated Deployment Services) notwendig, was eine Windows Server 2003 Enterprise Edition erfordert.

## Ultimate-P2V

[http://www.rtfm-ed.co.uk/?page\\_id=174](http://www.rtfm-ed.co.uk/?page_id=174)

Ultimate-P2V ist ebenfalls kein automatisches P2V-Tool. Basierend auf einer BartPE-CD können Sie mit diesem kostenlosen Tool nachträglich die Treiber für die virtuellen Controller im Zielsystem installieren, ohne dass dieses System laufen muss. Ultimate-P2V funktioniert damit ähnlich wie der kostenpflichtige DDChanger, bietet aber nur Treiber für einen P2V-Vorgang unter VMware. In den mitgelieferten Registry-Dateien sind auch die notwendigen Einträge zum manuellen „Impfen“ der Registry mit den richtigen SCSI-Treibern ersichtlich (siehe Abschnitt 6.5.10, „Registry des Zielsystems nachträglich ändern“).





# 7 Nützliche Zusatzprodukte, Tools, Links und Tipps

Einige Zusatzprogramme und Tipps erleichtern die Arbeit mit virtuellen Maschinen. Hier finden Sie eine Auswahl nützlicher Tools, Fremdherstellerprodukte und interessanter Informationsquellen im Internet. Weiterhin gibt es Hinweise und Beispiele zum Skripting und zum Erstellen von Vorlagen für geklonte VMs.

**Klonen, Scripting, Tools und Tipps**

## Aktuelle Linkliste auf [www.vmaschinen.de](http://www.vmaschinen.de)

Die Linkliste finden Sie ständig aktualisiert auf meiner Webseite <http://www.vmaschinen.de>, da sich Links ändern können oder neue hinzukommen. Außerdem ersparen Sie sich damit das Abtippen der Links in den Browser, wenn Sie zu den Webseiten gelangen wollen.



## 7.1 Tools und Hilfsprogramme für die Arbeit mit virtuellen Maschinen

Für den Umgang mit virtuellen Maschinen sind einige Zusatzprogramme nützlich, die nicht immer direkt mit Virtualisierung zu tun haben. Der Texteditor zum direkten Editieren der Parameter virtueller Platten, das Programm zum Erstellen von ISO-Images oder ein Tool, was den belegten Platz eines Rechners bildlich darstellt. Hier finden Sie einige Vorschläge, zum großen Teil handelt es sich um Tools, die ich selbst in der Praxis einsetze.

### 7.1.1 Klonen von Mustervorlagen mit NewSID oder Sysprep

Wenn Sie Mustervorlagen für virtuelle Maschinen erstellen, dann müssen Sie in jedem erzeugten Klon für eindeutige IP-Adressen, Rechnernamen und gegebenenfalls auch für eine eindeutige *SID* (*Security Identifier*) in Windows-Gästen sorgen. Sie können das Ändern der SID nach dem Klonen in jedem Gast mit dem Tool *newsid* manuell erledigen oder vor dem Klonen in der Muster-VM bereits mit *sysprep* vorbereiten, so dass beim ersten Start automatisch eine Art Minisetup abläuft. Wie Sie den Master vor dem Klonen weiterhin vor-

bereiten sollten, z.B. Dateisystem aufräumen und verschiedene Einstellungen treffen, das finden Sie unter *Abschnitt 7.1.2, „Vorlagen und Templates (Master-Images) erstellen“*.



Für Clients einer Testumgebung ist der zeitaufwändige Vorgang der SID-Änderung nicht unbedingt notwendig, es genügt, wenn Sie in der Netzwerkumgebung den Rechnernamen und die IP-Adresse ändern (oder Sie verwenden DHCP). Lesen Sie dazu auch den sehr guten Artikel zur SID auf der unten genannten Seite von Sysinternals.

### **NewSID generiert eine SID im Klon nach dem Kopieren der VM**

*NewSID* setzt *nach* dem Klonen in jeder VM eine neue SID und ändert auf Wunsch auch gleich den Rechnernamen. Am besten Sie kopieren das Tool in die Vorlage-VM und führen es bei Bedarf in den Klonen aus:

<http://www.sysinternals.com/Utilities/NewSid.html>

### **Sysprep bereitet die Muster-VM auf das Kopieren vor**

*Sysprep* setzt *vor* dem Klonen Ihr Muster zurück und startet danach in jeder Kopie beim ersten Bootvorgang mit einem Minisetup, das u.a. den Rechnernamen und den Product Key abfragt und auch eine neue SID generiert. Die benötigten Dateien befinden sich in den Support-Tools auf der Windows-CD, in der Datei `\support\tools\deploy.cab`, oder Sie installieren die kompletten Tools mittels `\support\tools\supporttools.msi`. Gehen Sie zur Vorbereitung auf das Klonen folgendermaßen vor:

1. Kopieren Sie die Dateien *sysprep.exe* und *setupcl.exe* in ein Verzeichnis *sysprep* auf Ihrer virtuellen Festplatte im Gast.
2. Starten Sie *sysprep.exe* von der Festplatte.
3. Mit dem Haken an **MINISETUP VERWENDEN** und einem Klick auf **ERNEUT VERSIEGELN** bereitet Sysprep das System auf den nächsten Neustart vor und fährt es anschließend herunter.
4. Sie können die VM jetzt vervielfältigen. Beim Start eines jeden Klons läuft dann das Minisetup.

### **Antwortdatei für Sysprep zum Automatisieren erstellen**

Als Erweiterung von Sysprep können Sie mit dem Programm *setupmgr.exe* eine Antwortdatei *sysprep.inf* erstellen, in der Sie alle Parameter vom Product Key bis zur Domänenmitgliedschaft hinterlegen (siehe auch <http://support.microsoft.com/kb/298491/de>).



Ein Beispiel für eine fertig erstellte *sysprep.inf* finden Sie auf der Buch-CD.

1. Starten Sie *setupmgr.exe*, und wählen Sie ANTWORTDATEI NEU ERSTELLEN.
2. Wählen Sie SYSTEMVORBEREITUNGSINSTALLATION.
3. Folgen Sie dem Wizard, Beenden müssen Sie zum Schluss mit ABBRECHEN.
4. Legen Sie die erzeugte Datei *sysprep.inf* in der Muster-VM zusammen mit *sysprep.exe* und *setupcl.exe* in einem Verzeichnis *c:\sysprep* ab. Der Name und Ort müssen genau so lauten!
5. Starten Sie aus diesem Verzeichnis die *sysprep.exe*, um das System zu versiegeln, danach fährt die VM herunter, und Sie können die VM vervielfältigen.

Das *Minisetaup* in jedem Klon holt jetzt seine Antworten aus der *sysprep.inf* und löscht anschließend das Verzeichnis *c:\sysprep*. Alles, was nicht in der Antwortdatei steht, fragt das Minisetaup ab, z.B. den Rechnernamen.

Klonen Sie keine Domänencontroller, sondern stufen Sie einen Server erst nach dem Klonen und nach dem Ändern der SID mit dem Befehl *dcpromo* zum Domänencontroller hoch. Tipps zum Umgang mit den MAC-Adressen virtueller Netzwerkkarten beim Klonen finden Sie in *Teil 3, Kapitel 2*.



### 7.1.2 Vorlagen und Templates (Master-Images) erstellen

Gehen Sie folgendermaßen vor, um eine möglichst schlanke Vorlage für weitere Klone zu erstellen:

1. Installation des Gastbetriebssystems von CD oder ISO-Image. Setzen Sie vorher keinen Snapshot, bzw. aktivieren Sie keinen Rückgängig-Datenträger, sonst landet die gesamte Installation im Redo-Log.
2. Installation der VMware Tools oder Virtual Machine Additions im Gast.
3. Aufspielen aller Service-Packs und Patches für das Gastsystem. Sollten Sie zum Testen Versionen ohne Service-Pack benötigen, kann das auch erst später in den Klonen erfolgen, so erzeugen Sie wiederum mehrere Vorlagen mit und ohne Patches.
4. Installation Ihrer bevorzugten Tools und Utilities im Gast.
5. Verschiedene Einstellungen, wie Abschalten des Bildschirmschoners und Abschalten von Anzeigeeffekten. Sie können z.B. auch die lästige Ereignisprotokollierung beim Herunterfahren unter Windows 2003 abschalten mittels *gpedit.msc*. Unter COMPUTERKONFIGURATION/ADMINISTRATIVE VORLAGEN/SYSTEM deaktivieren Sie EREIGNISPROTOKOLLIERUNG FÜR HERUNTERFAHREN ANZEIGEN.

6. Sicherungen von Service-Packs und Patches löschen, damit können Sie richtig Platz schaffen. Zuerst müssen Sie im Explorer unter EXTRAS/ORDNEROPTIONEN/ANSICHT dafür sorgen, dass Sie alle Dateien und Ordner und auch Inhalte von Systemordnern angezeigt bekommen, damit Sie alle Dateien sehen können.  
Dann löschen Sie im Ordner C:\WINDOWS\ folgende Unterordner:
  - ▶ \$NtServicePackUninstall\$
  - ▶ \$NtUninstallKBxxxxxx\$
7. Bereinigung des Dateisystems mit der Datenträgerbereinigung unter START/PROGRAMME/ZUBEHÖR/SYSTEMPROGRAMME/DATENTRÄGERBEREINIGUNG oder einfach mit dem Kommando *cleanmgr*. Wählen Sie alle Optionen außer ALTE DATEIEN KOMPRIMIEREN. Unter WEITERE OPTIONEN können Sie noch überflüssige Programme und Komponenten entfernen
8. Defragmentieren der Festplatte im Gastsystem.
9. *Shrink* ausführen (VMware) bzw. *Precompact* (Microsoft) – siehe Platten-Workshop in Teil 3, Kapitel 3.
10. Optional zum Abschluss *Sysprep* ausführen. Sie können später in den Klonen genauso auch *NewSID* laufen lassen (siehe Abschnitt 7.1.1, „Klonen von Mustervorlagen mit NewSID oder Sysprep“).

Nach dem Erstellen und Optimieren können Sie die komplette VM oder auch nur die virtuelle Systemplatte als Muster verwenden und kopieren bzw. linked Clones erstellen und Differenzplatten aufsetzen. Vor dem Kopieren der kompletten VM können Sie noch unnötige Hardware entfernen, etwa das Floppylaufwerk.

### 7.1.3 Platz sparen beim Archivieren oder Weitergeben von VMs

Um beim Transportieren oder Archivieren der virtuellen Maschinen möglichst viel Platz zu sparen, sollten Sie einige Vorkehrungen treffen:

- ▶ *Snapshots und Differenzplatten ausdünnen* – Jeder Snapshot belegt zusätzlichen Platz, da Sektoren der Platte in jedem Redo-Log (bzw. Differenzplatte bei Microsoft) mehrfach enthalten sein können. Löschen Sie im Snapshot-Manager alle unnötigen Snapshots, führen Sie unter Microsoft die Differenzplatten zusammen.
- ▶ *Snapshots im laufenden Betrieb* – Ein Snapshot im laufenden Betrieb sichert auch den RAM-Inhalt einer VM. Haben Sie der Maschine 256 MB RAM zugewiesen, dann entsteht bei jedem Snapshot eine Datei in dieser Größe. Entfernen Sie Snapshots, oder setzen Sie diese im ausgeschalteten Zustand der VM.
- ▶ *Kein Suspend* – Auch bei einem Suspend wird der RAM-Inhalt in einer Datei gespeichert. Also fahren Sie die VM richtig herunter vor der Weitergabe.

- ▶ *Platten in Segmente teilen* – Platten, die zu groß für eine DVD sind, können unter VMware mit folgendem Kommando nachträglich in 2-GB-Segmente aufgeteilt werden, wenn das bei der Erstellung verpasst wurde:

```
C:\Programme\VMware\VMware Workstation\vmware-
vdiskmanager.exe" -r quellplatte.vmdk -t 1
zielplatte.vmdk
```

- ▶ *Platten mit Shrink verkleinern* – Zuwachsplatten belegen zwar nur den Platz, der in der VM wirklich belegt ist. Wurden Inhalte im Gast wieder gelöscht, werden Zuwachsplatten aber nicht automatisch kleiner. Die Shrink-Funktion der VMware-Tools gibt nicht benötigten Platz von Zuwachsplatten wieder frei bzw. komprimiert virtuelle Festplatte (Microsoft), siehe *Teil 3, Kapitel 3*.
- ▶ *Separate virtuelle Platte für das Swapfile* – Auch das Swapfile im Gastsystem einer VM benötigt Platz. Liegt es auf einer extra Platte, können Sie diese vor dem Brennen mit einer Version ersetzen, in der das File noch leer war.
- ▶ *Komprimierung* – Die VMs zu komprimieren spart zwar Platz, benötigt aber sehr viel Zeit zum Auspacken. Sinnvoller kann eine Verwendung von komprimierten Dateisystemen in den VMs selbst sein.

#### 7.1.4 Invirtus Virtual Machine Optimizer spart Platz in virtuellen Maschinen

Eine sehr komfortable Alternative, um Muster-VMs vorzubereiten oder vorhandene Gäste möglichst platzsparend zu verkleinern, ist der *Invirtus Virtual Machine Optimizer*. Er arbeitet mit VMs von VMware und Microsoft zusammen und nimmt Ihnen die manuelle Arbeit ab, Ihre virtuellen Maschinen, die Gastsysteme und die virtuellen Platten zu optimieren und den Platz freizugeben. Bei vielen VMs und in größeren Testumgebungen lohnt sich die Anschaffung der preiswerten Software auf jeden Fall.

<http://www.invirtus.com>

#### 7.1.5 TweakUI aus den Microsoft PowerToys

*TweakUI* hat eigentlich nichts mit virtuellen Maschinen zu tun, es bietet eine Oberfläche, um unterschiedlichste Systemeinstellungen von Windows an einer zentralen Stelle zu verwalten. Es kann gute Dienste für eine Vorlage-VM leisten, beispielsweise um einzustellen, dass die VM beim Hochfahren automatisch mit einem bestimmten Nutzer angemeldet wird.

<http://www.microsoft.com/windowsxp/downloads/powertoys/xppowertoys.mspx>

### 7.1.6 CD-Tools – ISO Images erstellen und mounten

Erstellen Sie aus häufig benötigten CDs am besten ein ISO-Archiv, weil ISO-Images schneller „eingelegt“ sind als echte Scheiben und nicht zerkratzen.

#### Tools, um ISO-Images zu erstellen

**WinISO:** <http://www.winiso.com/>

**UltraISO:** <http://www.ezbsystems.com/ultraiso/main.htm>

**LC ISO Creator** (klein und kostenlos): <http://www.lucersoft.com/freeware.php>

**WinImage** ermöglicht als besondere Funktion auch das mounten von Microsofts virtuellen Platten (\*.vhd) am Host, ähnlich dem Tool VMware Disk Mount (siehe auch Teil 3, Kapitel 3):

<http://www.winimage.com/winimage.htm>

#### ISO-Images auch am Host unter Windows oder Linux mounten

Um ein ISO-Image auch am Host anstelle einer echten CD zu verwenden, können Sie es auch direkt mounten. Damit können Sie Ihre ISO-Sammlung nicht nur in VMs benutzen, sondern auch an einem physischen PC.



Bei Virtual PC ist das übrigens die einzige Möglichkeit, ein ISO-Image von einer DVD, das größer als 2,2 GB ist, dem Gastsystem zur Verfügung zu stellen. Mounten Sie die CD am Host, geben Sie diese im Netzwerk frei, und verbinden Sie sich im Gast auf diese Freigabe. Um von der DVD zu booten (z.B. Installation Windows Vista), müssen Sie die DVD brennen und physisch ins Laufwerk einlegen.

**Virtual CD Control Panel** – Microsofts einfaches und effektives Tool zum Mounten von ISO-Images:

[http://download.microsoft.com%2fdownload%2f7%2fb%2f6%2f7b6abd84-7841-4978-96f5-bd58df02efa2%2fwinxpvirtualcdcontrolpanel\\_21.exe](http://download.microsoft.com%2fdownload%2f7%2fb%2f6%2f7b6abd84-7841-4978-96f5-bd58df02efa2%2fwinxpvirtualcdcontrolpanel_21.exe)

**Daemon Tools** – sehr umfangreiches Tool für virtuelle CDs:

<http://www.daemon-tools.cc>

**Unter Linux** funktioniert das Mounten mit einem einfachen Befehl:

```
mount -o loop -t iso9660 mein_image.iso /mnt/isoimage/
```

### 7.1.7 Virtuelle Festplatten erstellen, verwalten und mounten

Die Handhabung der Tools *vmware-vdiskmanager.exe* und *vmware-diskmount*, um virtuelle Festplatten zu erstellen, zu konvertieren oder direkt am Host zu mounten, finden Sie im Platten-Workshop von Teil 3, Kapitel 3. Dort finden Sie auch Anleitungen zu Microsofts *SCSI Shunt Driver* oder VMwares optimierten SCSI-Treibern.

**VMware SCSI-Treiber und VMware Disk Mount:**

[http://www.vmware.com/download/ws/drivers\\_tools.html](http://www.vmware.com/download/ws/drivers_tools.html)

**Grafische Oberflächen für die VMware-Kommandozeilentools:**

<http://petruska.stardock.net/software/VMware.html>

### 7.1.8 Sonstige Tools – Editoren, Fernsteuerung, kleine Helferlein

Weitere kleine Hilfsprogramme im Gast oder auf dem Host:

**SequoiaView** stellt den belegten Platz auf einer Festplatte grafisch dar und ermöglicht so das Aufspüren von Dateileichen und Platzverschwendern vor P2V oder Shrink:

<http://www.win.tue.nl/sequoiaview/>

**Process Explorer** von Sysinternals zeigt auf einem Windows-Host übersichtlich alle laufenden Prozesse mit mehr Funktionen als der Windows Taskmanager. Auf der Webseite existieren viele weitere nützliche Tools, z.B. der File Monitor zum Überwachen von Dateizugriffen oder auch NewSID:

<http://www.sysinternals.com/>

**UltraEdit** ist ein Texteditor, der einige Funktionen beherrscht, die bei der Manipulation von Dateien virtueller Maschinen nützlich sind, z.B. die richtige Anzeige von Textdateien im Unix-Format (z.B. Kopfdateien der virtuellen Platten) und direktes Editieren von sehr großen Dateien (z.B. monolithische virtuelle Platten), weiterhin Quelltextformatierung von Perl, eine Hex-Ansicht und spaltenorientiertes Editieren:

<http://www.ultraedit.com>

**RealVNC** ist eine Fernsteuerungssoftware für Windows und Linux-Desktops, mittlerweile in vielen Derivaten verfügbar:

<http://www.realvnc.com/>

**Radmin** ist schneller als VNC, aber nicht kostenlos:

<http://www.radmin.com/de/>



**Putty** ist ein Terminalprogramm zum Verbinden mit dem ESX Server oder mit einem Linux-Host:

<http://www.putty.nl/>

**WinSCP** dient zur Dateiübertragung zum ESX Server oder zum Linux-Host:

<http://www.winscp.net>

### 7.1.9 Imaging Tools und Notfall-CDs BartPE bzw. Knoppix

Einige Werkzeuge, die Sie auch für physische Rechner im Notfall benötigen, leisten in virtuellen Maschinen vor allem bei P2V-Vorgängen gute Dienste.

#### Imaging Tools zum Übertragen physischer oder virtueller Rechner

Mit Imaging Tools können Sie von physischen Maschinen Abbilder erstellen, um sie in virtuelle Maschinen zu übernehmen (P2V – siehe *Teil 3, Kapitel 6*). Auch das Übertragen des Gastsystems von einer virtuellen IDE auf eine virtuelle SCSI-Platte oder auf eine größere Platte ist damit möglich (siehe *Teil 3, Kapitel 3*). Hier finden Sie eine kleine Auswahl solcher Programme:

**Drive SnapShot** ist eine sehr handliche Image-Lösung, die sich als einfache \*.exe ohne Installation sofort starten lässt. Damit kann ohne Installation oder Neustart die Systempartition eines Servers im laufenden Betrieb gesichert werden, etwa für eine Testmigration. Leider existiert keine bootfähige CD, für konsistente Sicherungen im heruntergefahrenen Zustand ist BartPE o.Ä. notwendig:

<http://www.drivesnapshot.de/>

**Acronis True Image** ist eine sehr zuverlässige Image-Lösung mit bootfähiger CD und Unterstützung von Netzwerk sowie USB. Weiterhin unterstützt Acronis auch die automatische Anpassung des geklonten Systems an die neue Hardware mit dem Tool *Acronis Universal Restore* (siehe auch P2V Workshop in *Teil 3, Kapitel 6*):

<http://www.acronis.com>

**Symantec Livestate Recovery** bietet den großen Vorteil, dass die erstellten Images direkt mit dem VMware Virtual Machine Importer eingelesen werden können:

<http://www.symantec.com/>

## Notfall-CDs BartPE und Knoppix

Notfall-CDs, auch Live-CDs genannt, ermöglichen das Booten eines Minimalbetriebssystems von einer CD, z.B. um eine kaputte Installation auf der Festplatte zu reparieren. Sie bieten eine komfortable grafische Oberfläche mit verschiedenen Tools, vom Datei-Explorer bis zu Imaging-Tools. In virtuellen Maschinen als ISO-CD gestartet, können Sie damit z.B. die Boot.ini anpassen oder Treiber nach einem P2V-Vorgang nachträglich ersetzen. Die etabliertesten Notfall-CDs sind *BartPE* für die Windows-Welt und *Knoppix* für Linux:

<http://www.nu2.nu/pebuilder/>

<http://www.knopper.net/knoppix/>

## 7.2 Scripting zur Fernsteuerung von VMs oder zur Automatisierung

Vor allem bei der Datensicherung sind Skripte nützlich, um VMs automatisch in den Suspend-Modus zu bringen, herunterzufahren oder zu starten.

### 7.2.1 Skripte für Microsoft Virtual Server

Viele nachvollziehbare Beispielskripte für Microsoft Virtual Server finden Sie im *Virtual Server Script Repository* – eine Sammlung mit Beispielen zu allen Belangen, selbsterklärend :

<http://www.microsoft.com/technet/scriptcenter/scripts/vs/default.aspx?mfr=true>

Ein Beispielskript für die Verwendung des *Volume Shadow Copy Service* (VSS) für ein Hot Backup von Gästen unter Virtual Server finden Sie hier:

[http://www.adminnotes.com/index/2006/01/virtual\\_server\\_.html](http://www.adminnotes.com/index/2006/01/virtual_server_.html)

Um selbst Skripte für die Datensicherung mittels Schattenkopien im Gast oder auf dem Host zu erstellen, existiert das Tool *vshadow.exe* aus den *Volume Shadow Copy Service SDK 7.2*:

<http://www.microsoft.com/downloads/details.aspx?FamilyID=0b4f56e4-0ccc-4626-826a-ed2c4c95c871&DisplayLang=en>

### 7.2.2 Skripte für VMware Server oder Workstation

Unter VMware Server oder Workstation können Sie mit Skripten einiges automatisieren. Ohne Programmierkenntnisse ist der einfachste Weg die Verwendung der Tools *vmware-cmd* und *vmrun.exe*.



Einige Beispielskripte für *vmware-cmd* und *vmrun* finden Sie auf der Buch-CD.

#### vmware-cmd – VMware Perl API

Die VMware Perl API kann sehr komfortabel mit *vmware-cmd* über die Kommandozeile oder aus Skripten bedient werden, hier sind einige Beispiele. Damit können Sie beispielsweise vor der Datensicherung VMs automatisch herunterfahren und danach wieder starten. Die *vmware-cmd.bat* befindet sich auf dem Host im Verzeichnis *C:\Programme\VMware\VMware VmPerl Scripting API\*. Auf dem ESX Server hat sie einen erweiterten Funktionsumfang.



Beachten Sie Groß-/Kleinschreibung bei den Parametern! Die Parameter *-H*, *-U* und *-P* müssen am lokalen Host nicht angegeben werden, nur bei Remote-Zugriffen.

Sämtliche Parameter des Befehls anzeigen lassen:

```
vmware-cmd -h
```

Alle VMs eines Hosts auflisten lassen:

```
vmware-cmd -H mein_host -U nutzer -P passwort -l
```

Eine bestimmte VM registrieren, also ins Inventory aufnehmen (entfernen mit *unregister*):

```
vmware-cmd -H mein_host -U nutzer -P passwort -s
register "pfad\zur\vm\config.vmx"
```

Eine VM abschalten. Durch *trysoft* versucht VMware, das Gastsystem über die VMware Tools vorher ordentlich herunterzufahren (weitere Parameter sind *getstate*, *start*, *stop*, *reset*, *suspend*):

```
vmware-cmd -H mein_host -U nutzer -P passwort "pfad\
zur\vm\config.vmx" stop trysoft
```



Den Power-Status einer VM (*on/off*) mit *getstate* in einer Batch-Datei abzufragen ist etwas kompliziert, Sie finden ein Beispielskript auf der Buch-CD.

Ein Redo-Log im laufenden Betrieb zuschalten (nur am ESX Server möglich, siehe auch *Teil 2, Kapitel 9*). Dieser Befehl setzt einen Snapshot, mit *Quiescing* (Parameter 1) und ohne den RAM-Inhalt zu sichern (die 0 als zweiter Parameter):

```
vmware-cmd /vmfs/volumes/vmfs-id/test99/test99.vmx
createsnapshot "snap1" "vor Hotbackup" 1 0
```

### vmrun.exe – VMware-Programmierschnittstelle (VIX API)

Einige Funktionen der VMware-Programmierschnittstelle (VIX API), können Sie von der Kommandozeile mit dem Programm *vmrun.exe* verwenden. Damit lassen sich unter VMware Server einige Funktionen ausführen, die mit *vmware-cmd* nicht möglich sind, z.B. Snapshots setzen. Sie finden das Programm auf dem Host im Ordner *C:\Programme\VMware\VMware VIX\vmrun.exe* und auch für die VMware Workstation unter *C:\Programme\VMware\VMware Workstation*.

Zeigt alle verfügbaren Parameter:

```
vmrun.exe -?
```

Setzt einen Snapshot, auch im laufenden Betrieb:

```
vmrun.exe -h mein_host -u nutzer -p passwort snapshot
"pfad\zur\vm\config.vmx"
```

Löscht einen Snapshot und konsolidiert die Redo-Logs, das geht nur im abgeschalteten Zustand bzw. im Suspend-Modus:

```
vmrun.exe -h mein_host -u nutzer -p passwort
deleteSnapshot "pfad\zur\vm\config.vmx"
```

Schaltet eine VM hart ab (oder Parameter *suspend*):

```
vmrun.exe -h mein_host -u nutzer -p passwort stop
"pfad\zur\vm\config.vmx"
```

### Skripte im Gast über die VMware Tools ausführen

Zusätzlich können Sie im Gast im Verzeichnis *Programme\VMware\VMware Tools* Skripte hinterlegen, die bei bestimmten Aktionen von den VMware Tools automatisch abgearbeitet werden. Das Standard-skript *resume-vm-default.bat* sorgt beispielsweise dafür, dass der Gast nach dem Erwachen aus dem Suspend-Modus eine neue IP-Adresse über DHCP bezieht. Weitere Skripte können bei Power-On, Suspend oder PowerOff ausgeführt werden.

Das muss in den Einstellungen des Gastes unter *VM/SETTINGS/OPTIONS/POWER/RUN VMWARE TOOLS SKRIPTS* eingeschalten sein, und im Tray Icon der VMware Tools finden Sie unter *SCRIPTS* ebenfalls entsprechende Einstellungen.



### 7.2.3 psexec.exe – Tool zum Starten von Skripten in Windows-Gästen

Mit *psexec.exe* können Sie in Windows-Gästen hinterlegte Skripte starten, z.B. vor der Datensicherung. Sie finden das Programm hier: <http://www.sysinternals.com/utilities/psexec.html>

Der Parameter *meine\_vm* ist die IP-Adresse oder der Name des Gastes:

```
psexec.exe \\meine_vm -u nutzer -p passwort "pfad\zum\skript\skript.bat"
```

In der Datei *skript.bat* im Gast können Sie z.B. einen bestimmten Dienst beenden oder mit einem anderen Skript starten:

```
net stop "Name des Dienstes"
net start "Name des Dienstes"
```

Oder Sie können das Betriebssystem, trotz Meldungen und offener Applikationen, herunterfahren. Die *shutdown.exe* ist bei Windows XP/2003 mit dabei, sonst zu finden im *Windows 2000 Resource Kit*:

```
shutdown /s /t 0 /f
```

### 7.2.4 DevCon – Windows-Gerätemanager per Kommandozeile

In Zusammenhang mit Skripten ist noch das Windows-Tool *DevCon* interessant, mit dem Sie unter Windows den Gerätemanager per Kommandozeile bedienen können, um beispielsweise Netzwerkarten ab- oder anzuhängen:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;Q311272>

### 7.2.5 AutoIT – kostenloses mächtiges Scripting Tool für alle Belange

Um am Host oder in den Gästen komplexere Automatisierungen vorzunehmen, sollten Sie sich das kostenlose Tool *AutoIT* anschauen, mit dem Sie sogar fertige Skripte als ausführbare \*.exe-Dateien kompilieren können:

<http://www.autoitscript.com/>

<http://www.german-autoit.de/>

## 7.3 Fremdherstellerprodukte zur Verwaltung virtueller Maschinen

Mittlerweile existieren einige Hersteller, die für virtuelle Umgebungen Software anbieten. Das reicht von der Datensicherung bis zur komfortablen Verwaltung von Test- und Laborumgebungen. Mit einigen dieser Zusatzprodukte kann Ihre virtuelle Infrastruktur deutlich an Wert gewinnen.

**Sicherung,  
Verwaltung,  
Workflow**

### 7.3.1 Komfortable Oberfläche VSPlus für Microsoft Virtual Server

*VSPlus* für den Microsoft Virtual Server 2005 ist eine grafische Oberfläche, welche die Verwaltung mehrerer VMs auf unterschiedlichen Hosts erleichtert:

<http://citynav.com/vsplus/>

### 7.3.2 Dunes VS-O und VD-O – Workflow und Automatisierung (VMware und Microsoft)

*Dunes VS-O (Virtual Service Orchestrator)* ist eine umfangreiche Software zur Abbildung und Automatisierung von Arbeitsabläufen vor allem in größeren virtuellen Umgebungen mit VMware Virtual Center und Microsoft Virtual Server. Damit können Sie Ihre Infrastruktur sehr effektiv verwalten und Aufgaben besser delegieren. Ein Vorgang wäre z.B. die Beantragung einer virtuellen Maschinen durch einen Anwender über ein zentrales Interface, die automatische Weiterleitung an einen zuständigen Admin und der Abschluss des Vorganges durch die Bereitstellung der VM. Der gesamte Arbeitsablauf kann in einer grafischen Übersicht modelliert werden. Automatisierung, Überwachung, Sicherung, Wiederherstellung, Rechteverwaltung und Benachrichtigung sind einige Schlagwörter zu den umfassenden Möglichkeiten der Software.

*Dunes VD-O (Virtual Desktop Orchestrator)* verwaltet dagegen virtuelle Desktops der VMware Virtual Desktop Infrastructure (siehe in Teil 1, Kapitel 2, bei Die weiteren VMware-Produkte im Überblick).

<http://www.dunes.ch>

Sie finden auf den Seiten auch sehr aussagekräftige Online-Demos und Tutorials.

### 7.3.3 Platespin PowerRecon – Überwachung und Inventarisierung zur P2V Vorbereitung

*PowerRecon* dient eigentlich zur Überwachung und Inventarisierung kompletter Rechenzentren und liefert verschiedene Auswertungen zu den vorhandenen Servern und Diensten. Das können Sie sehr gut zur Vorbereitung auf eine Virtualisierung und zum Planen der Hardware Ihrer Hosts anhand der vorhandenen Auslastung der physischen Systeme nutzen.

*PlateSpin PowerConvert* dient zum Übertragen von Systemen zwischen Servern, physisch oder virtuell, siehe auch *Teil 3, Kapitel 6*.

<http://www.platespin.com/>

#### Weitere P2V-Tools zur Übernahme physischer Maschinen

Viele Tools, die Ihnen das Übernehmen physischer Maschinen in Ihre VM erleichtern oder sogar komplett automatisieren, finden Sie mit- samt Beschreibung in *Teil 3, Kapitel 6, Physische Server in virtuelle Maschinen übernehmen*.

### 7.3.4 Vizioncore esxMigrator, esxRanger, esxReplicator, esxCharter für ESX Server

Von der Firma Vizioncore stammen verschiedene etablierte Programme für den ESX Server, z.B. zur Migration auf ESX 3:

- ▶ *esxMigrator* – Migration Ihrer Infrastruktur von ESX Server 2 auf Virtual Infrastructure 3 (ESX Server3 mit Virtual Center 2). Der Umstieg wird dadurch automatisiert und vereinfacht, vor allem in größeren Umgebungen.
- ▶ *esxRanger* – Komfortable Sicherung und Wiederherstellung virtueller Maschinen auf dem ESX Server mit Hot Backup. Integration ins Virtual Center und dateibasierte Rücksicherungen sind möglich.
- ▶ *esxReplicator* – Repliziert laufende VMs in Echtzeit (je nach Verbindung) auf einen zweiten ESX Server im LAN oder über WAN-Verbindungen. Diese Lösung kann als preiswerte Alternative zu SAN-Spiegelungen eingesetzt werden.
- ▶ *esxCharter* – Auswertungen sowie Leistungsüberwachung und Optimierung auf dem ESX Server.

<http://www.vizioncore.com/>

### **7.3.5 Datensicherung ESX Server**

Für den ESX Server existieren einige spezielle Sicherungsprogramme, die in *Teil 3, Kapitel 5*, kurz vorgestellt werden. Die Links zu den Herstellern finden Sie hier nochmals als Übersicht:

- ▶ FalconStor Application Snapshot Director for VMware ist ein Zusatztool zur konsistenten Sicherung von Datenbanken:  
<http://www.falconstor.com/>
- ▶ Vizioncore esxRanger und esxReplicator:  
<http://www.vizioncore.com/>
- ▶ esXpress:  
<http://www.esxpress.com/>
- ▶ aeXia Virtual Solution Box (VSB):  
<http://www.aexia.ch/>
- ▶ kostenloses Backup-Skript für den ESX Server:  
<http://www.vmts.net/vmbk.htm>

## **7.4 Links zu Downloads, weiteren Informationen und aktuellen Meldungen**

Im Internet existieren eine ganze Reihe von Blogs und Informationsseiten zu den im Buch vorgestellten Produkten und zu allgemeinen Themen der Virtualisierung. Die informativsten habe ich hier für Sie zusammengestellt. Inhalte auf Deutsch sind leider eher selten, die englischen Seiten sind oft aktueller und auch informativer.

### **7.4.1 Seiten mit Informationen zu VMware und Microsoft**

- ▶ Blog mit sehr gut sortierten Verweisen und Links zu allen Themen der Virtualisierung – sehr interessant zum Stöbern:  
<http://www.run-virtual.com/>
- ▶ Informative Seite mit aktuellen Meldungen, Artikeln zu allen Themen der Virtualisierung und Verweisen zu HowTos:  
<http://vmblog.com/>
- ▶ Alessandro Perillis Seite zum Thema Virtualisierung mit Interviews, Neuigkeiten, Hintergründen:  
<http://www.virtualization.info/>
- ▶ Meldungen und Artikel zum Thema, teilweise Registrierung erforderlich:  
<http://www.virtual-strategy.com/>



- ▶ Deutsche Seite mit aktuellen Meldungen zu allen Themen der Virtualisierung und Verweisen zu Artikeln und HowTos auf anderen Webseiten:

<http://www.vmachine.de/>

#### 7.4.2 Links VMware – alle Produkte

- ▶ Das englische Forum zu den VMware-Produkten – die erste Anlaufstelle bei Fragen und Problemen:

<http://www.vmware.com/community/>

- ▶ Das inoffizielle deutsche Forum, nicht ganz so umfangreich wie das englische, aber mit vielen freundlichen Helfern in deutscher Sprache:

<http://vmware-forum.de/>

- ▶ Hacks zu VMware Player, Workstation und Server, teilweise auch auf Deutsch:

<http://sanbarrow.com/>

- ▶ Meine Seite mit deutschsprachigen Tipps und ausführlichen HowTos und Anleitungen zu virtuellen Maschinen, Schwerpunkt VMware:

<http://www.vmaschinen.de/>

#### 7.4.3 Links VMware – Schwerpunkt ESX Server

- ▶ Infos, Tipps und sehr gute HowTos zum ESX Server und Virtual Center:

<http://www.rtfm-ed.co.uk/>

z.B. eine Beschreibung der Service Console oder eine Anleitung zum Upgrade auf ESX Server 3:

<http://www.rtfm-ed.co.uk/docs/vmwdocs/ESX3.x-VC2.x-ServiceConsole-Guide.pdf>

<http://www.rtfm-ed.co.uk/docs/vmwdocs/ESX3.x-VC2-upgradeguide.pdf>

- ▶ Tipps mit Schwerpunkt ESX Server 2.5:

<http://trivore.com/vmware/>

- ▶ Schweizer Testcenter zum Mieten mit Remote-Zugriff über das Internet:

<http://www.kybernetika.ch/setc.htm>

#### **7.4.4 Links Microsoft Virtual PC**

- ▶ Offizielle Microsoft-Seiten (die englischen sind häufig aktueller):  
<http://www.microsoft.com/windows/virtualpc/>  
<http://www.microsoft.com/germany/windows/virtualpc>
- ▶ Virtual PC Guy's WebLog – Tipps, Tricks, Links und aktuelle Meldungen zu Virtual PC, ebenfalls Tipps zu Virtual Server:  
[http://blogs.msdn.com/virtual\\_pc\\_guy/](http://blogs.msdn.com/virtual_pc_guy/)
- ▶ Robert Moirs Virtualisation Site – viele Tipps, FAQ und Best Practice zu Virtual PC:  
<http://www.robertmoir.co.uk/Virtualisation.html>
- ▶ Virtually Vista – Alles zu Windows Vista unter Virtual PC/Server:  
<http://blogs.msdn.com/mikekol/>

#### **7.4.5 Links Microsoft Virtual Server**

- ▶ Offizielle Microsoft-Seite (auch hier ist die englische Version aktueller und ausführlicher):  
<http://www.microsoft.com/windowsserversystem/virtualserver/>  
<http://www.microsoft.com/germany/virtualserver/>
- ▶ The Soul of a Virtual Machine – Tipps, Tricks, Links, HowTos und aktuelle Meldungen zu Virtual Server:  
<http://blogs.technet.com/megand/>
- ▶ Tipps, Tricks, HowTos zu Virtual Server und Virtual PC:  
<http://www.virtualserver.tv/>



# 8

# Aktualisierungen, Ergänzungen und Neuerungen zum Buch

Kaum ein anderes Thema im IT-Bereich ist derzeit mehr in Bewegung als Virtualisierung. Dieses Buch war gerade einmal drei Monate auf dem Markt, da gab es bereits neue Produkte und Versionen der Virtualisierungshersteller. Da durch das große Leserinteresse ein Nachdruck weiterer Buchexemplare erforderlich wurde, habe ich die Chance genutzt und den Inhalt um interessante Neuerungen erweitert.

Zusätzlich zu kleineren Korrekturen, die im Buch vorgenommenen wurden, finden Sie in diesem Kapitel ein paar umfangreichere Ergänzungen.

## 8.1 VMware Virtual Lab Manager für virtuelle Test- und Schulungsumgebungen

Virtuelle Testumgebungen erleichtern enorm die Arbeit in der IT – ganz egal, ob ein Techniker komplexe Netzwerke nachstellen will, ein Programmierer seinen Entwicklungsserver samt unterschiedlicher Clients immer mit dabei haben muss oder ob der Support das realistische Abbild einer Kundenumgebung benötigt. Neben den Desktopprodukten für den lokalen Arbeitsplatzrechner, wie VMware Workstation und Virtual PC, bieten sich die Serverprodukte VMware Server, ESX Server oder Microsoft Virtual Server für eine zentrale Bereitstellung virtueller Maschinen an. Damit hält der Vertrieb beispielsweise eine Kundendemo mit dem Laptop im Konferenzraum, wobei die VMs der Vorführungsumgebung auf einem leistungsfähigen Host im fernen Serverschrank laufen.

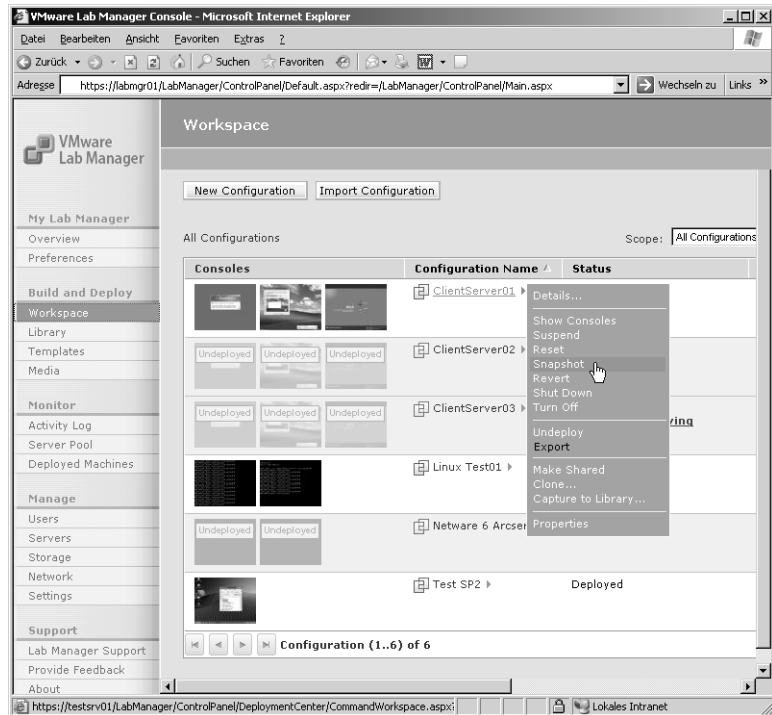
**Zentrale Schulungs-, Demo- und Testumgebungen verwalten**

### 8.1.1 Funktion und Komponenten des VMware Virtual Lab Manager

Managementtools, wie *VMware Virtual Center*, vereinfachen den Umgang mit virtuellen Infrastrukturen und vielen VMs deutlich. Für reine Testumgebungen fehlen diesen Verwaltungslösungen allerdings wichtige Funktionen, etwa das Zusammenfassen mehrerer VMs als eine Einheit. Hier kommt ein sogenannter *Lab Manager* ins Spiel. Er kann komplette Konfigurationen aus mehreren zusammengehörenden VMs zentral bereitstellen, datenbankgestützt verwalten und archivieren.

Beispielsweise holt ein Helpdesk-Mitarbeiter per Mausklick das gespeicherte Abbild einer Kundenumgebung samt Domänencontroller, Exchange-Server sowie Clients aus dem Archiv und startet die VMs in Sekunden auf einem freien Host. Genauso testen Entwickler neue Programmversionen in komplexen Szenarien, die vorher von der Qualitätssicherung zusammengestellt wurden. Die Verwaltung der virtuellen Umgebungen erfolgt über ein Webinterface mit Remote-Zugriff auf die Gastsysteme. Die VMs laufen auf Servern, ohne die Rechner der Anwender zu belasten. Dem Nutzer genügt zur Bedienung des Lab Manager ein Browser (Abbildung 8.1).

Abbildung 8.1:  
VMware Lab  
Manager verwaltet  
Konfigurationen  
virtueller Testumge-  
bungen aus mehr-  
eren VMs.



### Wichtige Komponenten des Lab Manager

VMware hat mit dem Kauf der Firma Akimbi das Produkt *Akimbi Slingshot* übernommen und zum *VMware Virtual Lab Manager* weiterentwickelt. Er besteht aus folgenden Komponenten:

- ▶ *Managed Hosts* – Auf allen ESX-Servern, die Test-VMs hosten sollen, werden Agenten des Lab Manager installiert. Sie übernehmen auf dem Wirt spezielle Aufgaben, z.B. das Erstellen und Steuern der VMs.
- ▶ *Lab Manager Verwaltungsserver* – Dieser Server stellt die eigentliche Steuerzentrale des Lab Manager dar. Er wird auf einer Windows-Maschine installiert und kommuniziert mit den Agenten der *Managed Hosts*. Er verwaltet den Speicher, die einzelnen VMs,

ganze Testumgebungen sowie Rechte und Ressourcen. Benutzer greifen über ein Web-Interface auf diesen Verwaltungsserver zu (Abbildung 8.1).

- ▶ *Shared Library* – Ein oder mehrere zentrale Speicherorte dienen als Bibliothek für ISO-Images und Muster-VMs (*Templates*) oder als Ablage für komplette Testumgebungen. Das können LAN-Freigaben, LUNs im SAN oder lokale SCSI-Platten sein (Abbildung 8.2). Der Lab Manager übernimmt die Verwaltung dieser Bibliotheken.
- ▶ *Tools für die Gastsysteme* – Zusätzlich zu den VMware Tools erweitern die *Lab-Manager Tools* in den VMs die Funktionalität, beispielsweise zur Anpassung von Namen, IP-Adressen oder SID der Gastsysteme bei Klonvorgängen.

## 8.1.2 Arbeiten mit dem Lab Manager

Die typischen Aufgaben in einer Testumgebung automatisiert der Lab Manager weitestgehend. Er stellt die zugrunde liegende physische Technik aus einzelnen Hosts und Datenträgern als eine Resource dar und entkoppelt sie von den Nutzern.

Im Web-Interface erstellen die Anwender zuerst saubere Vorlagen-VMs, die sogenannten *Templates*. Das sind Grundinstallationen der Betriebssysteme, teilweise bereits mit Applikationen wie Datenbanken oder Anwendungen (siehe auch *Teil 3, Kapitel 7 – Vorlagen und Templates erstellen*). Die Vorlagen können neu installiert oder von existierenden VMs importiert werden. Aus diesem Grundmaterial lassen sich dann sehr komfortabel komplette Testumgebungen zusammenstellen und im zentralen Pool, der *Library* des Lab Manager, ablegen. Damit entsteht beispielsweise eine Kombination aus virtuellem Datenbankserver und zwei Clients fast in Sekunden.

**Templates,  
Library und  
Workspace**

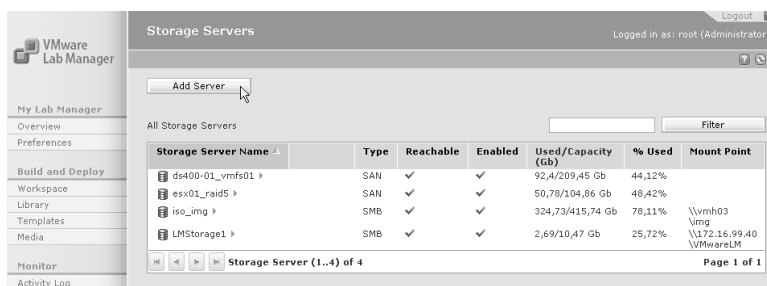


Abbildung 8.2: Hardware, wie physische Hosts oder Speicher, werden im Lab Manager als transparente Ressourcen eingebunden.

Solche gespeicherten virtuelle Umgebungen können von den Nutzern mit einem einfachen Mausklick in ihren persönlichen Arbeitsbereich, den sogenannten *Workspace*, kopiert werden. Das Original in der Datenbank bleibt dabei unberührt. Im Hintergrund sucht VMware Lab Manager nach verfügbaren Kapazitäten auf den physischen Hosts, kloniert die virtuellen Maschinen und startet die VMs. Der Benutzer hat nach kurzer Zeit im Web-Interface vollen Zugriff auf die

Bildschirme der laufenden VMs, ohne sich darum zu kümmern, auf welchem Host sie laufen und auf welchem Datenträger sie abgelegt sind. Er kann jede einzelne VM oder die gesamte Umgebung starten, beenden, Software installieren, Snapshots setzen oder zu alten Zuständen zurückkehren (Abbildung 8.1). Die Gruppen lassen sich auch um weitere VMs ergänzen.



Snapshots wirken im Lab Manager entweder auf einzelne VMs oder auf die gesamte Umgebung, so kann jederzeit ein konsistenter Zustand mehrerer VMs eingefroren werden. Das kann kein anderes der im Buch vorgestellten Produkte.

#### **Virtuelle Umgebungen archivieren und weitergeben**

Soll die neu entstandene Konfiguration für spätere Arbeiten oder für andere Kollegen weiterverwendet werden, kann der Anwender die gesamte Umgebung einfrieren und als neuen Eintrag in der Bibliothek speichern. Er kann selbst in seiner Version weiterarbeiten, während sich andere Mitarbeiter von dem gespeicherten Abbild sofort parallel lauffähige Kopien erstellen.

VMs werden vor dem Abspeichern im laufenden Betrieb in den Suspend-Modus versetzt und lassen sich später an genau dieser Stelle ohne Hochfahren sofort wieder auftauen. So friert die Qualitätssicherung festgestellte Fehler mitsamt der betroffenen Umgebung ein und leitet sie dem Entwickler zum Debuggen weiter. Mittels sogenannter *LiveLinks*, das sind Zeiger auf die Einträge in der Datenbank, kann der Anwender eine Verknüpfung zur abgespeicherten Umgebung sogar per Mail versenden.

### **8.1.3 Netzwerkisolation und weitere Besonderheiten**

#### **Networkfencing verhindert Konflikte**

Um bei parallel betriebenen Kopien der gleichen virtuellen Umgebung nicht die MAC- und IP-Adressen der Gäste anpassen zu müssen, was bei zusammenhängenden VMs teilweise gar nicht möglich wäre, bietet VMware Lab Manager das sogenannte *Networkfencing*. Diese Funktion beruht auf automatischer Adressumsetzung (*NAT – Network Address Translation*) und Routing (Grundlagen und erweiterte Workshops zu virtuellen Netzwerken finden Sie in *Teil 3, Kapitel 1 und Kapitel 2*). Die virtuellen Testumgebungen laufen entweder völlig isoliert oder sind mittels zugeordneter IP-Adressen aus dem LAN-Bereich von außen erreichbar. Dadurch können mehrere Kopien derselben Testumgebung intern die gleichen IP- und MAC-Adressen sowie Rechnernamen verwenden. Eine Anpassung der geklonten Gäste entfällt damit, was vor allem bei Client-Server-Konfigurationen sehr vorteilhaft ist. Sonst wären in manchen Fällen beispielsweise IP-Adressen in den Anwendungen umzukonfigurieren oder Lizenzen würden durch veränderte MAC-Adressen in den Klonen der virtuellen Testumgebungen nicht mehr funktionieren.

Weiterhin bietet der Lab Manager eine Rechteverwaltung, jeder Nutzer verfügt somit über seinen eigenen Arbeitsbereich und der Zugriff auf die zentral abgelegten Vorlagen kann gesteuert werden. Schließlich sind APIs für .NET und Java zur Automatisierung von Abläufen vorhanden.

Einziger Nachteil ist der relativ hohe Preis von einigen tausend Euro. Dafür verhindert der Lab Manager, vor allem in größeren Umgebungen, den virtuellen Wildwuchs dezentral verwalteter Test-VMs. Leider unterstützt VMware Lab Manager, im Gegensatz zum ehemaligen Akimbi Slingshot, nur noch den VMware ESX Server als Virtualisierungsplattform und nicht mehr die kostenlosen Serverprodukte, wie VMware Server oder Microsoft Virtual Server.

<http://www.vmware.com/products/labmanager/>

#### 8.1.4 Alternativen zum VMware Lab Manager

Zwei Alternativen zum VMware Lab Manager, welche auch die kostenlosen Serverprodukte VMware Server oder Microsoft Virtual Server verwalten, kommen von den Firmen Surgient bzw. VMlogix.

Surgient bietet spezialisierte Varianten seiner Produkte jeweils für Test-, Schulungs- und Demoumgebungen, das *Surgient Virtual QA/Test Lab Management System (VQMS)*.

<http://www.surgient.com/resourcecenter/>

Der *VMlogix Lab Manager* bietet als Besonderheit die Verwaltung physischer und virtueller Testmaschinen unter der gleichen Oberfläche. So können Testumgebungen gleichzeitig aus VMs und physischen PCs bestehen, die wegen bestimmter Hardware (Messplätze, Multimedia usw.) nicht virtualisiert werden können.

<http://www.vmlogix.com/labmanager/>

## 8.2 VMware Workstation 6 – Neuerungen und Unterschiede zur Version 5.5

Während der Entstehung dieses Aktualisierungskapitels befindet sich die neue Version *VMware Workstation 6* im öffentlichen Beta-Test und kann von jedem Interessierten gegen Registrierung heruntergeladen werden. Mit dem Erscheinen der finalen Version ist Mitte des Jahres 2007 zu rechnen.

<http://www.vmware.com/products/beta/ws/>





Alle in diesem Buch beschriebenen Funktionen und Workshops behalten auch mit VMware Workstation 6 ihre Gültigkeit. Der Sprung von der Version 5.5 zur Version 6 ist nicht so groß wie der Sprung von der Version 4 vor einigen Jahren, als VMware unter anderem seine multiplen Snapshots einführte.

### 8.2.1 Wichtige Neuerungen von VMware Workstation 6 im Detail

#### Kompatibel zur Workstation 5.5

Die Oberfläche von VMware Workstation 6 unterscheidet sich nur in Details von der Version 5.5 und ist voll kompatibel. An zentralen Themen, etwa der Netzwerkverwaltung oder dem Snapshot-Manager, ändert sich nichts (siehe Abbildung 8.3). Trotzdem sind einige sehr interessante Neuerungen hinzugekommen, die wichtigsten finden Sie hier.

#### Mehr als 4 GB RAM und Unterstützung von USB 2.0

VMware Workstation 6 verwendet für alle laufenden VMs jetzt den gesamten auf dem Host zur Verfügung stehenden Hauptspeicher, die Begrenzung auf 4 GB wurde aufgehoben. Damit sind umfangreichere Testumgebungen mit mehreren VMs möglich. Weiterhin können jeder VM bis zu 8 GB RAM (vorher 3,6 GB) zugewiesen werden.

Voraussetzung ist auf dem Host ein 64-Bit-Betriebssystem, das mehr als 4 GB Hauptspeicher adressieren kann. Auf 32-Bit-Systemen ist die PAE-Unterstützung eines entsprechend kompilierten Linux-Kernels bzw. der Windows Server 2003 Enterprise Edition notwendig (siehe auch Teil 1, Kapitel 1 – Grundlagen virtueller Maschinen und Hinweise zur Hardware).

#### USB 2.0 in den Gästen

USB 2.0-Geräte reicht Workstation 6 mit voller Geschwindigkeit in die Gäste durch, z.B. externe Festplatten, Speicherkarten an USB-Lesegeräten oder Kameras. Bisher wurde in den Gästen immer nur USB 1.1 emuliert.

#### Unterstützung mehrerer Monitore

VMware Workstation 6 kann jedem Gast mehrere Monitore zuweisen, unabhängig von der wirklich vorhandenen Hardware. Sie können bereits mit einem einzigen physischen Bildschirm Multi-Monitor-Konfigurationen testen oder entsprechende Applikationen entwickeln.

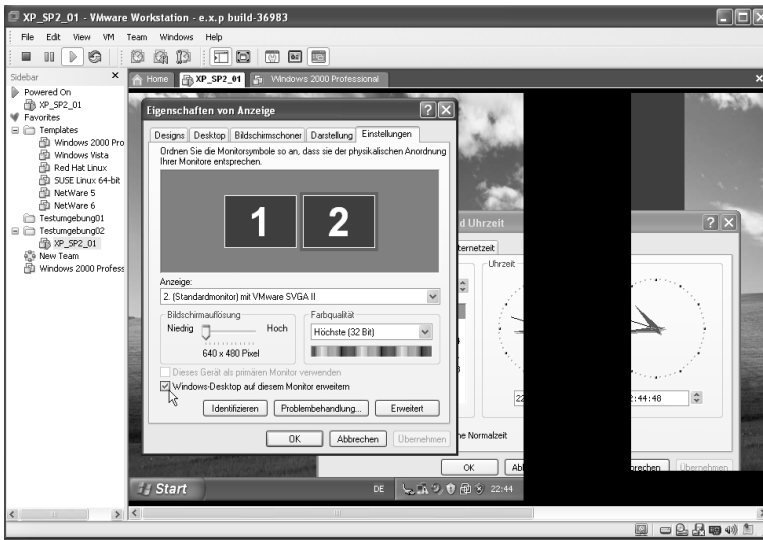


Abbildung 8.3:  
Eine Neuerung ist  
die Unterstützung  
mehrerer Monitore  
im Gast. Ansonsten  
ist die Oberfläche  
kompatibel zur  
Version 5.5.

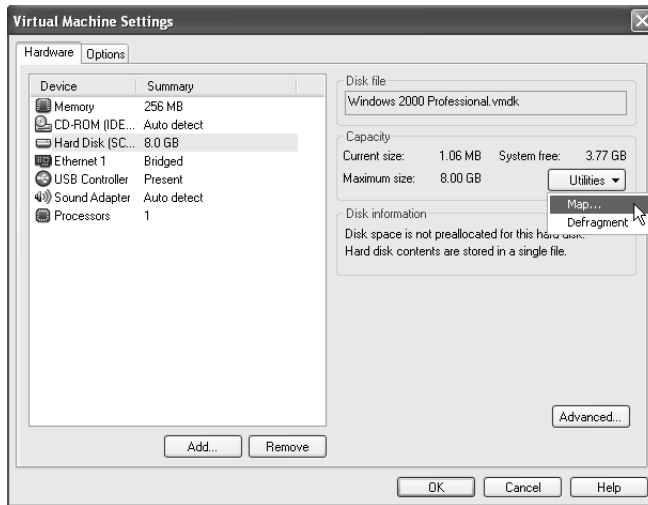
Jeder virtuelle Monitor erscheint im Gast wie ein physisches Gerät und kann auch unterschiedliche Auflösungen haben. Die Bildschirme der Monitore einer VM erscheinen im VMware-Fenster nebeneinander, gegebenenfalls ist Hin- und Herscrollen notwendig, um sie zu sehen (Abbildung 8.3). Genauso kann ein Gast aber auch mehrere physische Monitore nutzen, die am Host angeschlossen sind. Die Einstellungen finden sich unter VM/SETTINGS/HARDWARE/DISPLAY. Dort können Sie zusätzlich auch den virtuellen Videospeicher für den Gast einstellen.

### Mounten virtueller Festplatten über die Oberfläche

VMware kann bereits seit längerem virtuelle Festplatten auf einem Windows-Host direkt als Laufwerk einbinden und erlaubt so den direkten Zugriff auf die Partitionen in der virtuellen Platte, etwa um Reparaturen am Dateisystem auszuführen oder die *Boot.ini* anzupassen. Bisher erfolgte das mit dem Kommandozeilentool *VMware DiskMount* (siehe Teil 3, Kapitel 3 – Die virtuellen Platten als Herzstück der Gastsysteme).

VMware Workstation 6 bringt einen komfortablen Menüpunkt für diese Funktion mit. Unter FILE/MAP OR DISCONNECT VIRTUAL DISKS können Sie mehrere virtuelle Platten bestimmten Laufwerksbuchstaben auf dem Host zuweisen. Das funktioniert auch sehr praktisch mit einer neuen Schaltfläche in den Settings der VM (Abbildung 8.4). Die Funktion existiert nur auf einem Windows-Host und funktioniert deshalb nur mit Partitionen, mit denen Windows umgehen kann, also *NTFS* oder *FAT*. Die virtuelle Platte darf außerdem nicht von einer laufenden VM benutzt werden.

Abbildung 8.4:  
Das Mounten von  
virtuellen Platten  
funktioniert auch  
direkt über die  
Konfiguration  
der VM.



Auf eine Linux-Partition in der virtuellen Platte können Sie in gewissen Grenzen mit entsprechenden Zusatztools zugreifen, die Sie auf dem Windows-Host installieren, etwa das kostenlose *Ext2 Installable File System for Windows* oder das kommerzielle *Paragon Ext2FS Anywhere*:

<http://www.fs-driver.org>, <http://www.ext2fs-anywhere.com>

### VMs im Hintergrund betreiben

Im sogenannten *Headless-Mode* laufen VMs auch dann weiter, wenn die VMware Workstation-Oberfläche beendet wurde. VMware fragt beim Beenden nach, ob laufende VMs abgeschaltet werden oder im Hintergrund weiterlaufen sollen (Abbildung 8.5). Damit leistet beispielsweise ein virtueller Webserver auch ohne sichtbare GUI weiterhin seinen Dienst. Die laufenden VMs bleiben im Hintergrundmodus über das Netzwerk erreichbar. Sie erscheinen im Infobereich der Taskleiste unter einem grünen PowerOn-Pfeil (Abbildung 8.6) und lassen sich von dort wieder zusammen mit der Oberfläche aufrufen.

Abbildung 8.5:  
Beim Beenden der  
Oberfläche können  
VMs weiterlaufen.



Abbildung 8.6:  
Über ein Symbol in  
der Taskleiste sind die  
VMs zu erreichen.



Eine VM unter Workstation 6 läuft nur dann im Hintergrund, wenn ein Nutzer am PC angemeldet ist. Sobald sich der Nutzer abmeldet, wird auch die VM beendet. Nur mit der Funktion BENUTZER WECHSELN von Windows XP laufen auf dem Host die Applikationen des Nutzers im Hintergrund weiter und somit auch die VMs.

Damit unterscheidet sich der *Headless-Mode* von der Funktion des VMware Server, Gäste als Dienst laufen zu lassen. Dort startet eine VM auf Wunsch völlig unabhängig von einer Nutzeranmeldung am Host (siehe auch *Teil 1, Kapitel 4 – Bedienung der Produkte, wichtige Funktionen und Tipps*).



## Integrierte VNC Remote-Steuerung der Gäste

Jeder Gast kann unter Workstation 6 über einen integrierten VNC-Server ferngesteuert werden. Der Vorteil ist, dass dadurch für eine Fernsteuerung keine Installation von Remote-Tools in den Gästen notwendig ist. Der integrierte VNC-Server erlaubt, ähnlich einem KVM-Switch, die Sicht auf das Geschehen in der VM auch beim Bootvorgang des Gasts, im CMOS-Setup oder bei BlueScreens.

Jede VM benötigt einen eigenen Port für die Fernsteuerung, dieser lässt sich unter VM/SETTINGS/OPTIONS/REMOTE DISPLAY einstellen (Abbildung 8.7). Weiterhin lässt sich ein Passwort für den Zugriff festlegen. Unter VM/CONNECTED USERS bzw. über ein Symbol in der Statusleiste der VM sind die mit der VM verbundenen Remote-Nutzer sichtbar.

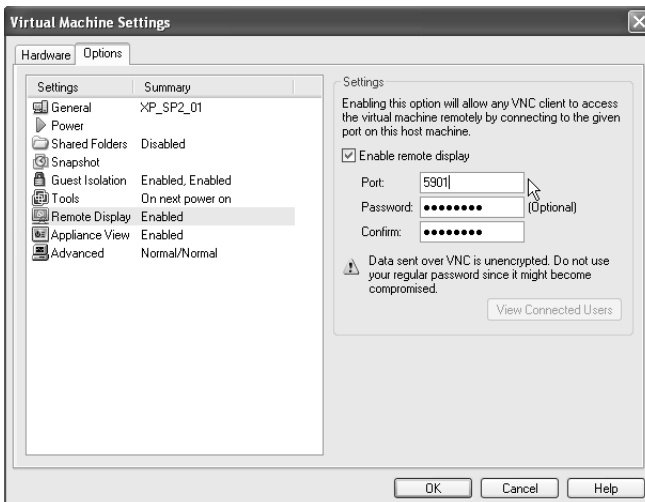


Abbildung 8.7:  
Jede VM muss mit  
einem eigenen VNC  
Port konfiguriert  
werden.

Trotzdem ist der Unterschied zur *Remote Console* von VMware Server zu beachten. Die VNC-Steuerung der Workstation 6 erlaubt nur eine Kontrolle des Geschehens im Gast, aber keinerlei Steuerung der VM, wie POWERON/OFF, SUSPEND, SNAPSHOTS o.Ä. Außerdem erfolgt der Datenverkehr unverschlüsselt, VMware Server bietet dagegen SSL.

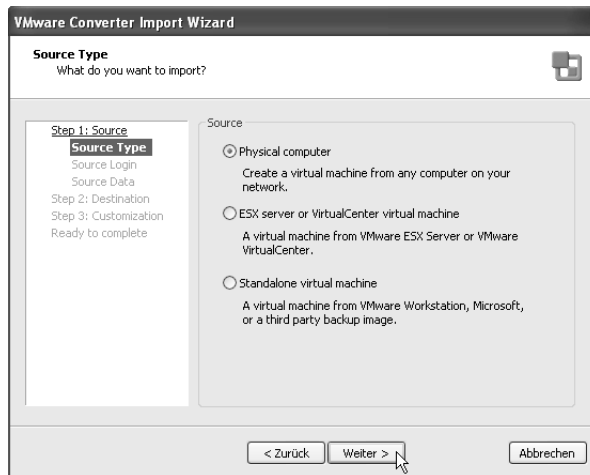


Bei Verwendung des *RealVNC Viewer* als Fernsteuerungs-Client müssen Sie dort unter OPTIONS/COLOR&ENCODING/PREFERRED ENCODING die Einstellung *Hextile* wählen und unter COLOUR LEVEL die Einstellung *Full*. Ansonsten wird die Verbindung zum Gast mit der Fehlermeldung *Connection reset by peer (10054)* zurückgewiesen. Weiterhin funktioniert in der derzeitigen Beta-Version kein deutsches Tastaturlayout in der ferngesteuerten VM.

### Integrierter VMware Converter für Import von VMs oder PCs

Der bereits in der Workstation 5.5 vorhandene Wizard zum Importieren von Gästen unter FILE/IMPORT wurde stark erweitert. VMware hat Teile der Funktionalität des separaten Produkts *VMware Converter* integriert (Abbildung 8.8). Damit ist es jetzt möglich, Gäste anderer VMware-Produkte, etwa vom ESX Server, VMs der Microsoft-Virtualisierer, Image-Dateien von Symantec bzw. Ghost und sogar physische Maschinen direkt in eine VM zu importieren.

Abbildung 8.8:  
Der neue Import-  
Wizard enthält  
Funktionen des  
VMware Converter.



### Automatisches Update der VMware Tools im Gast

Im Menü VM/SETTINGS/OPTIONS/TOOLS findet sich eine Einstellung, wie sich der Gast bei einer neu vorhandenen Version der VMware Tools verhalten soll. Mit UPGRADE THEM AT NEXT POWER werden beim Neustart der VM automatisch die aktuellen VMware Tools im Gast installiert. Damit entfällt beispielsweise das manuelle Update bei Gästen, die von älteren Vorlagen-VMs (*Templates*) geklont wurden.

Das standardmäßige Verhalten für alle VMs, bei denen der Punkt USE GLOBAL PREFERENCE gewählt ist, können Sie unter EDIT/PREFERENCES/WORKSPACE/TOOLS einstellen.



## Neues Interface für Virtual Appliances

Virtual Appliances sind vorkonfigurierte, sofort lauffähige VMs, die bestimmte Funktionen oder Dienste bereitstellen (siehe auch *Teil 1, Kapitel 2 – Das richtige Virtualisierungsprodukt für Sie*), beispielsweise eine vorkonfigurierte Firewall oder ein Webserver als Gast. Eine wesentliche Vereinfachung in der Handhabung solcher Appliances für den Endanwender ist der neue sogenannte *Appliance View*.

Im Gegensatz zum üblichen *Console View*, bei dem der Bildschirminhalt des Gastsystems im VMware-Fenster sichtbar ist, zeigt der *Appliance View* nur eine kurze Beschreibung des Gasts an und einen Link zum laufenden Gastsystem. Mit einem Klick auf diesen Link öffnet sich der Browser des Wirts und stellt eine Verbindung mit einem im Link festgelegten Port im Gastsystem her. Der Entwickler der Appliance kann im Gast auf diesem Port einen Webdienst laufen lassen, mit dem die Appliance zu bedienen oder zu konfigurieren ist. Dadurch muss sich der Anwender nicht um das System in der VM kümmern, sondern er kann sofort mit dem Web-Interface die Appliance steuern.

Unter VM/SETTINGS/OPTIONS/APPLIANCE VIEW wird der Port und die Beschreibung samt Logo festgelegt (Abbildung 8.9). Über eine neue Schaltfläche in der Werkzeugleiste von VMware Workstation 6 können Sie zwischen *Appliance View* und *Console View* umschalten.

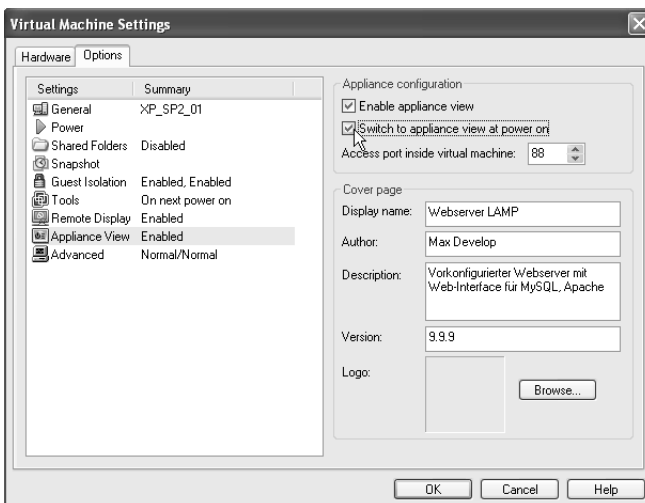


Abbildung 8.9:  
Für den Appliance View lassen sich der Port eines Dienstes im Gast und eine Beschreibung definieren.



Besonders interessant ist der Appliance View mit dem neuen *VMware Player 2.0*, um damit besonders einfach zu bedienende VMs zu verteilen. Daneben wird es im neuen Player sogar möglich sein, eigene Menüeinträge oder Schaltflächen in der Oberfläche zu integrieren. Dazu dient das sogenannte *Player Extensions Framework*, was sich derzeit noch in der Entwicklung befindet.

### Erweiterte Betriebssystemunterstützung, z.B. Windows Vista

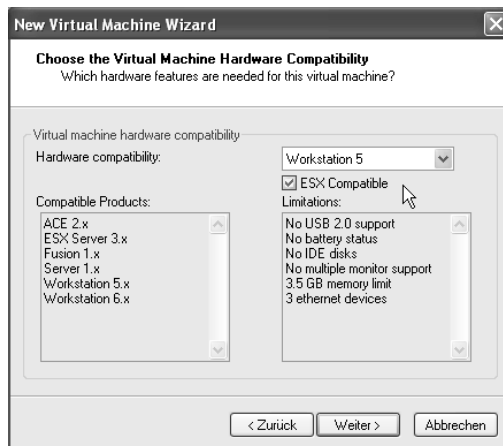
VMware Workstation 6 kann unter Windows Vista installiert werden, ebenso läuft Windows Vista als Gast. Als Gast wird allerdings nicht die Oberfläche *Aero Glass* unterstützt (Bemerkungen zu Windows Vista als Gast siehe 8.5 Windows Vista als Host und in VMs).

Einige neue 32-Bit- und 64-Bit-Versionen verschiedener Betriebssysteme werden ebenfalls unterstützt, z.B. Solaris 10. Eine detaillierte Auflistung finden Sie in den jeweils aktuellen Releasenotes auf der VMware-Webseite.

### Umschalten der Hardwareversion der VMs

Eine weitere sehr nützliche Funktion verbirgt sich unter VM/CHANGE VIRTUAL MACHINE VERSION. Der *Convert Hardware Version Wizard* ermöglicht einen Wechsel der Hardwareversion des Gasts. Damit kann beispielsweise eine unter VMware Workstation 5 erstellte VM in eine kompatible Version zur Workstation 4 oder zum GSX Server zurückkonvertiert werden. Dazu waren bisher manuelle, nicht unterstützte Tricks in der Konfigurationsdatei (\*.vmx) der VM notwendig. Der neue Wizard kann die VM direkt umwandeln oder eine Kopie erstellen.

Abbildung 8.10:  
Mit Workstation 6  
lassen sich zu allen  
anderen Versionen  
kompatible VMs  
erstellen.



Im Wizard für eine neu erstellte VM (FILE/NEW/VIRTUAL MACHINE) können Sie im Modus *Custom* ebenfalls die gewünschte Hardwareversion und damit die Kompatibilität zu den anderen VMware-Produkten wählen (Abbildung 8.10).

Die Standardversion der verwendeten Hardware für neu erstellte VMs legen Sie unter EDIT/PREFERENCES/WORKSPACE/DEFAULT HARDWARE COMPATIBILITY fest.



## 8.2.2 Weitere Neuerungen und zukünftige Entwicklungen der Workstation 6

Neben den genannten Neuerungen gibt es einige weitere Verbesserungen, die ich hier kurz aufliste:

- ▶ In den Favoriten existiert eine neue Sektion POWERED ON, unter der Sie sofort erkennen, welche VMs gerade laufen (siehe auch Abbildung 8.3).
- ▶ Unter VM/MESSAGE LOG bzw. über ein kleines Icon in der Statusleiste des VMware-Fensters erscheinen aktuelle Log-Meldungen der laufenden VM, etwa Meldungen über den Netzwerkstatus oder über aufgetretene Fehler.
- ▶ *Drag&Drop* sowie *Cut&Paste* von Texten, Dateien oder kompletten Verzeichnissen ist jetzt zwischen Gästen bzw. Hosts mit Linux-, Windows- oder Solaris-Gästen möglich. Bisher funktionierte *Drag&Drop* nur zwischen gleichen Betriebssystemfamilien.
- ▶ Der Batterieladezustand eines Laptops wird in einem Gast im Vollbildmodus angezeigt, einzustellen über VM/SETTINGS/OPTIONS/GENERAL/BATTERY INFORMATION.
- ▶ Verbesserte Unterstützung von 64-Bit-Gästen, unter anderem ein neuer 64-Bit-Sound-Treiber und Unterstützung von 64-Bit-Hardwarevirtualisierung (*Intel EM64T VT*)
- ▶ VMware Workstation 6 unterstützt paravirtualisierte Linux-Kernels mit *VMware VMI (Virtual Machine Interface) 3.0*. Bei Paravirtualisierung stellt der Virtualisierer bestimmte Schnittstellen bereit, die vom Gastsystem angesprochen werden können, z.B. für Platten- oder Netzwerkzugriffe. Dadurch entfällt die aufwändige Emulation dieser Hardwarekomponenten, wodurch die Geschwindigkeit steigt. Die Option lässt sich unter VM/SETTINGS/OPTIONS ADVANCED einschalten. Allerdings ist ein entsprechend modifiziertes Gastsystem notwendig, was bei Windows-Gästen nicht möglich ist.



- Die Programmierschnittstelle *VIX API*, die bisher vom VMware Server unterstützt wurde, ist nun auch unter Workstation 6 verfügbar. Aus Skripten heraus können einige Funktionen dieser Schnittstelle bereits über das Programm *vmrun.exe* erreicht werden, welches schon bei der Workstation 5 und auch beim VMware Server vorhanden ist (siehe Teil 3, Kapitel 7 – Scripting zur Fernsteuerung von VMware oder zur Automatisierung).
- Für Entwickler ist die Integration von VMware in die Entwicklungsumgebung von *Visual Studio* oder *Eclipse* interessant, um in VMs Programme zu entwickeln oder zu debuggen.

**Erweiterung  
der Snapshot-  
Funktion**

Auf der VMworld Konferenz 2006 in Las Vegas wurde zusätzlich eine entscheidende Erweiterung der Snapshot-Funktionalität angekündigt. Es soll möglich werden, nicht nur statische Snapshots vom momentanen Zustand der VM aufzuzeichnen (siehe Teil 3, Kapitel 4 – Ein praktischer Workshop zum Umgang mit multiplen Snapshots), sondern den gesamten Ablauf im Gastsystem mitzuschneiden, inklusive der Möglichkeit des späteren Abspielens mit Vor- und Rücklauf sowie Weiterausführens des Gastsystems. Wohlgermerkt nicht als Video des Bildschirms, sondern als Aufzeichnung der internen Aktivitäten des Gastsystems! Damit kann ein Entwickler beispielsweise immer wieder bis zur Stelle eines Absturzes spulen und ab dort den Ablauf analysieren. Zum aktuellen Stand der Beta fehlt diese Funktion leider noch, sie soll aber bis zur endgültigen Version nachgerüstet werden.

Die Version 6 von VMware Workstation etabliert das Produkt weiterhin als Profiwerkzeug der Wahl für umfangreiche und anspruchsvolle Test- und Entwicklungsumgebungen auf dem Laptop, dem PC oder teilweise sogar auf einem zentralen Host für kleinere Entwicklergruppen.



Diese Vorstellung der VMware Workstation 6 soll Ihnen einen möglichst frühzeitigen Überblick zu den neuen Funktionen liefern. Denken Sie aber daran, dass es sich um eine Beta-Version handelt, die sich bis zur fertigen Version noch ändern kann. Weiterhin sind Fehler und Leistungseinschränkungen möglich. Ich empfehle Ihnen vor den ersten Versuchen einen Blick auf die Releasenotes der gerade aktuellen Version.

## 8.3 VMware Fusion für Apple Macintosh auf Intel-PC bringt VMs auf den Mac

Zusätzlich zur Workstation 6 für Windows und Linux hat VMware seine Workstation auf Apple Macintosh portiert. Allerdings läuft das Produkt unter dem Namen *VMware Fusion* nur auf Apple-Computern mit Intel-Architektur und nicht auf PowerPC. Das einzige kommerzielle Virtualisierungsprodukt, das auf PowerPC läuft, bleibt also Microsoft Virtual PC für Macintosh.

Im Gegensatz zur langsamen Emulation von Microsoft Virtual PC für Macintosh, bei der auf dem PowerPC ein kompletter Intel-Rechner samt CPU nachgebildet werden muss, läuft VMware Fusion wesentlich schneller, da es Virtualisierung und keine Emulation betreibt. Dabei laufen die meisten Befehle der Gastsysteme direkt auf der vorhandenen Intel-CPU und müssen nicht erst nachgebildet werden.

Der Unterschied von Emulation und Virtualisierung und die grundlegenden Techniken dazu werden in *Teil 1, Kapitel 1* des Buchs erklärt.



VMware Fusion wurde auf eine möglichst einfache Bedienbarkeit optimiert, die Oberfläche unterscheidet sich von VMware Workstation für Windows oder Linux. Die Software befindet sich zum Zeitpunkt dieser Aktualisierung im öffentlichen Beta-Stadium:

<http://www.vmware.com/vmtn/beta/>

### 8.3.1 Die Alternative Parallels Desktop for Mac

Ein anderes Produkt, das auf einem Apple Macintosh Windows- oder Linux-Gäste sehr flott laufen lässt und bereits einige Zeit vor VMware als fertige Version auf dem Markt war, ist *Parallels Desktop for Mac*:

<http://www.parallels.com/>

## 8.4 Microsoft Virtual PC 2007 – Neuerungen und Unterschiede

Microsoft stellt Virtual PC 2007 als Release Candidate vor, die endgültige Version wird im ersten bis zweiten Quartal 2007 erwartet und laut Microsoft kostenlos bleiben. Die Neuerungen sind allerdings schnell aufgezählt, an der Oberfläche hat sich nichts Entscheidendes getan (Abbildung 8.11). Die Beta-Software steht zum öffentlichen Download bereit, erfordert aber ein Passport- oder LiveID-Konto:

<https://connect.microsoft.com/>



Alle in diesem Buch beschriebenen Funktionen und Workshops behalten auch mit Microsoft Virtual PC 2007 ihre Gültigkeit, es gibt kaum sichtbare Änderungen.

Abbildung 8.11:  
Bis auf Kleinigkeiten  
hat sich an der  
Oberfläche von  
Virtual PC 2007  
im Vergleich zur  
Version 2004 kaum  
etwas geändert.



#### Keine Vista Home Edition

Virtual PC 2007 unterstützt Windows Vista als Wirtssystem, also auf dem physischen PC, und auch als Gast in einer virtuellen Maschine. In einer VM funktioniert allerdings nicht die Vista-Oberfläche Aero Glass, sondern nur die Basic-Variante, was an der emulierten S3 Trio-Grafikkarte liegt (siehe 8.5 Windows Vista als Host und in VMs). Die schlechte Nachricht für Privatanutzer dürfte sein, dass Microsoft keine Installation von Virtual PC 2007 auf den Home-Editionen von Windows Vista sowie Windows XP unterstützt und dass Vista Home noch nicht einmal als Gastssystem läuft.

Virtual PC 2007 verwendet wie VMware zur Virtualisierung der Gast-systeme auch Intels Vanderpool (VT) und AMDs Pacifia, sollte der physische Prozessor diese Funktionen bieten. Mit dieser Hardware-unterstützung ist weniger softwareseitiger Emulationsaufwand, etwa für bestimmte CPU-Befehle (privilegierte Operationen), notwendig. Allerdings läuft bereits mit der herkömmlichen Virtualisierung ein Großteil der Maschinenbefehle direkt auf der CPU, weshalb der oft beworbene Leistungszuwachs in den Gästen in der Praxis eher gering ausfällt. Hinzu kommt noch, dass andere wichtige Komponenten, etwa Festplatten oder Grafikoperationen, durch diese Virtualisierungsunterstützung nicht beschleunigt werden.

Virtual PC 2007 kann jetzt auch auf 64-Bit-Systemen installiert werden. In den virtuellen Maschinen laufen allerdings immer noch ausschließlich 32-Bit-Betriebssysteme. Genauso wurde keine Unterstützung von mehreren Prozessoren implementiert. Dafür funktionieren jetzt endlich ISO-Images größer 2,2 Gbyte als virtuelle CDs und die Zusammenarbeit mit Energiesparfunktionen auf Laptops wurde verbessert.

**64 Bit nur auf dem Host, kein SMP**

Die Oberfläche von Virtual PC 2007 ähnelt fast völlig der des Vorgängers Virtual PC 2004. Hinzugekommen sind z.B. der Haken zum Einschalten der Hardwarevirtualisierung (Abbildung 8.11) und einige Details beim Wizard zum Erstellen neuer VMs. Dort kann der Anwender beispielsweise die Größe für eine neu erstellte virtuelle Platte festlegen, ohne diese vor dem Erstellen der VM erst mit dem separaten Festplattenwizard anlegen zu müssen (Abbildung 8.12).

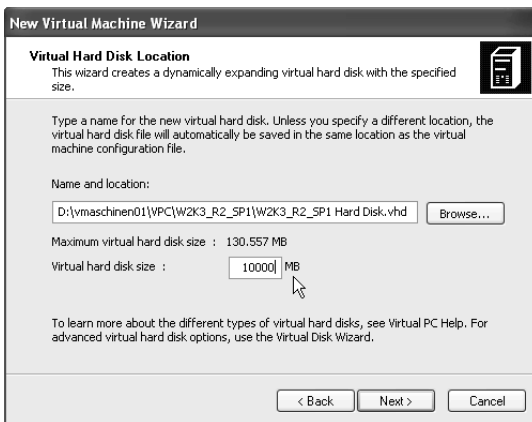


Abbildung 8.12:  
Bei der Erstellung neuer VMs können einige Parameter besser beeinflusst werden als bei Virtual PC 2004.

Virtual PC 2007 verzichtet immer noch auf eine emulierte USB-Schnittstelle in den VMs. Außer USB-Maus und Tastatur kann ein Gastsystem auf kein angeschlossenes USB-Gerät zugreifen.

**Kein USB**

Auch die Undo-Funktionen für die Gäste hat der Hersteller nicht überarbeitet, es existieren zwar weiterhin die Rückgängigdatenträger zum Verwerfen der letzten Änderungen und die Differenzplatten. Eine komfortable Snapshot-Funktion oder eine menügestützte Funktion zum Clonen von VMs hat Microsoft dem neuen Produkt aber nicht spendiert.

Linux läuft zwar inoffiziell unter Virtual PC 2007, es fehlen aber immer noch die *Virtual Machine Additions* für flüssige Mausbewegungen, höhere Grafikauflösungen und einfachen Datenaustausch zwischen VM und Host. OS/2 wird weiterhin unterstützt, das bleibt ein Alleinstellungsmerkmal der Microsoft-Lösung gegenüber VMware.

**Linux nicht offiziell**

## 8.5 Windows Vista als Host und in VMs

### Kein Aero Glass in VMs

Seit Windows Vista kommt erstmals die unzureichende Graphikkartenemulation aller Virtualisierer zum Tragen. Zwar läuft das aktuelle Windows-Betriebssystem als Gast in einer VM, allerdings nur mit der Basis-Oberfläche ohne viele der 3D- und Transparenzeffekte, die Aero zu bieten hat. Gerade für Tests von Applikationen oder um sich einen vollständigen Eindruck von Windows Vista zu machen, kann das ein Handicap sein. Das Problem ist weder in den aktuellen VMware-Versionen noch in anderen Virtualisierern gelöst.

### 8.5.1 Aero Glass auch in virtuellen Maschinen über den Umweg RDP

Es gibt allerdings einen Trick, die Vorteile der Isolation eines Testsystems in einer VM zu nutzen und gleichzeitig mit Aero Glass zu arbeiten. In der Version 6 seines RDP-Protokolls bietet Microsoft die Möglichkeit, auch Grafikeffekte zu übertragen. Mit einer *Remote Desktop-Verbindung* (RDP) zum Gastsystem arbeiten Sie mit Aero Glass im Gast. Voraussetzung dafür ist, dass auf dem RDP-Client (der fernsteuernde PC) auch Aero Glass läuft. Es muss also ein genügend leistungsfähiger Rechner mit Windows Vista sein. Als Client bietet sich der Host selbst an, wenn Vista auf ihm läuft, oder jeder beliebige Vista-PC im LAN.

### 8.5.2 Lizenzierung von Windows Vista Enterprise in VMs

### Vier VMs und der Host mit nur einer Lizenz

Die gute Nachricht betrifft professionelle Anwender. Mit einer einzigen Lizenz der Windows Vista Enterprise Edition erlaubt es Microsoft, auf dem gleichen Host bis zu vier virtuelle Gäste mit Vista zu betreiben, zusätzlich zum Wirtssystem. Für den Windows Server 2003 R2 Enterprise Edition hat Microsoft diese vereinfachten Lizenzbedingungen für virtuelle Maschinen bereits vor längerer Zeit eingeführt, sie gelten unabhängig vom Virtualisierungsprodukt (siehe *Teil 1, Kapitel 3 – Vereinfachte Lizenzierung von Microsoft Windows Server 2003 R2 Enterprise Edition*).

## 8.6 VMware Converter 3.0 – physische Maschinen und VMs konvertieren

Die Funktionen des bekannten *VMware P2V Assistant* und die des relativ neuen *VMware Virtual Machine Importer* (siehe auch Teil 3, Kapitel 6 – P2V) werden in einem neuen Konvertierungstool gebündelt, dem *VMware Converter*. Damit bietet VMware ein sehr mächtiges Tool für Konvertierungen physischer Maschinen in VMs oder zwischen den unterschiedlichen Versionen der Virtualisierer an. Einige besondere Merkmale von VMware Converter sind:

- ▶ P2V von laufenden physischen Windows-Systemen ohne Herunterfahren der Quelle
- ▶ Konvertierung verschiedener Formate, etwa Microsoft Virtual Server/PC, Symantec bzw. Norton Ghost Images und alle Formate der VMware-Produktpalette untereinander
- ▶ Eine einheitliche Konsole für alle Vorgänge erlaubt beispielsweise ferngesteuertes Klonen, ohne direkt an der Quellmaschine Hand anzulegen.
- ▶ Es wird, im Gegensatz zum P2V-Assistenten, keine Hilfs-VM mehr benötigt, um das Quellsystem in eine VM zu übertragen.

**Übernehmen  
laufender  
Systeme**

<http://www.vmware.com/products/beta/converter/>



# Stichwortverzeichnis

## Symbols

/etc/network/interfaces 510  
/etc/vmware/vmnetX/dhcpd 483  
/etc/vmware/vmnetX/nat 483

## Numerics

0xc000000f 634  
1  
    1 Clone 626  
10 GBit Ethernet 52  
4GBit/s Fibre-Channel 52  
64-Bit-Betriebssystem 48  
64-Bit-Hardware 48  
64-Bit-Hosts, nativ 252

## A

A disk read error occurred 628  
Abgesicherter Modus 630  
Absolute Pfade linked Clones 288  
Accelerated SCSI Controller 544  
ACPI Uniprocessor PC 631  
Acronis 621  
Acronis Universal Restore 641  
Active Directory 352  
ActiveX-Plugin 136  
Adaptec 539  
adduser 265  
Aero Basic 680  
Aero Glass 680  
AES (Advanced Encryption Standard) 427  
aexia Virtual Solution Box (VSB) 601  
Agenten, Sicherung 588  
Akimbi Slingshot 664  
Aktive Partition 627  
Alarms 435  
Allocate all Disk Space now 166  
AMD-PCNet 440  
Änderungen  
    festschreiben 559  
    verwerfen 559  
    zusammenführen Virtual PC 203  
Angreifer 245  
Anhalten Virtual PC 197  
Anmeldebildschirm STRG+ALT+ENTF 171  
Anmeldekonto VMware Server 243  
Anschluss  
    Typ umschalten Netzwerk VMware 178  
Any-Any-Patch 94, 253  
AnywhereUSB 60  
Apache 187  
apache 262

Apple 38  
Apple Macintosh 677  
Appliance View 673  
apt-get 94, 258  
apt-get install 260  
Aptitude 257  
Archivieren  
    von Testsystemen 602  
    von VMs 648  
Assistent  
    für neue virtuelle Computer 188  
    zum Installieren von Active Directory 353  
Auflösung 116  
Auslagerungsdatei 47, 539  
Auslastung 82  
Ausnullen unbenutzter Sektoren 548  
Ausschalten  
    einer VM Virtual PC 200  
    Virtual PC 197  
AutoIT 656  
Automatisch starten, Microsoft 149  
Automatisches Neustarten verhindern 619  
Automatisierung 653  
    von Arbeitsabläufen 657  
automount disable 390  
Autonegotiation 504  
AVM KEN! 60

## B

Backup-Proxy 379, 389  
Bare Metal 36  
BartPE 623, 653  
base-config 258  
Behälterdatei 39  
Benutzer anlegen ESX 425  
Benutzermodus 42  
Bereinigen von Testsystemen 561  
Besitzer  
    Konfigurationsdatei, Linux 264  
Betriebssystem im Gast installieren 169  
    Überblick VMware 179  
Bildschirmauflösung, Player 284  
Bildschirmgröße 116  
Binärmodule 93, 274  
Blade-Center 82  
Blade-Server 82, 394  
Blaster 239  
Blinkender Cursor 628  
Blockorientierter Zugriff 56, 384  
Blogs 659  
blowfish 427



- BlueScreen 540, 619
  - P2V 626
- Bochs 38
- boot from SAN 394
- Boot.ini 626
  - anpassen 629
  - PAE 48
- Boot-Diskette 627
- Bootloader (Ntldr) 628
- Bootmanager 537
- Bridge Protocol 474
- Bridged 178, 445
- Bridged to an automatically chosen adapter 472
- Bridge-Protokoll 463
- Browser Appliance 281
- Browserversionen 186
- Buffer Overflows 245
- build-essential 94, 260
- BusLogic 539
- C**
- CD 49
  - Mounten, Linux 650
- CHAP Authentication 411
- chmod 265
- CHS-Geometrie 515
  - in Kopffdatei 551
  - P2V 628
- CIFS (Common Internet File System) 55, 383
- Citrix Metaframe 78
- Citrix Secure Gateway 244
- Class-B-Netzwerk 459
- Class-C-Netzwerk 459
- cleanmgr 648
- Client-Rollout 155, 174
  - mit Master VM 174
- Clonen
  - mit Differenzplatten 326
  - von Gästen 180
- Cluster 604
  - across boxes 344, 383
  - ESX 386
  - Failover testen 369
  - für Hochverfügbarkeit 337
  - für Lastverteilung (Load Balancing) 337
  - gemeinsame SCSI-Festplatte 372
  - Knoten 338
  - mit virtuellen Maschinen 335
  - Ressource 338
- Cluster-Dienste, installieren 365
- Cluster-Konstellationen, Typen 343
- Cluster-Ressource, konfigurieren 367
- Cluster-Skript havm.vbs 375
- Cluster-Verwaltung 365
- coalescing 502
- Cold Backup 590
- Collisions 505
- Commit ESX Server 391
- Commit Player 310
- compat-32 273
- Compiler 93, 274
- confclus.doc 346
- Console View 673
- ControlFlags 543
- Controllermodell 531
- Convert Hardware Version Wizard 674
- Copy&Paste VMware 119
- COS (Console Operating System) 380
- CPU in einer VM 42
- CPU-Kernel 82
- CPU-Leistung 83
- CPU-Shares 393
- CPU-Verwaltung, Virtual Server 148
- cramfs patch 270
- Crashkonsistente Sicherung 591
  - mit Snapshot 597
- Crashkonsistentes Backup 595
- Crossover-Kabel 234
- Custom 446, 466
  - Modus Player 292
  - Netz Player 292
- Custom-Konfiguration, VMware 159
- Custom-Netzwerke, Linux 483
- Cut&Paste 176
  - Virtual Server 146
- D**
- Daemon Tools 650
- DAS (Direct Attached Storage) 51
- Datacenter 72, 386, 434
- Datastore VMFS 413
- Dateifreigaben im LAN 54
- Dateiorientierter Zugriff 56
  - ESX 384
- Dateiserver 54
- Dateisperre 529
- Dateizugriffe überwachen 651
- Datenbankserver, virtuell 185
- Datenbankupdates 617
- Datensicherung
  - ESX 390
  - Wiederherstellung 587
- Datenträger im Wirt 83
- Datenträgerbereinigung 648
- dcpromo 353, 647
- ddb.geometry 552
- DDChanger 641
- Debian 3.1 94
  - als Host 251
- Default-Gateway 460
- Defragmentierung 538
- Demo-Umgebung
  - mit dem Player 297
  - virtuell 185

Desaster Recovery 587, 600  
Desktop-Produkte 63  
DevCon, Gerätemanager 656  
devmgr\_show\_nonpresent\_devices 512  
DHCP 457  
    im LAN 453  
    in den Gästen 453  
    Virtual Server 490  
    VMware 475  
DHCP-Dienst 461  
Dienste  
    VMware Server, Linux 262  
Dienstekonto  
    für die VM VMware 162  
    VM virtual Server 149  
Differenz-Backup 617  
Differenzierende Festplatte erstellen 328  
Differenzierende Platten, Virtual PC 202  
Differenzplatten 524  
DirectUpdate 242  
Direktes Kopieren virtueller Platten ESX 419  
Disable Autorun 91  
disk.locking 373, 529  
diskpart 390  
Distribution, unterstützte 85  
DMZ (demilitarisierte Zone) 211  
DNS-Proxy 479  
DNS-Server 229, 239, 461  
Domänencontroller 346, 634  
    Snapshots 578  
    virtuell 596  
Dongles 60, 614  
Downloads 659  
dpkg 271  
Drag&Drop 176  
    Virtual PC 206  
    VMware 119  
Drive SnapShot 621  
DriveImage 621  
Dropped Packets 54  
DSL-Flatrate 211  
DSL-Modem 219, 228, 451  
Dual-Boot 536  
    ESX 403  
Dual-Core 44, 82  
Dual-CPU 44, 82  
Dualprozessor  
    im Player 289  
    P2V 631  
Dunes VS-O (Virtual Service Orchestrator) 657  
Duplex-Einstellung 504  
DVD 2,2 GB, Microsoft 650  
Dynamic Discovery 411  
Dynamisch erweiterbare virtuelle Festplatte 517  
Dynamisch erweiterbare virtuelle Platte 191  
DynDNS 242

## E

e1000 467  
Echtzeitüberwachung 539  
Emulation 38  
Emulatoren 38  
Emulierte Netzwerkkarten 439  
Entwicklungsumgebung 281  
Ereignisprotokollierung beim Herunterfahren 647  
Erstellen einer VM  
    im Überblick, VMware 167  
    Virtual PC 189  
ESX Ranger 389  
ESX Server 2.x 76  
ESX Server 3 377  
    lizenzieren 405  
ESX Server installieren 396  
esxBasics 601  
esxcfg-nics 430  
esxcfg-vswif 430  
esxcfg-vswitch 430  
esxCharter 658  
esxMigrator 658  
esXpress 601  
esxRanger 601  
esxReplicator 601  
eth1 483  
Evaluierung ESX 400  
Evaluierungsphase 88  
    VMware Workstation 280  
Exception 43  
Exchange Server, Backup 591  
Exchange-Datenbanken 83  
ExcludeFromSelect 543  
export CC=gcc 94  
Export-Vorgang 417  
Ext3 84  
Externer Speicher 51  
Externer Speicherplatz 84  
Externes Netzwerk 448, 485

## F

Failover 604  
Failover Cluster 339  
    testen 369  
fakeroot 270  
FalconStor Application Snapshot 392, 592  
FAT 536  
Favorites 110  
FAX-G3-Option 614  
FDISK 627  
fdisk /mbr 628  
fdisk, Linux 266  
Fehlermeldungen, P2V 627  
Fernsteuerung von VMs 653  
Festplattencontroller, P2V 619  
Festplattelektronik 40

- Fibre-Channel 51
  - Cluster 341
- Fibu Server archivieren 602
- Fileservers 56
- Fileserver-Bereiche 83
- Firefox 136
- Firewall 211
- Firewall-Ports 99
- Firewall-VM 214
- FireWire 60, 614
- Firmen-LAN 240
- Fit Window, Fit Guest 116
- fixboot 628
- fixmbr 628
- Flash Copy 594
- Flexibilität gegenüber echter Hardware 24
- Floppy 49
- Flush Completed 431
- Fokus, Tastatur, Maus 171
- Fokuswechsel
  - Microsoft 145
  - VMware 117
- Fragmentierte Dateien 538
- Freigegebene Ordner, Virtual PC 206
- Fremdherstellerprodukte 645
- fstab 266
  - ESX 429
- Full Clone 578
- full duplex 505

## G

- Gast 36
- Gast-System 36
- Gateway 229, 460
- gcc 273
- gcc-c++ 273
- Gemeinsamer Zugriff 55
- Gemeinsames Netzwerk (NAT) 449
- Generic Resource 375
- Geometriedaten 418
- Gerätemanagers 542
  - per Kommandozeile 656
- Gerätetreiber 40
- Ghost 621
- Gigabit-Ethernet 84
- Gigabit-Netzwerk, Performance 501
- Glasfaserleitungen 52
- Google-Suchleiste 88
- Grafikintensiv 616
- grep 262
- growable Disks 517
- GRUB 256, 537

## H

- Hacker 239
- HAL (Hardware Abstraction Layer) 632
- Hal.dll 633

- half duplex 505
- Hardware 35
  - ESX Server 398
    - nicht unterstützte 59
- Hardware-Ausfall 603
- Hardware-Kompatibilitätsliste 398
- Hardware-Prüfsummen 616
- Hardware-Unabhängigkeit 25
- Hardwarevirtualisierung 679
- Hardware-Voraussetzungen auf dem Host 81
- Hauptspeicher auf dem Host 47
- Hauptspeichernutzung 83
- Hauptspeicherverwaltung
  - Microsoft 148
  - VMware 120
- havm.vbs, Cluster-Skript 375
- HBA (Host Bus Adapter) 52
- Header File 418, 528
- Headless-Mode 670
- Heartbeat-Netzwerk 339
- High Availability 375
- Hilfsprogramme 645
- Hilfs-VM 621
- HKEY\_LOCAL\_MACHINE 635
- Hochverfügbarkeit ESX 388
- Hochverfügbarkeits-Cluster 337
- Host 36
- Host Based License 400
- Hostadapter 470
- Host-Betriebssysteme 74, 85
  - unterstützte 85
- Host-Cluster 70, 344, 374
- Hosted Server-Produkte 68
- Hosted-Produkte 75
- Host-only 445
- Hot Backup 591
- Hot-Backup Snapshot ESX 430
- Hotplug 518
  - virtuelle Platte beim ESX 394
- httpd.vmware stop 262
- Hyperthreading 45
- Hypervisor 36

## I

- i386 42
  - Debian 252
- ICA-Protokoll (Independent Computing Architecture) 244
- ICS 499
- IDE-Controller 620
  - virtuell 39, 531
- ifconfig 259, 456, 510
- IIS (Internet Information Server) 85
  - installieren 90
- Imaging Tools 652
- Importer 642
- Importvorgang 417

Inaccessible Boot Device 540, 629  
Independent 576  
Independent nonpersistent 525, 532  
Independent-persistent 175, 532  
Informationsquellen 645  
Informationsseiten 659  
initrd 270  
Inkrementelle Sicherung 589  
Installation  
    des Betriebssystems, Virtual PC 195  
    Gastbetriebssystem, Virtual Server 169, 322  
    VMware, Debian Host 260  
    von Microsoft Virtual PC 96  
    von Microsoft Virtual Server 2005 97  
    von Virtual Center 431  
    von VMware Player 87  
    von VMware Server 89  
    von VMware Workstation 87  
Instant-Demo 281  
Int13, 8 GB, Problem 633  
Intel PCI-Fast Ethernet 440  
Intel PRO/1000 Gigabit Adapter 440  
Internes Netzwerk 449, 485  
Internet Connection Sharing (ICS) 499  
Internet Information Server 85  
Internet, Links 659  
Interrupt Coalescing 502  
Interrupt-Drosselung 502  
Inventarisierung 658  
Inventory 110  
Invirtus Virtual Machine Optimizer 649  
IP-Adresse  
    Aufbau 458  
    Netzwerkteil, Hostteil 458  
ipconfig 456  
ipconfig /all 618  
IPCop 211, 217  
    als installierte Appliance 217  
    Zertifikat 238  
IP-Konfiguration, manuell 455  
IPX/SPX 440  
ISA Server 211  
iSCSI (Internet Small Computer  
    System Interface) 52  
iSCSI Cluster 341  
iSCSI Initiator Microsoft, installieren 359  
iSCSI Software Initiator 346  
iSCSI Software Initiator ESX 407  
iSCSI-Initiator 53  
iSCSI-Target 53, 335  
    Installation 354  
ISDN 452  
ISDN-Karten 59, 614  
ISO Images erstellen 650  
ISO-Image 50  
    im Player 293  
    Virtual PC 195  
    Virtual Server 322  
    VMware 169

ISO-Images ESX, Windows 429  
Isolieren von VMs 246

## J

Journaling-Dateisysteme 84  
Jumbo Frames 54

## K

Kaskadierende Differenzplatten 329  
Kernel mit PAE-Option 269  
Kernel32.dll 633  
Kernel-Headers 94, 126, 260  
kernel-image 271  
Kernel-Modus 42  
kernel-source 273  
Klonen 646  
    unabhängiger VMs 348  
    Virtual PC 204  
    von Muster-Vorlagen 645  
Knoppix 623, 653  
Kommandozeile 655  
Komprimierung 649  
    virtueller Festplatten 548  
Konfigurationsdatei vmx 530  
Konservierung alter Systeme 612  
Konsistente Sicherung 592  
    mit Snapshot 598  
Konsistenter Zustand, Backup 391  
Konsolidierung 612  
Kopfddatei 528  
    der virtuellen Platte 419  
    editieren 551

## L

Lab Manager 663  
Laborumgebungen 657  
LAN-CAPI 59, 614  
LANCOM 60  
LAN-Freigaben 55  
Lastmessungen vor der Virtualisierung 83  
Lastspitzen 83  
LBA-Adressierung 515  
Legacy-Anwendungen virtualisieren 612  
Legacy-VM 160, 532  
Lehrgangsteilnehmer 562  
Leistungsindikatoren 83  
Leostream P>V Direct 641  
Lilo 537  
Linked Clone 180, 578  
    im Player 288  
    unter VMware Server 584  
    VMware Player 307  
Linkliste 645  
Links 645, 659  
Linux  
    VMnet 481  
    VMware installieren 93  
linux26 253

Linux-Host  
    Installation 267  
    VMware Server 249  
Live-CD 623  
LiveLinks, Lab Manager 666  
Lizenzdatei ESX, Virtual Center 400  
Lizenzierung  
    VMware ESX 395  
    VMware HA, DRS 434  
    von Microsoft Windows Server 2003 86  
Lizenzierung von Windows Vista 680  
Lizenzserver 405  
Load Balancing mit DRS 388  
local Host 92  
Lock-Datei 529  
Loopback-Adapter 247  
    einrichten 491  
    Virtual PC 208  
LSI Logic 539  
LUN (Logical Unit) 52

**M**

MAC (Media Access Control) 464  
MAC-Adressen  
    beim Klonen 506  
    fest vergeben 506  
    Microsoft 511  
Macintosh 38, 677  
Mailserver DMZ 244  
make cloneconfig 94  
make menuconfig 270  
make oldconfig 270  
make-kpkg clean 270  
Managed Hosts, Lab Manager 664  
Maps 435  
Maschinenbefehle 46  
Master-Boot-Record (MBR) 628  
Master-Images erstellen 647  
Masterstatus 137  
Master-VM 174  
Maus 170  
    Virtual PC 196  
    VMware 117  
Maximalwerte ESX 416  
Memory Ballooning 47  
Memory over-commitment 47  
Memory Page Sharing 122  
Memory Page Trimming 47  
Memory Sharing 47  
Memory Trimming 122  
Microsoft Cluster-Dienste 337  
Microsoft Loopback-Adapter 247, 491  
Microsoft SQL Server Desktop Engine (MSDE) 431  
Microsoft Virtual PC 2004 SP1 66  
Microsoft Virtual PC 2007 677  
Microsoft Virtual Server 2005 R2 70  
Microsoft Virtual Server, Bedienoberfläche 135

Microsoft Windows Services für Unix 383  
Midnight-Commander 258  
Migration 313, 616  
Migrationskonzept, Testumgebung 333  
Minisetaup 646  
Monitoring-Programme 618  
monolithic flat 418  
Monolithische Platten 521  
    reservierte Platte 528  
    Zuwachsplatte 528  
Motorola 38  
Mounten  
    CD unter Linux 650  
    ISO Image 650  
    virtueller Platten 547  
Mountpoint 266  
Mozilla 136  
MPS Multiprozessor PC 631  
MTU Jumboframes 54  
Multicast, USV 605  
Multimedia 616  
Multipathing 394, 606  
Multiple Snapshots 554, 561  
    unter VMware Server 580  
Multiprozessor 44  
    P2V 631  
Muster-VM, vorbereiten SID 645  
Muster-VMs Player 302  
MySQL 187  
MYVIRTUALMACHINES 97  
    Umgebungsvariable 188

**N**

Nachteile virtueller Maschinen 26  
Named Pipe 58  
NAS (Network Attached Storage) 55, 383  
    einrichten ESX 407  
NAT 178, 445  
    Virtual PC 449  
    VMware 475  
NAT Service, VMware 469  
NAT-Router 463  
net stop 656  
netinst-Images 252  
netstat 262  
Networkfencing, Lab Manager 666  
Network-Labels 110  
Netzwerk 177  
    Anwendungsbeispiele 450  
    Debian Host 259  
    ESX 419  
    Komponenten 457  
    Virtual PC 206  
Netzwerkgrundlagen 457  
Netzwerkkarten 84  
    ESX 420  
    unsichtbare 512

Netzwerkconfiguration unter MS Virtual Server 484  
Netzwerkunterstützung VMware Player 291  
Netzwerkverkehr 83  
Neuregistrierungen 537  
Neustart bei Systemfehler 631  
New Virtual Machine Wizard 159  
NewSID 645  
NFS (Network File System) 55, 383  
NFS-Freigaben 384  
Nicht verbunden 485  
nonpersistent 576  
Not bridged 472  
NTBackup 389  
Ntbtlog.txt 630  
NTDS 634  
NTFS 84  
NTFS-Partition unter Linux 266  
Ntldr is missing 628  
Ntoskrnl.exe 633  
Nutzen virtueller Maschinen  
    Anwendergruppen 23

## O

Öffentliches Netzwerk, Cluster 339  
Offload 342  
    Einheit, Netzkarte 376  
    TCP Segmentation 505  
Online-Sicherung 591  
Open-E iSCSI 53  
OpenSUSE 271  
Optimieren von VMs 648  
Ordnerstruktur 84  
OS/2 679  
Overhead RAM 47

## P

P2V (Physical to Virtual) 611  
    Assistant 640  
    auf einen Blick 638  
    Fehler 626  
    Tools 613  
Pacifica AMD 43  
PAE (Physical Address Extension) 48  
    Linux 268  
Parallele Schnittstelle 58  
Parallels Desktop for Mac 677  
Paravirtualisierung 675  
Partitionierung  
    ESX 403  
    Linux Host 254  
pciide.sys 636  
pciidex.sys 636  
PCI-Steckkarten 59  
Performance  
    Netzwerk 501  
    virtueller Platten 521

Performanceprobleme 122  
Perl 187  
    API, vmware-cmd 654  
Persistent 532, 576  
    Targets 360  
PHP 187  
Physikalische Festplatte verknüpfen, Virtual PC 192  
Physische Adapter ESX 420  
Physische CPU 44  
Physische Datenträger 49  
    am Host 50  
Physische Platten in Gast einbinden 534  
Physische SCSI-Geräte 58  
Physischer RAM 47  
Physisches Quellsystem 622  
Pilotmigration 616  
Pilotumgebung, virtuell 313  
PlateSpin 658  
    PowerConvert 641  
    PowerRecon 83  
Plattennamen auswählen 166  
Plattentypen 523  
    Virtual PC 191  
Plattenzugriffe 83  
Platz sparen 648  
    in Gästen 290, 648  
Player  
    Netzwerkunterstützung 291  
    Versteckte Funktionen 292  
Player Extensions Framework 674  
Plug&Play 440  
pnpscsi.inf 543  
Port 902, SUSE 274  
Portforwarding  
    DMZ 244  
    VMware 479  
Portgruppen ESX 420  
PowerChute 605  
PowerOff 114, 168  
    Player 282  
PowerOn 114, 168  
PowerPC 38, 677  
PowerRecon 658  
PPPoE 228, 451  
PPPoE-Verbindung 238  
preallocated Disks 520  
Precompact.iso 548  
Privates Netzwerk, Cluster 339  
Privilegierte Operationen 42–43  
Process Explorer 651  
Produktivbetrieb 313  
Programmierer 563  
Programmierschnittstelle, vmrun.exe 655  
Promiscuous Mode 464  
Protected Mode 42  
Proxy-Server 245  
Prozesse 651

Prozessoren  
    auf dem Host 44  
    im Host 82  
Prüfpunktdateien 591  
psexec.exe 594, 656  
Putty 264, 426, 428, 652

## Q

Qemu 38  
Quellsystem 618  
Quick Switch 117  
Quiescing 430  
    Funktion 390  
Quorumdatenträger 340

## R

Radmin 651  
RAID6 51  
RAID-Controller (Redundant Array of Independent Disks) 51  
RAID-Konfigurationen zur Ausfallsicherheit 84  
RAID-Systeme 606  
RAM-Ausstattung des Host-Rechners 82  
RAM-Inhalt speichern 558  
Raw Device Mapping 383, 534  
RDP Remote-Desktop-Protokoll 77  
RealVNC 651  
Rechte  
    auf Ordner 84  
    Konfigurationsdatei 609  
    Linux 265  
Rechteverwaltung 608  
Redeem license 400  
RedHat Enterprise Linux 380  
Redo-Log 524, 530, 557  
    bei multiplen Snapshots 566  
    einschalten 557  
    konsolidieren 572, 599  
    Player 310  
Redundanz 604  
reg load 635  
reg.exe 635  
regedt32.exe 634  
Registerinhalte speichern 558  
Registrierungszwang 537  
Registry von Fremdsystem ändern 634  
ReiserFS 84  
Remote Desktop Protokoll (RDP) 77  
Remote Desktop-Verbindung, Aero Glass 680  
Remotedesktop (RDP) 136, 215  
    freischalten 147  
    Virtual Server, Gäste 146  
Remote-Konsole  
    Port ändern 272  
    VMware Server 106  
Remote-Steuerung  
    Timeout Microsoft 146

Virtual Server 100  
Remote-Zugriff 78  
Remove Snapshot 599  
    Funktion 556  
Reservation/Limit 392  
Reset 168  
Resource Pool 388  
    anlegen 414  
Ressourcenpools 386  
Resume 115  
resume-vm-default.bat 655  
Revert 172  
    Funktion 555  
    Verwerfen von Änderungen 568  
Ring, Kernelmodus 42  
Router 457  
RouterControl 242  
Routers mit IPCop 234  
Routing  
    über den Host 498  
    über eine VM 498  
Routing-Tabelle 460  
RPM 127  
RPM-Paket 94  
Rückgängig-Datenträger 524  
    verwenden 326  
    Virtual PC 200  
Runtime-Umgebung 278

## S

S3-Trio-Adapter 59  
Samba 264  
SAN (Storage Area Network) 51  
    Cluster 340  
    Spiegelung 607  
Sandbox 245  
SANmelody 53  
SAN-Snapshots 394, 594  
Sarge, Debian 252  
Sasser 239  
SATA 51  
Schreibcashe 536  
Schüler-PC 299  
Schulungsumgebung mit dem Player 297  
Screenshot  
    Microsoft 148  
    VMware 118  
Script Repository 653  
Scripting 653  
Scripting Tool, AutoIT 656  
Scripting-APIs 68, 91  
SCSI  
    in IDE konvertieren 550  
    physisch 51  
    Shunt Driver 545  
    Treiber 539  
    Treiber vorinstallieren 541

- SCSI-Bus für Cluster freigeben 373
- SCSI-Controller, virtuell 531, 539
- SCSI-ID 374
- SCSI-Kits Cluster 340
- scsi-passthru 535
- Segmentation, TCP 505
- Segmente
  - virtueller Platten 521
- Segmentierte Platte 529
- SequoiaView 618, 651
- Serielle Schnittstelle 58
- Server Based License 400
- Service Console 378, 380
- setupcl.exe 646
- setupmgr.exe 646
- sFTP ESX 426
- Shared Folders 119, 176
  - Player 279
- Shared Library, Lab Manager 665
- Shared Storage Cluster 340
- sharedBus 373
- Shares ESX 392, 416
- shell access ESX 425
- Shrink 548
- Shunt-Treiber 545
- Shutdown 656
  - Microsoft 149
- Sicherung des Host-Systems 602
- Sicherungssoftware 588
- SID (Security Identifier) 645
- single disk 521
- Skripte
  - in Gästen starten 656
  - Microsoft 150
  - Microsoft Virtual Server 653
  - VMware Server 654
  - VMware Tools 123, 655
- Slipstream-CD 636
- SMB (Server Message Block) 55, 383
  - Freigaben ESX Server 428
  - Signing 429
- smb.conf 265
- SMB-Freigabe für ISO 429
- SMB-Mount 265
- smbmount 428
- smbpasswd 265
- SMP (symmetrisches Multiprocessing) 46
- SMTP 244
- Snapshot 530, 553
  - ESX 430
  - Funktion 555
  - im Hintergrund 596
  - im laufenden Betrieb 577
  - im Player 285
  - in produktiven Umgebungen 578
  - löschen 571
  - Manager 563
  - mit vmrun.exe 586
  - Tipps 575
  - Überblick 172
  - verwerfen 572
- Snapshotbaum 564
  - Verzweigung 569
- Snapshotstatus
  - beenden 573
  - entfernen, VMware Server 585
- Softwareinitiator
  - iSCSI 54
  - iSCSI, Cluster 342
- Software-Pakete verteilen, Player 281
- Software-Target 356
- Softwareverteilung 155
- Sound 58
- Soundausgabe, Virtual Server mit RDP 147
- Speichernetzwerk 343
- Speichervirtualisierung 336
- split disk 521
- SQL-Datenbank 186
- SSH ESX 426
- sshd\_config 426
- SSH-Tunnel 245
  - DMZ 244
- SSL 111
- SSL-Tunnel 215
- SSL-Verschlüsselung, Virtual Server 100
- Stacking 460
- Standard-IDE-Treiber 620
- Standardordner, Virtual Server 139
- Standardpfad, VMs, Linux Host 263
- Standardverzeichnis, Virtual PC 188
- Standard-Zweikanal-PCI-IDE-Controller 620
- Stand-by
  - Cluster 344
  - Netzwerk ESX 422
- Startprotokollierung 630
- Startreihenfolge
  - CD Virtual Server 322
  - der VMs 110
- Startup/Shutdown 110
- Starwind, Testversion 346
- Status
  - des Gastes 558
  - speichern 142
- Stop 0x0000007b 540
- Stopp-Fehler 00007b 642
- Storage Adapter 411
- Storage Processor 606
- Streamer im Gast 534
- striped disk 521
- Stromausfall 605
- Stromversorgung 605
- Subnet, VMware 473
- Subnetzmaske 459
- Suchpfade Virtual Server 99, 138, 316
- sudo 94



Surgient Virtual QA/Test Lab Management  
  System (VQMS) 667  
SUSE 10 94  
  als Host 251  
SUSE Linux 130, 271  
Suspend 115, 168  
  Player 282  
  Virtual PC 197  
Swapfile 649  
Swap-Partition 539  
  Linux Host 255  
Switch 457, 460  
Symbolischer Link 429  
Sysinternals 651  
Sysprep 645  
  Antwortdatei 646  
sysprep.inf 647  
Systemmonitor zur Lastmessung 83  
Systemstatus 596

## T

TAR 127  
TAR-Archiv 94  
Taskmanager 651  
Tastatur  
  im Gast VMware 170  
  und Maus im Gast 58  
  Virtual PC 196  
  VMware 117  
TCP Segmentation 505  
TCP/IP 460  
Teaming 505  
  ESX 393  
Teaming-Profil 421  
Teaming-Regeln 423  
Teams VMware Workstation 182  
Templates 579  
  erstellen 647  
Templates, Lab Manager 665  
Terminalserver 78, 215  
  DMZ 244  
Testcenter, online ESX 397  
testdisk 628  
Testnetzwerk 333  
Testumgebung 83  
  mit VMware 155  
Testumgebungen, Lab Manager 663  
Thin Clients 78  
Timeout Remotesteuerung, Microsoft 146  
Tipps 645  
Transaktionsorientiertes Dateisystem 591  
Transportieren  
  virtueller Maschinen 290, 648  
  von VMs 648  
Treiber vorinstallieren 619

## U

Übernehmen, VMs auf ESX 416  
Ubuntu Linux 94, 127  
udev 483  
Ultimate-P2V 643  
UltraEdit 651  
Umgebungsvariablen 97  
UMTS-Zugang 452  
Umwandeln IDE in SCSI 550  
uname -r 94, 260  
Undoable 525, 532  
Undo-Log 524, 533  
  Rückgängig Datenträger 331  
  Virtual PC 200  
Uplink 421, 460  
  virtuell 464  
USB 1.1 57  
USB 2.0 60, 614, 668  
USB-Dongles 614  
USB-Platte 51, 284  
USB-Stick 299  
USN rollback 596  
USV-Steuerung 123, 605  
USV-Steuerung (USV – Unterbrechungsfreie  
  Stromversorgung) 243  
UUID (Universally Unique Identifier) 507  
uuid.action 508  
UUID-Abfrage, Player 293

## V

V2P, VM zurück auf Hardware 639  
Vanderpool 43  
Verborgene Geräte aufspüren 637  
Verdichten virtueller Zuwachsplatten 547  
Verfügbarkeit virtueller Maschinen 603  
Vergrößern virtueller Platten 549  
Verknüpfte virtuelle Festplatte 535  
Verlorene Pakete 54  
Versiegeln 646  
Verwaltungswebseite (Web-Interface)  
  von Microsoft Virtual Server 137  
  von Virtual Server 99  
VGA-Adapter in einer VM 59  
vhd Datei Virtual PC 192  
vhd, virtuelle Plattendatei 533  
vi, Editor 259  
Video Capture VMware 118  
Virenbefall 587  
Virens Scanner 539  
Virtual Appliances 673  
Virtual CAPI 59  
Virtual CD Control Panel 650  
Virtual Center  
  Agent 379, 386  
  Installation 431  
  Management Server 379, 386, 431  
  Network-Labels 110  
  Warnmeldungen 435

- Virtual Center 1.4 69, 76
- Virtual Center 2 76, 377
- Virtual Desktop Infrastructure 77
- Virtual Infrastructure Client (VI Client) 379, 384
  - installieren 404
- Virtual Infrastructure Web Access 385, 432
- Virtual Machine Account 162
- Virtual Machine Additions 132
  - Virtual PC 198
- Virtual Machine Center 281
- Virtual Machine Ex, Cluster 375
- Virtual Machine Monitor (VMM) 36, 378
- Virtual Machine Network Services 489
- Virtual Machine Tabs 111
- Virtual Machine Wizard 159
- Virtual Machine-Remotesteuerungsclient (VMRC) 136, 316
- Virtual PC 297
  - im VMware Player 294
  - Netzwerk 206
- Virtual PC 2007 677
- Virtual PC-Konsole 190, 194
- Virtual Server Migration Toolkit (VSMT) 643
- Virtual Server, Unterschiede Virtual PC 134
- Virtual Server-Remotesteuerung 143
- Virtual Server-Verwaltungswebseite 315
  - Webadministration 136
- Virtual SMP 379
- Virtualisierung 38
  - physischer Rechner 614
- Virtualisierungslayer 36
- Virtualisierungsvorhaben Lastmessung, Vorbereitung 83
- Virtuelle Adapter 221
  - Anschlussarten 440
- Virtuelle CPU im Gast 46
- Virtuelle DMZ 211
- Virtuelle Domänencontroller 596
- Virtuelle Festplatte
  - komprimieren 548
  - mit fester Größe 520
- Virtuelle Festplatten
  - auf dem Host 49
- Virtuelle Netzwerke 457
  - Komponenten 461
  - Linux 481
  - Schnellstart 439
  - Virtual PC 447
- Virtuelle Netzwerkkarten
  - auf dem Host 462
  - Firewall-VM 218
  - unter VMware 465
  - Virtual Server 484
- Virtuelle Pilotumgebung 313
- Virtuelle Platten 513
  - erstellen VMware 164
  - Player 284
  - vergrößern 549
- Virtual PC 191
- Virtual Server 318
- Virtuelle Switches 463
  - ESX 420
- Virtuelle Testumgebungen 663
- Vista 650, 680
- VIX API 676
- VIX API, vmrun.exe 655
- Vizioncore 658
- vltance 467
- VLAN-ID 424
- VLANs 393
- VM aufnehmen
  - Virtual Server 142
  - VMware 114
- VM entfernen
  - Virtual Server 141
  - VMware 113
- VM erstellen
  - ESX 414
  - Virtual PC Überblick 193
  - Virtual Server 140, 317
  - VMware 111, 167
- VM Network, Portgruppe 421
- VM übernehmen auf ESX 416
- vmc, Datei, Virtual PC 192
- vmc, Konfigurationsdatei 533
- vmdk, Plattendatei 527
- vmem
  - Datei 115
  - Snapshotdatei 567
- VMFS (Virtual Machine File System) 84
- VMFS (VMware Filesystem) 381
- VMFS 3 378
- VMFS, Datenspeicher anlegen und erweitern 412
- VMFS-Dateisystem anlegen 407
- VMFS-Volumen 382
- VMkernel 378, 380
- vmkfstools 417
- VMlogix Lab Manager 667
- vmmemctl-Treiber 47
- VMnet0, Bridged 471
- VMnet1, Host-only 471
- VMnet8, NAT 471
- vmnetcfg.exe 292
- vmnet-dhcpd 262
- vmnetnat.conf 479
- vmnet-natd 262
- VMnet-Switches 221
- vmnic0 420
- VMotion 379, 387
- VmPerl Scripting API 654
- VMRC Client 100
- vmrc.exe 100, 136
- vmrun.exe 586, 597, 676
  - Beispielskript 654
- vmsn, Snapshotdatei 567
- vmsnap.pl 601

- vmss, Datei 115
  - VMTN (VMware Technology Network) 78
  - VMware Accelerated AMD PCNet 467
  - VMware ACE (Assured Computing Environment) 77
  - VMware Consolidated Backup (VCB) 379, 389
  - VMware Converter 672, 681
  - VMware DHCP Service 475
  - VMware DiskMount 545
  - VMware DiskMount, Workstation 6 669
  - VMware DRS (Distributed Resource Scheduler) 379, 387
  - VMware ESX Server 3 72
  - VMware Fusion 677
  - VMware HA (High Availability) 379, 388
  - VMware Infrastructure 3 377
  - VMware Management Interface 93, 262
    - Debian Host 261
  - VMware NAT Service 475
  - VMware PCI Ethernet Adapter 440
  - VMware Player 63
    - Anleitung 277, 297
    - Anwendung, Vorteile 298
    - Anwendungsbeispiele 280
    - Bedienung 105
    - Schulung oder Demo 297
    - Unterschiede und Gemeinsamkeiten 278
  - VMware Player 2.0 674
  - VMware Server 68
    - Bedienoberfläche 106
    - Console 92
    - Console (Remote Console) 93, 109
    - Console Befehlszeile 109
    - Console for Windows 263
    - Management Interface (Web-Interface) 109
      - unter SUSE Linux 271
    - Vergleich zur Workstation 107
  - vmware stop 262
  - VMware Technology Network (VMTN) 78
  - VMware Tools 171
    - Funktionsbeschreibung 104
    - im Player 295
    - im Player installieren 306
    - installieren 125
    - Skripte 655
  - VMware Virtual Center 2 (VC2) 379, 386
  - VMware Virtual Desktop Infrastructure 77
  - VMware Virtual Lab Manager 663
  - VMware Virtual Machine Importer 613, 642
  - VMware Virtual Machine Importer 2 417
  - VMware Virtual SCSI Driver 541
  - VMware VMI (Virtual Machine Interface) 3.0 675
  - VMware Workstation 5.5 65
    - Bedienoberfläche 106
  - VMware Workstation 6 667
  - VMware, SCSI-Treiber 541
  - vmware-any-any-update 253
  - vmware-authd 274
  - vmware-cmd ESX 430
  - vmware-cmd, Beispielskript 654
  - vmware-config.pl 95, 262, 481
  - vmware-config-mui.pl 262
  - VMware-DiskMount, P2V 624
  - VMware-Fenster, Bedienung 168
  - vmware-install.pl 95, 260
  - vmware-mount.exe 545
  - vmware-mui 262
  - vmware-mui-distrib 261
  - vmware-serverd 262
  - vmware-server-distrib 260
  - vmware-uninstall.pl 262
  - vmware-vdiskmanager.exe 546, 550
  - vmx, Konfigurationsdatei 530
  - vmx-Datei 292
  - vmx-Generatoren 294
  - vmxnet 467
  - VNC 651
  - VNC-Server, Workstation 6 671
  - Vollbildmodus
    - Microsoft 146
    - Player 284
  - Vollbild-Player 310
  - Vollqualifizierter Pfad, Virtual Server 139
  - Volume Shadow Copy Services (VSS) 593
    - Skript 653
  - Volumenschattenkopien 593
  - Voraussetzungen zur Installation 81
  - Vorlageclients 563
  - Vorlagen erstellen 647
  - Vorreservierte Platten fester Größe 520
  - Vorteile virtueller Maschinen 24
  - VPN 215
  - vshadow.exe 594, 653
  - VSPlus für Virtual Server 657
  - vswif 430
  - vswif0 420
  - vSwitch0 420, 430
  - VT (Virtualization Technology) 43
- W**
- Webdesigner 563
  - Web-Interface 262
  - Webserver
    - im VMware Player 281
    - virtuell 185
  - WebsitePort 1024 98
  - Weitergeben von VMs 648
  - Wiederanlaufpunkte 554
    - setzen 561
    - Virtual PC 202
    - Virtual Server 326
  - Wiederherstellung 587
    - des Hosts 602
  - Wiederherstellungskonsole 628
  - Windows Vista 650, 680

Windows-Client 262  
Windows-Firewall 99  
WinImage 547, 650  
WinISO 650  
WinSCP 426, 652  
Winscp 264  
WinTarget 53  
Wirt 36  
Wirtsrechner 36  
Workspace, Lab Manager 665  
Würmer 239

## **X**

XAMPP 187  
xlibs-dev 94  
XRN (Expandable Resilient Networking) 606

## **Y**

YaST 94, 271  
You are here 564  
You do not have VMware Tools installed! 224

## **Z**

Zeitscheibe 45  
Zentraler Fileserver 55  
Zusammenarbeit, Workstation Player 311  
Zusatzprodukte 645  
Zuwachsplatten 517

