

*Leitfaden für Installation,
Konfiguration und Optimierung*

2. Auflage

Praxishandbuch VMware vSphere 5



O'REILLY®

Ralph Göpel

Praxishandbuch VMware vSphere 5

Ralph Göpel

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Sebastopol • Tokyo

Die Informationen in diesem Buch wurden mit größter Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden. Verlag, Autoren und Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für eventuell verbliebene Fehler und deren Folgen.

Alle Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt und sind möglicherweise eingetragene Warenzeichen. Der Verlag richtet sich im Wesentlichen nach den Schreibweisen der Hersteller. Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Alle Rechte vorbehalten einschließlich der Vervielfältigung, Übersetzung, Mikroverfilmung sowie Einspeicherung und Verarbeitung in elektronischen Systemen.

Kommentare und Fragen können Sie gerne an uns richten:

O'Reilly Verlag

Balthasarstr. 81

50670 Köln

E-Mail: kommentar@oreilly.de

Copyright der deutschen Ausgabe:

© 2012 by O'Reilly Verlag GmbH & Co. KG

1. Auflage 2010

2. Auflage 2012

Die Darstellung einer Qualle im Zusammenhang mit dem Thema Virtualisierung ist ein Warenzeichen von O'Reilly Media, Inc.

Bibliografische Information Der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Lektorat: Christine Haite, Volker Bombien, Köln

Korrektur: Eike Nitz, Köln

Satz: III-satz, Husby, www.drei-satz.de

Umschlaggestaltung: Marcia Friedman, Boston & Michael Oreal, Köln

Produktion: Andrea Miß, Köln

Belichtung, Druck und buchbinderische Verarbeitung:

Druckerei Kösel, Krugzell; www.koeselbuch.de

ISBN 978-3-86899-164-2

Dieses Buch ist auf 100% chlorfrei gebleichtem Papier gedruckt.

Vorwort	IX
1 Einführung	1
Virtualisierung im Allgemeinen	1
Die Technik virtueller Maschinen	3
Hardwareausstattung	6
Virtualisierung mit VMware	8
2 Die Bestandteile von vSphere	11
Komponenten der vSphere-Umgebung	11
Die Editionen im Vergleich	15
3 Der Hypervisor	19
Embedded oder Installable	20
ESXi-Hardwareanforderungen	21
ESXi-Hardwareempfehlungen	23
ESXi interaktiv installieren	23
Alternative Installationsmöglichkeiten	31
Den ersten ESXi-Host verwalten	34
Den vSphere Client konfigurieren	36
4 Die virtuelle Maschine	41
Eine virtuelle Maschine erstellen	41
Betriebssystem installieren	53
VMware Tools installieren	55
Virtuelle Maschinen optimieren	68
Gasthardware ändern	72
Gasthardware hinzufügen	80

Optionen der virtuellen Maschine	88
Ressourcenkontrolle der VM	95
BIOS-Einstellungen der virtuellen Maschine	100
EFI-Einstellungen der virtuellen Maschine	104
Dateien der virtuellen Maschine	104
Die MAC-Adresse der VM	111
5 Konfiguration und Einstellungen des ESXi Servers	113
Hardwareeinstellungen des ESXi Servers	114
Softwareeinstellungen des ESXi Servers	118
Registerkarten des ESXi Servers	125
Die Menüleiste unter ESXi	137
6 Netzwerkconfiguration	143
Netzwerkkonzepte	143
Internet Protocol Version 6	147
Netzwerkdienste	149
VLAN	150
vNetwork-Standardswitches	153
Netzwerkconfiguration des VMkernels	156
Konfiguration des Management Network	159
vSwitches optimieren	166
Empfehlungen zu Netzwerkoptimierungen	169
Fehlerbehebung auf der Konsole	169
7 Storage-Konfiguration	179
Allgemeine Richtlinien	179
iSCSI-Speicher anschließen	181
iSCSI-Konfiguration unter Windows	182
NFS-Speicher anschließen	193
Fibre-Channel-Storage	196
VSA-Storage	197
Storage Alignment	198
Installation & Konfiguration eines Debian iSCSI-Storages	200
Virtuelle Maschinen verschieben	211
8 Snapshots	213
Was ist ein Snapshot?	213
Einen Snapshot erstellen	215
Den Snapshot-Manager verwenden	217

9	Arbeiten auf der Kommandozeile	223
	Der Standardeditor vi	224
	Dienste und Konfigurationsdateien	225
	Die Kommandozeile, wichtige Dateien und Befehle	232
	Skripten	245
	Weitere Tools	247
	Eigene Skripten schreiben	251
10	Der vCenter Server	255
	Funktionen des vCenter Servers	255
	Die technischen Voraussetzungen für einen vCenter Server	265
	Den vCenter Server installieren	269
	vCenter Server-Lizenzen	280
	Logdateien des vCenter Servers	283
	vCenter Server-Startprobleme beheben	286
	Einen Cluster erstellen	291
11	VSA und Hostprofile	315
	Hostprofil erstellen	315
	vSphere Auto Deploy	321
	VSA Storage	322
12	VMware vApp und Fernzugriff auf virtuelle Maschinen	327
	Eine vApp erstellen	328
	vApps löschen	332
	VMware WebAccess	332
	Die VMware Remote Console manuell einrichten	339
	Remote Desktop Protocol	342
13	VMware Update Manager, Upgrade und Converter	345
	Konsolidieren	345
	Update Manager	352
	vSphere Client-Plugin installieren	352
	Den Update Manager konfigurieren	353
	Einen Host updaten	355
	Upgrade der Umgebung	358
14	Templates (Vorlagen für virtuelle Maschinen)	369
	Templates und ihr Nutzen	369

15 vCenter Server – Konfiguration und Alarmer	381
Einstellungen des vCenter Servers	381
Alarmer	385
16 Datensicherung und -wiederherstellung	395
Backup-Unterschiede zwischen den Welten	395
Sicherung des Hosts	396
Sicherung der VMs	396
VMware Data Recovery	397
Data Recovery konfigurieren	403
Assistent für Sicherungsaufgaben	409
Virtuelle Maschinen wiederherstellen	410
Lösungen von Quest	417
Lösungen von Veeam	418
17 Sicherheit in der virtuellen Umgebung	419
Die Architektur der Sicherheitsfeatures	419
Portabsicherung virtueller Switches	422
Benutzerpasswortbeschränkungen	424
Allgemeine Sicherheitsempfehlungen	428
Firewall-Konfiguration im vCenter Server	431
18 Ressourcen, Optimierung und Troubleshooting	437
Ressourcenverwaltung	437
Virtueller Speicher der VMs	440
Ressourcenpools für VM-Gruppen	443
VM-Speicherprofil und Storage DRS	446
Optimierung von VMs	448
Performance überwachen	450
vSphere5-Troubleshooting	453
An HA beteiligte Komponenten	457
Weitere Tools	462
Index	467

Vorwort

Nach dem Erfolg mit der ersten Version meines Buches über VMware vSphere 4 und den vielen Nachfragen nach einer Neuauflage, habe ich die letzten sechs Monate fast jede freie Minute mit vSphere 5 zugebracht. Ein reines Aktualisieren der alten Fassung war mir nicht genug: Alle bisherigen Optionen mussten erneut überprüft werden, und alle neuen Funktionen sollten so einfach und detailliert wie möglich beschrieben werden. Deshalb ist der Umfang dieses Buches auch deutlich größer und mit vielen Beispielen, Hinweisen und Tipps bestückt.

Viele meiner Seminarteilnehmer, die das Praxishandbuch vSphere 4 zum Unterricht bei der GFU Cyrus AG in Köln bekommen haben, sagten mir erstaunt, wie einfach verständlich die teils doch schwierige Materie darin erklärt würde. Deshalb habe ich mir dieses Mal noch mehr Mühe gegeben, das beizubehalten und auszubauen.

Aufbau des Buchs

Diese Lektüre ist wieder so aufgebaut, dass man sich vom Anfang bis zum Ende eine eigene produktive Umgebung schaffen kann, ohne später auf etwas zu stoßen, das man vorher nicht wusste. Auch als Nachschlagewerk ist es gedacht, wenn man weitere Bausteine dem System hinzufügen oder nachträglich etwas ändern möchte.

Kapitel 1, *Einführung*, soll Ihnen kurz erläutern, was Virtualisierung im Allgemeinen ist, warum jedermann virtualisieren möchte und wann man darauf verzichten sollte. Weiterhin wird besprochen, was eine virtuelle Maschine ausmacht und warum man dafür VMware nehmen sollte.

In Kapitel 2, *Die Bestandteile von vSphere*, stelle ich Ihnen die einzelnen Komponenten der Umgebung vor. Dazu finden Sie dort eine Tabelle mit allen Editionen und den darin enthaltenen Funktionen.

Das Kapitel 3, *Der Hypervisor*, gibt zunächst einen Überblick über dessen Aufbau und Funktionsweise sowie über die Unterschiede der einzelnen Varianten. Dann geht es direkt weiter zur »richtigen« Installation mit vielen Hinweisen und Tipps.

In Kapitel 4, *Die virtuelle Maschine*, wird die Installation, Konfiguration und Optimierung von virtuellen Maschinen besprochen. Auch hier gibt es wieder viele Fingerzeige dazu, was (noch?) nicht funktioniert und was man besser machen kann, als der integrierte Assistent es vorschlägt.

Sind die ersten VMs erstellt, sollte man sich mit Kapitel 5, *Konfiguration und Einstellungen des ESXi Servers*, beschäftigen und die notwendigen Einstellungen dort vornehmen. Auch die Berechtigungen und Rollen kommen dabei nicht zu kurz.

Der *Netzwerkkonfiguration* habe ich das Kapitel 6 gewidmet. Darin geht es um die Einrichtung und Konfiguration der virtuellen Switches, um VLANs, Teaming, Optimierung und wie man zwei bis sechs Adapter bestmöglich zuweist.

In Kapitel 7, *Storage-Konfiguration* geht es um die Anbindung des ESXi Servers an einen externen und die richtige Konfiguration des internen Speichers. Sehr interessant dürfte für viele die kostenlose iSCSI-Anbindung der ESXi Server unter Windows und Linux sein.

Um *Snapshots* und alles, was man darüber wissen sollte, geht es in Kapitel 8.

Das Kapitel 9, *Arbeiten auf der Kommandozeile*, beinhaltet alles, was man dafür braucht und was wichtig ist. Es wird der zur Verfügung stehende integrierte Editor besprochen, was man als Windows-User statt dessen nutzen kann, welche Befehle für welchen Zweck eingesetzt werden können und wie man Probleme über die Kommandozeile beheben kann.

Die Installation, Konfiguration und Fehlerbehebung des vCenter Servers wird in Kapitel 10, *Der vCenter Server*, besprochen. Dazu gehört natürlich auch die Erstellung eines Clusters und mögliche Funktionskomponenten wie HA, DRS, DPM, FT usw.

Kapitel 11, *VSA und Hostprofile*, zeigt Ihnen detailliert, wie Sie Hostprofile nach dem Einrichten der vSphere-Umgebung nutzen können und sollten und erklärt die Einrichtung, Vor – und Nachteile von der vSphere Storage Appliance.

Was ist eine vApp, und wie kann ich sie einsetzen? Das wird in Kapitel 12, *VMware vApp und Fernzugriff auf virtuelle Maschinen*, besprochen. Weiterhin behandelt das Kapitel den Fernzugriff auf virtuelle Maschinen. Dort habe ich mehrere Möglichkeiten aufgezeigt, wie man z.B. Usern die Remote-Console bestmöglich einrichten kann.

Das Kapitel 13 behandelt den *VMware Update Manager* den *VMware Converter* und das *Upgraden* einer älteren Umgebung. Dort werden aber auch weitere Möglichkeiten von anderen Herstellern aufgezeigt.

Von *Templates (Vorlagen für virtuelle Maschinen)* handelt das Kapitel 14. Wie erstelle und wie nutze ich diese richtig, und wo müssen die Sysprep-Dateien hin? Hier wird es gezeigt.

Der *Konfiguration des vCenter Servers* und den *Alarmen* habe ich das Kapitel 15 gewidmet. Hier wird jede Option der Einstellungen besprochen. Gerade bei den Alarmen hatte ich viel Spaß.

Das Kapitel 16 handelt von der *Datensicherung und Wiederherstellung*, worin die Unterschiede zwischen virtuellen und physikalischen Maschinen bestehen und wie das neue

Tool *VMware Data Recovery* eingesetzt werden kann. Nicht unerwähnt bleiben dabei zwei wichtige Produkte von anderen Herstellern.

In Kapitel 17, *Sicherheit in der virtuellen Umgebung*, habe ich viele Hinweise und Tipps über die Nutzung der VMware-eigenen Funktionen niedergeschrieben. Dabei geht es natürlich um die Sicherheit von Netzwerk, Speicher und VMs sowie um den Zugriff der User von außen.

Das letzte Kapitel (Kapitel 18), *Ressourcen, Optimierung und Troubleshooting*, behandelt zentral die Ressourcenverwaltung, Optimierung und Fehlerbeseitigung der gesamten Umgebung. Hier werden auch noch weitere Tools vorgestellt.

Für wen ist dieses Buch?

Ich gehe davon aus, dass Sie schon wissen, dass Sie virtualisieren wollen, oder es bereits gemacht haben. Trotzdem wollen Sie mehr über dieses Thema wissen und vielleicht herausbekommen, warum die eine oder andere Sache nicht funktioniert, oder Sie glauben, etwas übersehen zu haben. Vielleicht wurde Ihre Umgebung auch von einem externen Dienstleister eingerichtet, und Sie stehen davor wie der häufig zitierte Ochs vorm Berge? Auch dann ist dieses Buch etwas für Sie.

Typografische Konventionen

In diesem Buch werden die folgenden typografischen Konventionen verwendet:

Kursivschrift

Wird für Datei- und Verzeichnisnamen, E-Mail-Adressen und URLs, aber auch bei der Definition neuer Fachbegriffe und für Hervorhebungen verwendet.

Nichtproportionalschrift

Wird für Kommandozeilenbefehle, Skripte und den Inhalt von Konfigurationsdateien etc. verwendet.

Nichtproportionalschrift fett

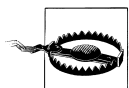
Wird in den Codebeispielen zur Hervorhebung einzelner Zeilen oder Abschnitte verwendet.

KAPITÄLCHEN

Verwenden wir für alle GUI-Elemente wie Buttons und Menüeinträge.



Die Tierspur kennzeichnet einen Tipp oder einen generellen Hinweis mit nützlichen Zusatzinformationen zum Thema.



Die Falle kennzeichnet eine Warnung oder ein Thema, bei dem man Vorsicht walten lassen sollte.

Zusätzliches Material online

Unter der URL http://examples.oreilly.de/german_examples/praxvbmwarevs5ger finden Sie einige der hier vorgestellten freien Dokumentationen und nützlichen Werkzeuge sowie Dateien des Autors zum Download.

Danksagung

In diesem Abschnitt möchte ich meiner Frau Barbara für ihr erneutes Verständnis und die viele Zeit danken, die sie mir gab, um auch dieses Buch fertig stellen zu können.

Weiterhin danken möchte ich der Firma GFU Cyrus AG, bei der ich seit einigen Jahren Seminare u.a. zum Thema Virtualisierung anbiete, weil sie mir die erforderliche Hardware zur Verfügung stellte.

Weiterhin soll Herr Christian Schneiker nicht unerwähnt bleiben, der mir bei dem Aufbau eines Debian-iSCSI-Storages hilfreich unter die Arme griff.

In diesem Kapitel wollen wir uns kurz mit der Thematik der Virtualisierung im Allgemeinen befassen und die wichtigsten Begrifflichkeiten klären. Anschließend geht's dann direkt los mit dem Produkt vSphere5 von VMware.

Virtualisierung im Allgemeinen

Um mal eben etwas auszuprobieren oder ein weiteres Betriebssystem zu installieren, muss man nicht unbedingt eine zusätzliche Partition zur Installation haben oder gar einen weiteren Rechner anschaffen. In den meisten Fällen reicht es, eine Software zu starten, »in« der ein zusätzlicher Computer unabhängig läuft. Die Anwendung einer solchen Konstellation nennt man *Virtualisierung*. Der Computer, auf dem die Software installiert wird, heißt dann *Host* oder *Wirt*, und den Rechner, der im Fenster läuft, nennt man *virtuelle Maschine* (im Folgenden oft mit VM abgekürzt).

Natürlich erlauben viele Betriebssysteme und Anwendungen heute eine Testphase von 30 oder sogar mehr Tagen. Aber wer möchte schon gerne auf seinem Arbeitsrechner geschweige denn auf einem Server eine Software zu Testzwecken installieren, nur um nach ein paar Tagen festzustellen, dass sie sich nicht mehr so einfach deinstallieren lässt? In einer virtuellen Maschine kann keine Software Schaden anrichten, und mit den meisten Virtualisierungsprogrammen lässt sich vor der Installation der aktuelle Zustand einfrieren und anschließend nach Belieben wiederherstellen.

Ein Computer, der beliebig viele virtuelle PCs emulieren kann, also unabhängige und verschiedene Betriebssysteme in Fenstern laufen lassen kann, ist der Traum jedes Entwicklers, Supporters und auch versuchsfreudigen Anwenders. Programme von VMware, Microsofts Virtual PC/Server, Virtual Iron, Blochs oder anderen erzeugen einen kompletten virtuellen Rechner. Mit nur ein paar Mausklicks steht ein neuer Test-PC schnell zur Verfügung.

So ein PC-Emulator ist ein Programm, das nach dem Start virtuelle Maschinen (kurz VMs) auf einem Hostsystem (also dem realen Hardwarecomputer) zur Verfügung stellt, in denen sich weitere Betriebssysteme installieren lassen (die *Gastsysteme*). Eine VM verfügt – wie jeder echte PC – über die üblichen Hardwarekomponenten Prozessor, Arbeitsspeicher, Festplatte, Netzwerkkarte usw. und bringt auch ein eigenes BIOS oder EFI (Extensible Firmware Interface) mit. Die im Fenster installierten Gastbetriebssysteme bemerken üblicherweise nicht, dass die Hardware, auf der sie laufen, nur emuliert wird.

Die meisten Hersteller solcher Virtualisierungslösungen sind sich dabei sogar einig und nutzen die gleiche Hardwareausstattung für ihre virtuelle Umgebung. Da sich der i440BX-Chipsatz von Intel zu Zeiten des Pentium II als sehr stabil erwiesen hat, wird meist dieser in der VM zur Verfügung gestellt. Das wiederum hat den Vorteil, dass sowohl alte als auch neue Microsoft-Betriebssysteme und auch so gut wie alle Linux-Distributionen in der virtuellen Maschine installiert werden können. Abhängig vom Hersteller der eingesetzten Applikation sind auch andere Betriebssysteme einsetzbar, z. B. DOS, Novell, Unix, OS/2, Mac OS X, usw.

Warum virtualisieren?

Viele spezielle Anwendungen, gerade auf Serverbetriebssystemen, erfordern einen eigenständigen Rechner. Nur so garantiert der Hersteller einen reibungslosen Einsatz. Gerade in der öffentlichen Verwaltung und in Krankenhäusern werden diese Anforderungen an den Einsatz der Software im produktiven Bereich gestellt. In der Praxis sind das dann häufig Computer, die bei 2 bis 5 % CPU-Auslastung laufen! Als virtuelle Maschine könnten aber gut zehn solcher Server eine einzige Hardware benutzen, um die Systemauslastung dann bei 20 bis 50 % zu halten. Die gesparten neun Computer verbrauchen somit keinen Strom und belasten die Klimaanlage nicht – in der Regel rechnet sich die Anschaffung einer Virtualisierungssoftware daher schon nach wenigen Monaten. Das ist auch im Sinne von Green IT und wohl auch die beste Möglichkeit, große Einsparungen zu erreichen.

Wie Sie im Laufe des Buches noch lesen werden, ist die Energieeinsparung beim Virtualisieren jedoch nur einer von mehreren wichtigen Aspekten. Da eine VM nur von wenigen Dateien repräsentiert wird, ist das Kopieren oder *Klonen* des Systems äußerst einfach. Durch das Nachhalten mehrerer Zustände des Gastbetriebssystems (Snapshots) lässt sich ohne Probleme mal eben etwas ausprobieren sei es eine zusätzliche Software, einer neuer Release-Stand oder auch ein Servicepack für das Betriebssystem. Funktioniert alles bestens, kann dieser Zustand getrost übernommen werden. Geht etwas daneben oder funktioniert nicht wie gewünscht, kann jederzeit zu einem vorherigen Stand zurückgewechselt werden.

Ein weiterer Einsatzzweck für Virtualisierung: Ältere Betriebssysteme wie Windows NT laufen auf aktueller Hardware nicht mehr meistens können sie noch nicht mal auf neuen

Rechnern installiert oder auf sie portiert werden. In einer virtuellen Maschine ist das kein Problem.

Wann nicht virtualisieren?

Einzige Ausnahme bei den installierbaren Betriebssystemen sind wohl Echtzeitsysteme wie QNX, RTOS und VXworks, bei denen es auch nichts bringt, sie virtuell laufen zu lassen. Zeitgenaue Abfolgen bei Betriebssystemen oder Anwendungen sollten nicht virtuell laufen dafür ist das Laufzeitverhalten der VM nicht genau genug. Auch bei manchen Linux-Systemen, gerade mit spezieller Software, ist von der Virtualisierung grundsätzlich abzuraten.

Außerdem wird nur eine Standardhardware zur Verfügung gestellt, so dass spezielle Komponenten wie ISDN-Karten, Steuerungssysteme oder spezielle Bus-Karten usw. leider nicht emuliert werden können.

Was manche SysAdmins abschrecken kann: Die Administration der Systeme ist mit Virtualisierung zwar einfacher und sicherer, in gewisser Weise aber auch komplexer, weil zusätzliche Systeme (ESXi Server, vCenter Server etc.) berücksichtigt werden müssen.

Die Technik virtueller Maschinen

Auf Großrechnern wie den Mainframes von IBM sind virtuelle Maschinen schon seit langer Zeit nichts Besonderes. Das Grundprinzip ist einfach: In einer Sandbox (von Betriebssystem und Dateisystem unabhängige Laufzeitumgebung, in der sich ggf. gefährlicher Code ohne Gefahr für die Stabilität und Sicherheit des Systems testen lässt) wird ein Computer emuliert, der über alle notwendige Hardware sowie Maus und Tastatur verfügt. Innerhalb dieses geschlossenen Systems kann ein Betriebssystem gestartet werden, das auf die virtuelle Hardware zugreift, als sei es ein echter Computer.

In der Praxis gestaltet sich diese Aufgabe jedoch erheblich schwieriger. Immerhin muss eine Vielzahl benötigter Komponenten virtuell erzeugt werden. Da das Betriebssystem auf dem Hostrechner immer den exklusiven Zugriff auf die Hardware behält, kann ein virtuelles Gastbetriebssystem keinen direkten Zugriff auf die reale Hardware bekommen (mit wenigen Ausnahmen). Deshalb findet das Betriebssystem in der virtuellen Maschine auch andere Hardware vor als tatsächlich im PC eingebaut ist.

Die wichtigsten zu emulierenden Komponenten sind folgende:

- Prozessor
- (A)PIC ((Advanced) Programmable Interrupt Controller)
- DMA (Direct Memory Access)
- IDE-Controller, ggf. SCSI oder SAS
- CMOS (BIOS-Setup) oder (U)EFI ((Unified) Extensible Firmware Interface)

- Realtime-Clock (Echtzeituhr)
- PIT (Programmable Interval Timer)
- Memory und I/O-Controller
- Festplattenspeicher
- PCI-Bus und -Host sowie PCI-Bridge
- Videoadapter
- Keyboard-Controller
- Keyboard und Maus (ggf. über USB)

Neben diesen wesentlichen Komponenten wird häufig auch noch eine Reihe anderer Komponenten in der virtuellen Maschine benötigt, wie beispielsweise diese:

- APM oder ACPI (Power Management)
- Netzwerkkarte(n)
- CD-/DVD-Laufwerke
- Soundkarte
- COM- und LPT-Anschlüsse
- Game- bzw. Midi-Port
- USB-Anschlüsse

Zwei der wichtigsten Komponenten – CPU und Festplatte – widme ich einen eigenen Abschnitt, weil hier die meisten Missverständnisse auftreten und sich bei Unwissenheit über bestimmte Details auch Fehler einschleichen können.

Virtueller Prozessor

Die CPU ist der Hauptbestandteil des echten und des virtuellen PCs. Die AMD- oder Intel-Architektur hat allerdings hinsichtlich der Abbildung virtueller Maschinen gegenüber den Mainframes einige Schwächen. Letztere sind schon architektonisch auf VMs ausgelegt. Intel-Entwickler hatten früher hingegen nie einen virtuellen Rechner als Ziel vorgesehen. Einen ersten Schritt machte AMD mit der »Pacifica« genannten Virtualisierungstechnik im Prozessorkern, Intel zog nach und nannte seine Virtualisierungsfunktion zunächst »Vanderpool Technology«. Heute heißt diese Funktion AMD-V bzw. Intel VT und lässt sich im BIOS des Servers aktivieren.

Die AMD- und Intel-Architektur der 32- und 64-Bit-CPUs bietet vier verschiedene Privilegien an, mit denen dem Betriebssystem, Treibern und Programmen unterschiedliche Rechte zugewiesen werden können, was Sie in Abbildung 1-1 sehen können. Normalerweise laufen OS und einige Treiber im sogenannten Ring 0 (Kernel mode) und Applikationen im Ring 3 (User Mode). Der Trick beim Erzeugen eines virtuellen Systems besteht darin, es im Benutzermodus als Applikation ablaufen zu lassen.

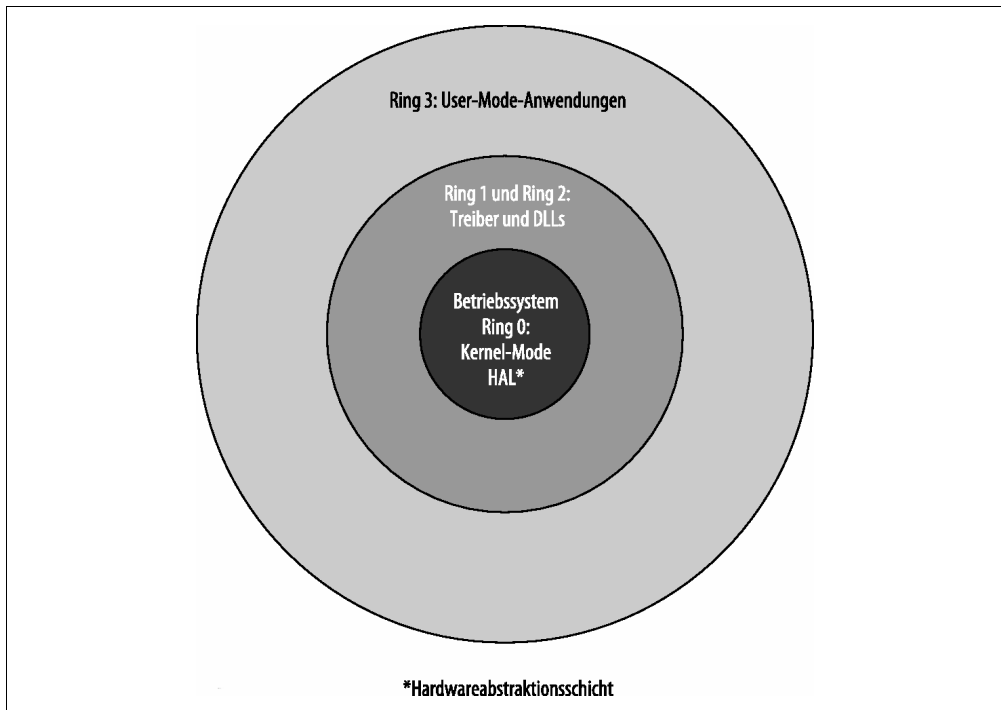


Abbildung 1-1: Die vier Ringmodi eines Betriebssystems

Wenn das Betriebssystem des virtuellen Rechners nun einen Befehl ausführen will, der nur im Ring 0 gestattet ist, löst der Prozessor eine Exception (Ausnahme) aus. Routinen zur Behandlung dieser Ausnahmen können dann den privilegierten Befehl emulieren. Dabei behält das Hostsystem die volle Kontrolle über das System. Die wichtigste Voraussetzung für das Funktionieren dieses Ansatzes ist, dass der Prozessor bei jeder unberechtigt durchgeführten privilegierten Anweisung eine Exception auslöst.

Leider sind die Prozessoren bei den Ausnahmen nicht ganz so gründlich, wie man es sich wünschen könnte. Beispielsweise werden Speicherzugriffe beim x86 über eine GDT (*Global Description Table*, globale Beschreibungstabelle) abgewickelt. Diese ist eine globale Ressource und wird vom Betriebssystem verwaltet. Eigentlich müsste jeder direkte Zugriff auf diese Ressource als privilegierte Handlung angesehen werden und dürfte dementsprechend im User Mode nicht erlaubt sein. Die LGDT-Anweisung (Load Global Descriptor Table) behandelt der x86 sehr wohl als privilegiert, aber die SGDT (Store Global Descriptor Table) führt nicht zu einer Schutzverletzung. Allein diese Inkonsistenz macht es unmöglich, die GDT zu »virtualisieren«.

Um dennoch virtuelle Maschinen auf einer Intel-Architektur mit 32 oder 64 Bit realisieren zu können, müssen sich die Entwickler von Virtualisierungssoftware eine ganze Menge einfallen lassen. Connectix (2003 von Microsoft aufgekauft) untersuchte bei-

spielsweise Code, der im Kernel Mode laufen soll, vor der Ausführung und änderte kritische Sequenzen um.

Damit erklärt sich auch der Eintrag im Gerätemanager der virtuellen Maschine: Er sieht den tatsächlichen Prozessor, kann aber nicht unbedingt jede Funktion von ihm nutzen – dazu später mehr.

Emulation der Festplatte

Ein weiterer wichtiger Bestandteil bei virtuellen Maschinen sind Massenspeicher. Generell funktioniert der Zugriff auf Massenspeicher ähnlich wie beim virtuellen Prozessor. Wenn das Gastsystem eine I/O-Anweisung (Input/Output, Ein- /Ausgabeanweisung) ausführt, wird eine Exception ausgelöst, da es sich dabei um eine privilegierte Anweisung handelt. Die Virtualisierungssoftware fängt diese Exception ab und übersetzt die Anweisung in eine Operation auf dem realen Dateisystem. Bei deren Realisierung steht der VM-Software eine ganze Reihe von Möglichkeiten zur Verfügung.

So könnte sie beispielsweise die Anweisungen direkt auf der physikalischen Festplatte ausführen. Das widerspräche allerdings dem Anspruch an eine Sandbox, denn kein Programm darin darf das Hostsystem beschädigen. Der direkte Zugriff wird zumeist nur bei CD-ROMs oder DVDs eingesetzt. Zwei Ausnahmen davon gibt es allerdings: RDM (Raw Device Mapping, also direkter Zugriff auf eine LUN im SAN) und Direct Pass Through, z.B. bei Netzwerkkarten. Dazu erfahren Sie später mehr.

Meistens wird die virtuelle Festplatte mit einer Datei auf dem Hostbetriebssystem realisiert. Die VM-Software verändert deren Größe teilweise dynamisch. Eine interessante Option sind dabei Festplatten, die beim Herunterfahren wieder in den Zustand von vor dem Start der virtuellen Maschine zurückversetzt werden. So kann man die virtuelle Maschine in einem immer definierten Zustand starten und kritische Tests ausführen. Beim nächsten Start befindet sich die VM wieder im Originalzustand.

Eine Datei auf der Platte des Hosts lässt sich aber auch als virtuelles CD-ROM-Laufwerk verwenden. Hier kommen meist ISO-Images zum Einsatz, so dass die VM-Software nur die reinen Lesebefehle umsetzen muss, ohne sich um das CD-Dateisystem kümmern zu müssen.

Hardwareausstattung

Welche Hardware die zu installierenden Betriebssysteme in einer VM vorfinden, hängt von mehreren Faktoren ab: Erstens von der emulierten Hardware, zweitens von den Komponenten des Wirts, die teilweise an die VM durchgereicht werden, und drittens von der Konfiguration durch den Anwender, der entscheiden kann, welche Hardware emuliert, wie viel davon dem Gast zur Verfügung steht oder was direkt durchgereicht wird. Abbildung 1-2 zeigt beispielhaft den Gerätemanager eines virtuellen Systems.

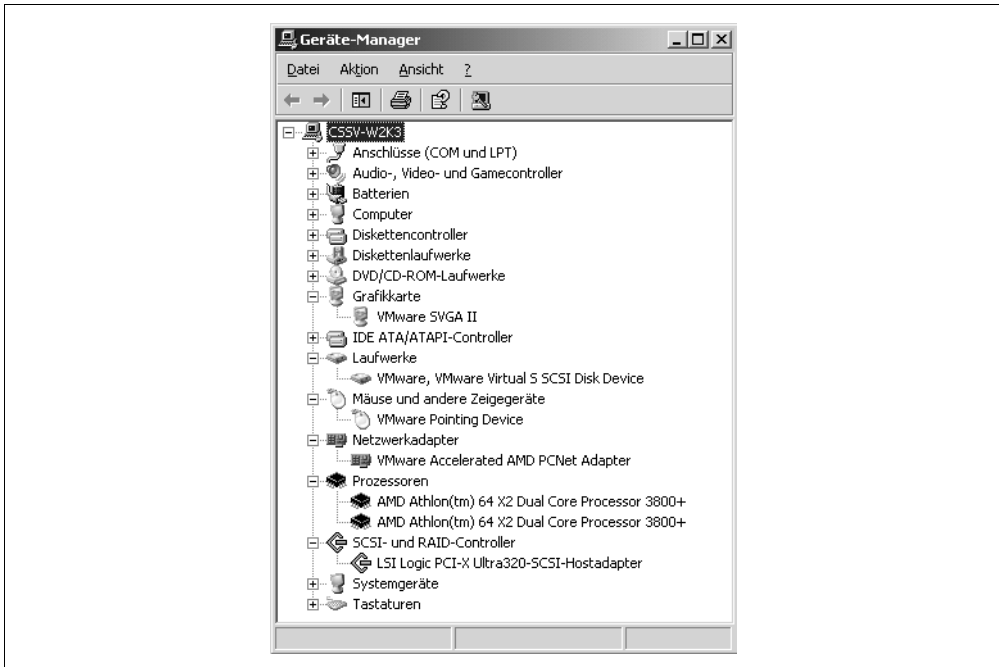


Abbildung 1-2: Gerätemanager unter Windows 2003 in der VM

Zu den emulierten Komponenten der VM gehören Board-Chipsatz (z.B. Intel 440BX), BIOS (AMI oder Phoenix) oder EFI, Festplatte sowie Grafik-, Sound- und Netzwerk-karte. Während Motherboard und Festplatte meistens mit den generischen Treibern der Betriebssysteme laufen, muss für die Grafikkarte ein angepasster Treiber installiert werden. VMware übergibt zum Beispiel der VM eine spezielle SVGA-II- oder sogar 3-D-Karte, Microsoft bevorzugt hier eine Trio 32/64. In den VMware Tools enthaltene Treiber müssen nach der Installation des Betriebssystems noch installiert werden.

Als Netzwerkkarte wird bei VMware eine AMD-PCnet-PCI-II- oder Intel-LAN-Pro-Karte, bei Microsoft eine Intel-21140-Karte emuliert, für die die meisten Linux-Derivate und moderne Windows-Versionen Treiber mitbringen. Weiterhin emuliert VMware als SCSI-Adapter BusLogic und LSIlogic, für den ältere Windows-Versionen passende Treiber haben, XP jedoch nicht. Neuere Windows-Versionen unterstützen zum Teil den einen oder anderen Adapter. Falls nicht, bietet VMware einen Treiber zum Download an, der auch auf der Webseite zu diesem Buch als Floppy-Image (*lsi.flp* und *buslogic.flp*) enthalten ist. In neueren Versionen der Virtualisierungssoftware werden noch weitere Netzwerkkarten und Festplattenadapter unterstützt.

Bei seriellen und parallelen Anschlüssen, CD-, DVD- und Diskettenlaufwerken kann man in der VM wahlweise auf die Hardware des Hosts zurückgreifen oder diese Geräte vollständig emulieren. Andere Hardware wie etwa FireWire-Anschlüsse, (DSL-)Modems

oder interne ISDN-Karten sucht man in der Hardwareausstattung vergeblich. VMware bietet in der neuen Version den Zugriff auf USB-2.0- und -3.0-Geräte sowie externe SCSI-Geräte wie Streamer.

Hypervisoren

Im Allgemeinen unterscheidet man zwischen zwei unterschiedlichen Ansätzen bei der Virtualisierung. Von einem Hypervisor des Typs 1 spricht man, wenn ohne installiertes Betriebssystem eine Virtualisierung von Gastbetriebssystemen direkt auf der Hardware möglich ist, wohingegen der Typ 2 ein vollständiges Betriebssystem voraussetzt und die Virtualisierung durch eine zusätzliche Anwendung zur Verfügung gestellt wird. Beim ersten Typ spricht man auch häufig von *Bare Metal Hypervisor* oder auch *Paravirtualisierung*. Zum Typ 1 zählen zum Beispiel der ESXi Server, XEN, KVM (Kernel-based Virtual Machine), dem Typ 2 ordnet man unter anderem die Workstation und Serverversionen von VMware und Microsoft zu sowie Produkte von Bochs, VirtualBox, QEMU usw.

Virtualisierung mit VMware

Das amerikanische Unternehmen VMware Inc. wurde 1998 in Palo Alto in Kalifornien gegründet, um ein Produkt zu entwickeln, das virtuelle Maschinen auf normalen Computern lauffähig machen kann. Der Mutterkonzern EMC Corporation brachte die Tochter im August 2007 an die Börse und verkaufte nur 10 % der Aktien. Nach dem ersten Tag stiegen die VMware-Aktien von 29 auf 54 US-Dollar und brachten an dem einem Tag über 19 Milliarden Dollar Gewinn.

VMware-Produkte

Als erstes Produkt brachte VMware die WORKSTATION heraus, die heute immer noch das bekannteste Produkt ist und mittlerweile in der Version 8 vorliegt. Diese Applikation wird auf einem bestehenden Betriebssystem (Windows oder Linux) installiert. Ähnlich verhält es sich mit dem kostenlosen Nachfolger des ehemaligen GSX-Servers, dem VMware SERVER, der zurzeit in der Version 2.0.2 vorliegt. Die Version 2.x wird rein über einen Browser gesteuert. Sowohl Workstation als auch Server sind Anwendungen, die aufgrund des darunterliegenden Betriebssystems und eingeschränkten Hardwareausbaus meist nur wenige VMs gleichzeitig laufen lassen können. Dabei ist es egal, ob das Betriebssystem Linux oder Windows ist und ob es sich um z. B. Windows XP oder Server handelt. Diese Version wird seit über zwei Jahren nicht mehr aktualisiert.

Weiterhin gibt es den für den nichtkommerziellen Gebrauch kostenlosen VMware PLAYER, der eigentlich nur vorhandene virtuelle Maschinen abspielen kann. Seit Version 3.0 ist man aber damit ebenfalls in der Lage, neue VMs zu generieren; aktuell liegt er in Version 4.0.1 vor. Der Player läuft unter 32-Bit-Betriebssystemen nur allein, unter 64-Bit

auch mit Server oder Workstation zusammen. Da die Konfigurationsmöglichkeiten hier eingeschränkter sind als beispielsweise bei der VMware Workstation, aber die Anwendung deutlich kleiner ist und weniger Ressourcen verbraucht, ist der Player durchaus dazu geeignet, als Ersatz für einige VMs eingesetzt zu werden.

VMware FUSION ist eine Virtualisierungssoftware für Apple Macintosh-Rechner, die auf einem Intel-Prozessor laufen. Damit hat man die Möglichkeit, Linux und Windows im Fenster zu installieren und laufen zu lassen. Unter Apple-Betriebssystemen ist das die einzige lauffähige Möglichkeit von VMware, denn weder Workstation und Server noch der Player laufen hier.

VMware ACE (Assured Computing Environment) bietet einem ACE-Manager die Möglichkeit, VMs zu erstellen, die zusätzliche Sicherheitsrichtlinien – unabhängig vom Betriebssystem – haben. Zu den Einstellungen gehören Zugriffsrechte und Systemressourcen wie Netzwerk, Drucker, Laufwerke und Ähnliches. ACE ist als Bestandteil in der Workstation enthalten, es gibt aber auch noch weitere Komponenten (ACE Management Server), die man zusätzlich käuflich erwerben kann.

Als Desktop-Virtualisierungslösung gibt es bei VMware VIEW in der Version 5. Der Name der Vorgängerversion, Virtual Desktop Infrastructure (VDI), war da schon aussagekräftiger. Der Sinn dieser Software ist, komplette Arbeitsplatzrechner auf Servern zur Verfügung zu stellen statt am Arbeitsplatz. Die Technologie lässt sich mit Terminals oder Thin Clients vergleichen, die auf einen Terminalserver zugreifen – nur wird hier nicht eine Anwendung zur Verfügung gestellt, sondern ein ganzer Rechner.

Um ähnlich wie bei virtuellen Maschinen nur eine Applikation zur Verfügung zu stellen, bietet VMware das Produkt THINAPP. Damit ist es möglich, jegliche Version jeglicher Software als Applikation für die Benutzer zur Verfügung zu stellen. ThinApp nutzt die *Thinstall*-Technik um Anwendungen in ein MSI-Paket oder eine EXE-Datei zu packen und dann auf einem Server, dem Netzwerk oder einem USB-Stick teilweise ohne Installation zur Verfügung zu stellen.

Für mittelständische bis große Unternehmen war VIRTUAL INFRASTRUCTURE gedacht, das jetzt vSPHERE5 heißt. Der große Unterschied zu den oben genannten Lösungen liegt im Zusammenfassen von mehreren Servern zu einer Ressource, der Verwaltung von mehreren Virtualisierungsservern und virtuellen Maschinen von einem Rechner aus, der Ausfallsicherheit und vielen weiteren Funktionen, die wir in den nächsten Kapiteln ausführlich besprechen werden.

Warum VMware?

Es gibt auf dem Markt mittlerweile sehr viele kommerzielle und Open Source-Lösungen für die Virtualisierung von Rechnern. Viele davon sind mit den oben genannten vergleichbar, mit einer Ausnahme: VMWARE vSPHERE5. Viele Funktionen, die bei diesem System seit einigen Jahren verfügbar sind, werden bisher von keinem anderen Hersteller

angeboten. Den Vergleich braucht VMware bezüglich Funktionen, Sicherheit, Skalierbarkeit, Zuverlässigkeit etc. nicht zu scheuen. Selbst Microsoft hat vor Kurzem auf einer Konferenz zugegeben, dass es ca. drei Jahre hinter der Technologie von vSphere5 hinterherhinkt. Und meiner Meinung nach sind es sogar mehr als drei.

Die Bestandteile von vSphere

In diesem Kapitel erhalten Sie einen groben Überblick über die einzelnen Bestandteile einer vSphere5-Umgebung sowie ihrer Begrifflichkeiten und Funktionen. Weiterhin werden wir die Unterschiede der verschiedenen Editionen besprechen. Die einzelnen ESXi-Einsatzszenarien werden im dritten Kapitel unter die Lupe genommen.

Komponenten der vSphere-Umgebung

VMware vSphere5 besteht aus mehreren Komponenten, die z. T. unabhängig voneinander sind, z.B. einem Betriebssystem und einer Anwendung. Mit einer Anwendung allein kann man allerdings nichts anfangen – man muss ein unterstütztes Betriebssystem haben, auf dem diese installiert werden kann. Genauso verhält es sich mit den Bestandteilen von vSphere: Es ist ein erweiterbares Paket mit Einzelteilen, die teilweise nur etwas bringen, wenn man auch andere Teile hat.

Zunächst ist der *ESXi-Server*, auch Host genannt, zu erwähnen. Er ist ein unabhängiger Computer, auf dem die Installation der Virtualisierungsschicht, also des eigentlichen Hypervisors, durchgeführt wird. Am Host selbst kann man keine virtuellen Maschinen erstellen oder verwalten, dafür benötigt man eine weitere Anwendung, die z.B. auf einem Windows-Client installiert wird. Das ist dann der vSphere Client (vSC). In Abbildung 2-1 sehen Sie, wie ein Client-PC auf den Host zugreift.

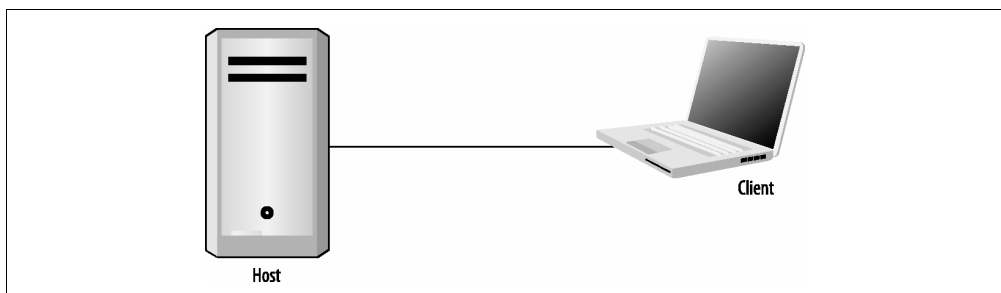


Abbildung 2-1: Hostzugriff über den vSphere Client

Mit diesem Client kann man alle täglich anfallenden Arbeiten auf dem Host durchführen. Auch die Konfiguration des Hosts, das Erstellen der virtuellen Maschinen, das Starten und Herunterfahren, Backup und Recovery usw.

Da man die Clientsoftware auch mehrfach starten kann, besteht die Möglichkeit, mehrere unabhängige Hosts gleichzeitig zu verwalten, wie in Abbildung 2-2 zu sehen ist. Das geschieht dann allerdings in verschiedenen Fenstern, und es ist nicht möglich, virtuelle Maschinen von einem ESXi-Server auf den anderen zu verschieben oder Ressourcen wie Arbeitsspeicher, CPU-Leistung etc. aufzuteilen oder zu bündeln.

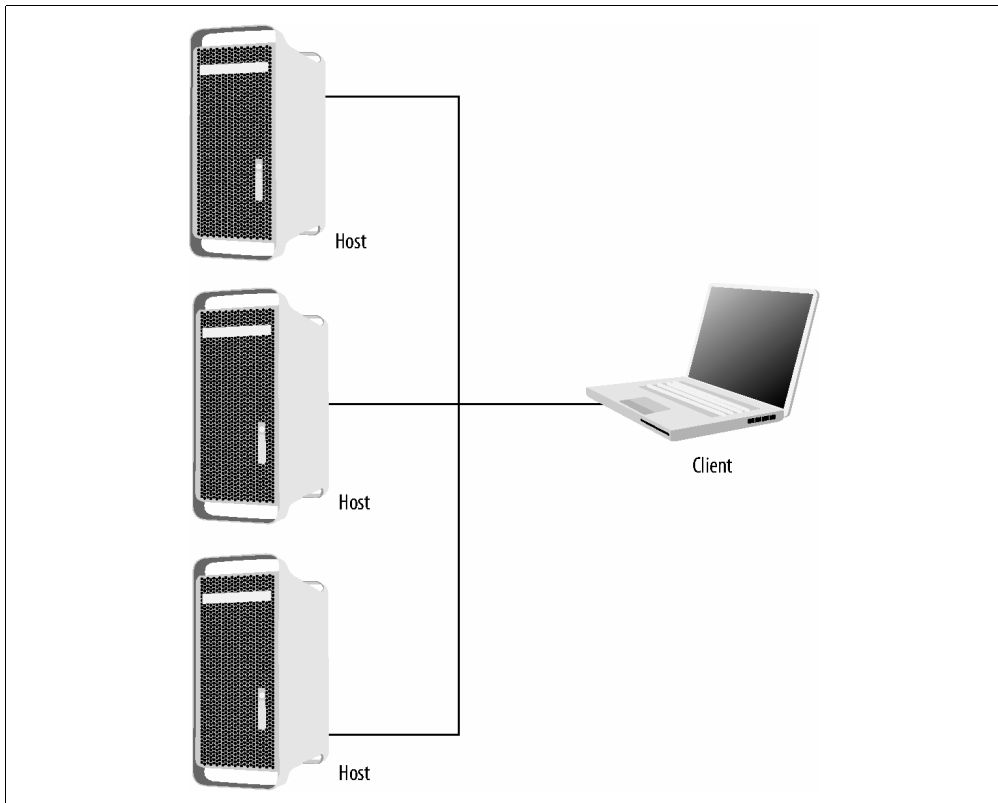


Abbildung 2-2: Ein vSphere Client greift auf drei Hosts zu.

Ist einer der Hosts mit virtuellen Maschinen zu stark belastet und die beiden anderen Hosts langweilen sich, wünscht man sich eine Art automatisches Load-Balancing zwischen den beteiligten Komponenten. Dieses lässt sich über einen vCenter Server erledigen, mit dem man alle ESXi-Server zu einem Cluster verbinden kann.

Fällt die Hardware eines Hypervisors aus, wäre ein automatischer Neustart der ausgefallenen VMs auf den verbliebenen Servern eine tolle Sache. Das (und noch einiges mehr) bekommt man über den vCenter Server hin. Dieser wird als zentrale Managementinstanz

zwischen einem oder mehreren Clients und den ESXi-Servern eingesetzt. In Abbildung 2-3 sehen Sie den Zugriff des Clients über den vCenter Server auf die Hosts und die darauf laufenden virtuellen Maschinen.

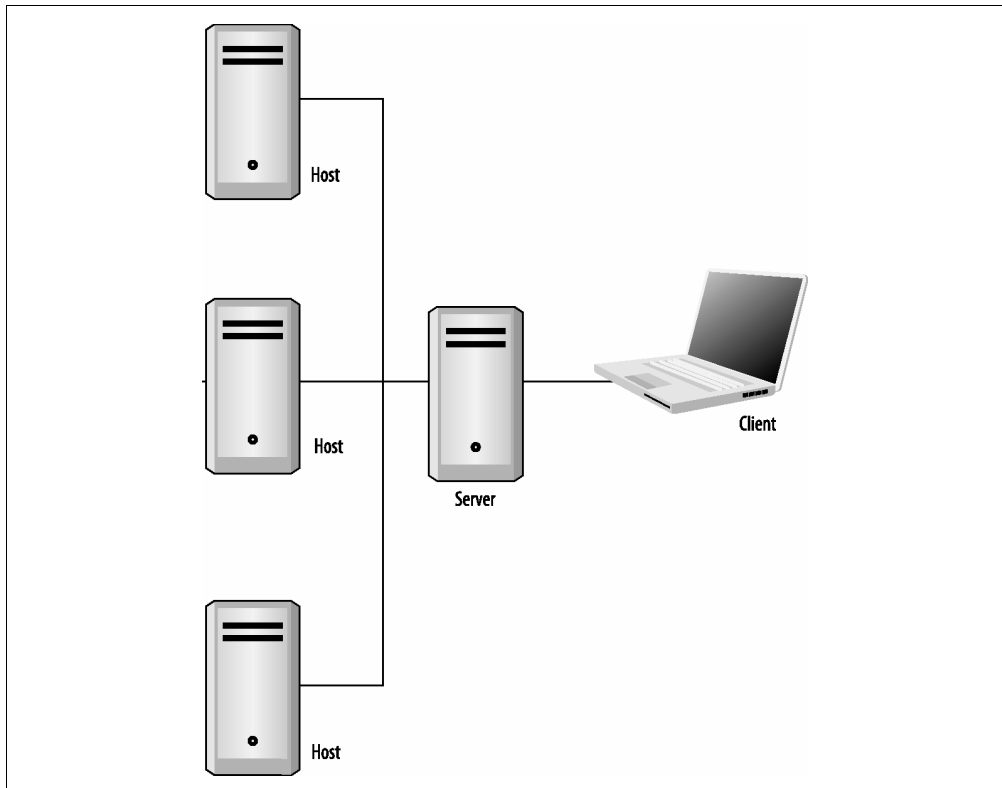


Abbildung 2-3: Zugriff des Clients über den vCenter Server

Ein vCenter Server ist eine Anwendung, die üblicherweise auf einem Windows-Server installiert wird und anschließend als Dienst im Hintergrund läuft. Der Benutzer kann wie vorher mit dem vSphere Client arbeiten und verbindet sich mit dem Managementserver. Dann bekommt er ein Fenster, in dem alle ESXi-Hosts und alle virtuellen Maschinen aufgelistet sind. Neu in der Version vSphere 5 ist eine fertige virtuelle Maschine namens »Appliance«, die auf der Basis von SuSE Linux 11 die Aufgaben des vCenter Servers fast vollständig übernehmen kann.

Um die schon vorher genannten Funktionen wie das Verschieben von VMs zur Laufzeit (vMotion), das Load-Balancing über die Auslastung von Prozessor und Arbeitsspeicher der Hosts (DRS, Distributed Resource Scheduling) oder den automatischen Neustart der VMs beim Ausfall einer Hosthardware (HA, High Availability) zu erreichen, ist ein gemeinsamer Storage (gemeinsame Festplatten, NAS- oder SAN-Speicher) notwendig. Dieser wird wie in Abbildung 2-4 gezeigt an die ESXi-Server angeschlossen.

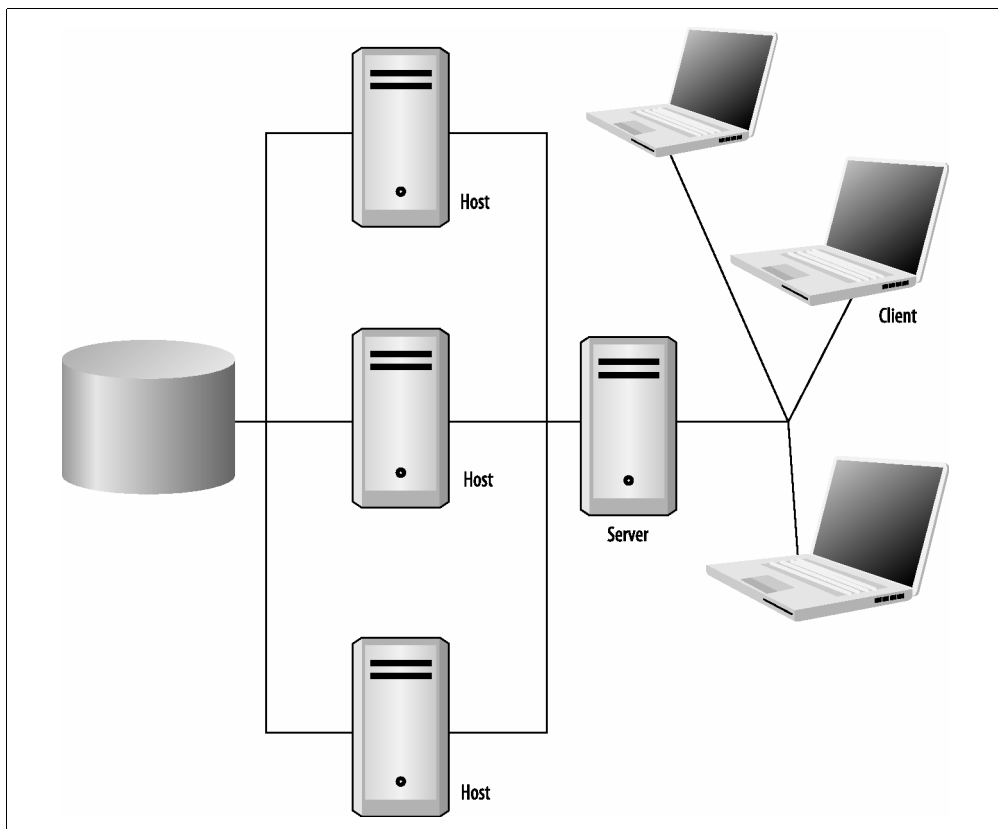


Abbildung 2-4: vSphere4-Umgebung mit SAN

Auf dem gemeinsamen Speicher werden alle Dateien der virtuellen Maschine abgelegt und sind dementsprechend von allen beteiligten Hosts erreichbar.

Das Betriebssystem VMware Cloud

Auf welchem Server sich eine Webseite befindet, spielt beim Zugriff über einen Browser im Internet keine Rolle – Hauptsache, sie wird erreicht. Das Internet wird deswegen in schematischen Zeichnungen meistens als Wolke (»Cloud«) dargestellt.

Da auf die VM immer vom vCenter Server zugegriffen (wie die Internetseite über den Browser) und über diesen gesteuert und kontrolliert wird, können wir die vSphere-Umgebung ebenfalls als Wolke darstellen. Bei VMware versteht man Folgendes unter einer Wolke:

- Auf welchem ESXi-Host sich wann welche virtuelle Maschine befindet, ist unwichtig,
- über welchen Switch eine Netzwerkverbindung zustande kommt, ist aus Sicht des Betriebssystems egal,

- wer Arbeitsspeicher und CPU-Leistung zur Verfügung stellt, spielt keine Rolle und
- wo sich der Festplattenplatz befindet, kann ebenfalls egal sein.

Deshalb nennt VMware vSphere5 ein *Cloud-Computing-Betriebssystem*.

Die Editionen im Vergleich

VMware bietet die Komponenten von vSphere5 in verschiedenen Bundles und den ESXi-Server auch allein an. Je nach Version sind einige der in diesem Buch beschriebenen Funktionen enthalten. Die folgende Tabelle zeigt eine Übersicht über das aktuelle Angebot.

Tabelle 2-1: VMware vSphere-Editionen mit zugehörigen Funktionen

	ESXi Single Server	Essentials	Essentials Plus	Standard	Enterprise	Enterprise Plus
Kompatibilität vCenter Server	keine	vCenter Server für Essentials	vCenter Server für Essentials	vCenter Server Foundation & Standard	vCenter Server Foundation & Standard	vCenter Server Foundation & Standard
vRAM	-	32 GByte	32 GByte	32 GByte	64 GByte	96 GByte
vSMP-Unterstützung	8 Wege	8 Wege	8 Wege	8 Wege	8 Wege	32 Wege
Thin Provisioning	ja	ja	ja	ja	ja	ja
VC Agent		ja	ja	ja	ja	ja
Update Manager		ja	ja	ja	ja	ja
High Availability			ja	ja	ja	ja
Data Recovery			ja	ja	ja	ja
VMotion			ja	ja	ja	ja
Virtual Serial Port Konzentrator					ja	ja
Hot Add HW					ja	ja
vShield Zones					ja	ja
Fault Tolerance					ja	ja
vStorage APIs					ja	ja
Storage VMotion					ja	ja
DRS + DPM					ja	ja
vNetwork Distributed Switch						ja
Host Profiles						ja
Auto Deploy						ja
Storage DRS + Profile						ja

Um eine Übersicht über die Preisunterschiede zu bekommen, können Sie sich auf der VMware-Webseite die Kaufoptionen ansehen. Häufig bekommt man aber bei Distributoren günstigere Preise. Auch gibt es für bestimmte Organisationen preiswertere Angebote, zum Beispiel für Akademien und Schulen.

Neu bei der Lizenzierung in der Version 5 ist der vRAM, also der Arbeitsspeicher, den die laufenden VMs bekommen haben. Dazu ein Beispiel: Wenn Sie sich für die Version Essentials Plus entscheiden, kaufen Sie insgesamt sechs Lizenzen für die Prozessoren und einen vCenter Server (alles im Bundle enthalten). Pro Lizenz können Sie 32 GByte an die VMs verteilen, das macht also $6 * 32 = 192$ GByte RAM. Dabei wird eine ausgeschaltete Maschine nicht berücksichtigt. Laufen bei Ihnen manchmal mehr und manchmal weniger VMs, wird ein Mittelmaß über ein Jahr zugrunde gelegt. Dabei ist es egal, wie viel RAM Ihr Host tatsächlich hat.

Der Arbeitsspeicher der VM wird nur bis zu einem maximalen Wert von 96 GByte gezählt, alles darüber zählt nicht.

Häufig werden auch vSphere Acceleration Kits angeboten. Diese gibt es dann üblicherweise in fünf verschiedenen Ausbaustufen, wie die nachstehende Tabelle 2-2 zeigt.

Tabelle 2-2: VMware vSphere Acceleration Kits mit zugehörigen Funktionen

	Essentials	Essentials Plus	Standard	Enterprise	Enterprise Plus
CPU-Lizenzen	6	6	8	6	6
vRAM	32 GByte, max. 192 GByte	32 GByte, max. 192 GByte	32 GByte, max. 256 GByte	64 GByte, max. 384 GByte	96 GByte, max. 576 GByte
vSMP-Unterstützung	8 Wege	8 Wege	8 Wege	8 Wege	32 Wege
Thin Provisioning	ja	ja	ja	ja	ja
VC Agent	ja	ja	ja	ja	ja
Update Manager	ja	ja	ja	ja	ja
High Availability		ja	ja	ja	ja
Data Recovery		ja	ja	ja	ja
VMotion		ja	ja	ja	ja
Virtual Server Port Konzentrador				ja	ja
Hot Add HW				ja	ja
vShield Zones				ja	ja
Fault Tolerance				ja	ja
vStorage APIs				ja	ja
Storage VMotion				ja	ja
DRS + DPM				ja	ja
vNetwork Distributed Switch					ja
Host Profiles					ja
Auto Deploy					ja
Storage DRS + Profile					ja

Dafür, für welche Umgebung welche Edition sinnvoll oder angebracht ist, gibt es keine Faustregel. Als Beispiel sei hier Fault Tolerance angesprochen: Gespiegelte virtuelle Maschinen auf unterschiedlichen ESXi-Servern laufen zu lassen, um eine fast 100%ige Ausfallsicherheit zu bekommen, ist schon verlockend. Wenn Sie sich aber die aufgeführten 23 Einschränkungen in Kapitel 10 und die dort aufgeführten unterstützten Betriebssysteme ansehen, wird schnell deutlich, dass man diese Ausfallsicherheit wohl nur selten erreicht. Als größtes Manko sehe ich an, dass nur Ein-Prozessor-Maschinen unterstützt werden. Die wichtigen Rechner, die möglichst immer zur Verfügung stehen sollen und von vielen Usern genutzt werden, haben meist deutlich mehr CPUs nötig.

Überlegen Sie sich, welche Ihrer Server Sie virtualisieren wollen, und machen Sie sich eine Liste. Nehmen Sie dann die Liste zur Hand und überprüfen jeden Server z.B. nach der gewünschten Verfügbarkeit. Wenn Sie zu dem Ergebnis kommen, dass es nicht schlimm wäre, wenn Ihre Server mal für ein paar Minuten nicht laufen, brauchen Sie keine Fault Tolerance. Wenn Sie die Auslastung der ESXi-Server gut im Blick haben, brauchen Sie kein DRS. Wenn eine Trennung der LAN-Verbindung von maximal einer Sekunde nicht schlimm ist, brauchen Sie keinen Distributed Switch, usw.

Bevor Sie sich entscheiden, eine der oben genannten Versionen anzuschaffen, sollten Sie sich in diesem Buch zunächst eine detaillierte Übersicht über die Funktionen verschaffen, die oben erwähnte Liste zur Hand nehmen und erst dann die für Sie richtige Edition wählen.

Der Hypervisor

Die erste Komponente, die man für eine virtuelle Umgebung braucht, ist der Host. In früheren Versionen – bis einschließlich vSphere 4.1 – gab es für diesen Server zwei unterschiedliche Ansätze: Eine Version mit einem stark abgespeckten RedHat-Linux-Betriebssystem (ESX) und eine Version ohne Betriebssystem (ESXi). In der aktuellen Ausgabe gibt es nur noch den ESXi, der nunmehr auf der Internetseite von VMware generell als »Hypervisor« bezeichnet wird, aber auf fast allen Bildschirmen und in den meisten Dokumentationen weiterhin als »ESXi« oder schlicht »Host« auftaucht.

Die physikalische Hardware des Hosts, auf der letztendlich die virtuelle Maschine laufen soll, muss diverse Voraussetzungen mitbringen, die bei den verschiedenen Virtualisierungslösungen sehr unterschiedlich sein können. VMware bietet dafür eine Webseite, auf der man die Kompatibilität vorhandener und/oder noch zu beschaffender Komplettsysteme mit einzelnen Geräten überprüfen kann, und zwar unter <http://www.vmware.com/resources/compatibility/search.php>. Bestenfalls unterstützt die Hardware beide Versionen des Hypervisor:

- ESXi 5.0 Installable
- ESXi 5.0 Embedded

Da VMware in unregelmäßigen Abständen Updates für den ESXi-Server herausbringt, kann in der Liste auch die Kompatibilität mit der jeweiligen Neuerung vermerkt sein, also z.B. »ESXi 5.0 U1« (kompatibel auch mit dieser oder erst ab dieser Version).

Die weiteren Angaben, die man auf der Internetseite in die dargestellte Maske eingeben kann, beziehen sich auf spezielle Funktionen wie EVC (Enhanced VMotion Compatibility) und FT (Fault Tolerance). Die Auswahl beruht auf dem oder den jeweils verbauten Prozessor(en), wozu Sie in Kapitel 10 mehr erfahren.

Der Begriff »ESX(i)« ist übrigens ein Name und keine Abkürzung, auch wenn im Internet teilweise etwas anderes behauptet wird.

Embedded oder Installable

Die Hypervisor-Versionen mit dem »i«, also *Embedded* und *Installable*, haben kleine Unterschiede, die in der Dokumentation von VMware aber nicht beschrieben werden. So ist es bei der zu installierenden Version zwar möglich, auf die Kommandozeile zu kommen und dort ein paar Befehle einzugeben, aber man wird wohl eher wie bei der Embedded-Variante das *vSphere Command Line Interface* (vCLI) oder PowerCLI dafür nutzen, das Sie sich bei Bedarf bei VMware oder von der Website zu diesem Buch herunterladen können. Das CLI kann man auf einem Linux- oder Windows-Rechner installieren und so Befehle an den ESXi-Server senden – fast so, als säße man direkt an der Konsole des Servers.

Beide Varianten (ESXi embedded und ESXi installable) sind sogenannte *Bare-Metal-Hypervisoren*, die direkt auf der Serverhardware installiert werden bzw. bereits im Server stecken, meist als Stick auf dem Motherboard. Damit ist das Ressourcenmanagement für die virtuelle Maschine mit seinen vier Kernkomponenten (»Four-Core«: CPU, RAM, Storage und Netzwerk) rein als virtuelle Schicht anzusehen.

Da der ESXi kein Betriebssystem hat, bietet er auch weniger Angriffsmöglichkeiten z.B. für Viren, Trojaner und Ähnliches.



Der ESXi Installable kann auch als kostenlose Version eingesetzt werden und hat die gleichen Hardwareanforderungen wie die andere Variante. Dort gibt es eine kleine, abgespeckte Konsole (die Busybox), mit der man diesen Server mit ein wenig Know-how zum Teil auch von der Kommandozeile aus bedienen kann. Nach der Installation auf einer Festplatte (siehe unten) können dort ähnlich wie beim ehemaligen ESX-Server Befehle eingegeben werden. Dazu später mehr in Kapitel 9.

Obwohl VMware nur noch den ESXi als vSphere Hypervisor anbietet, wird der Support der alten ESX-Version (bis 4.1) aber weitergehen.

Hier eine kurze Übersicht über die Besonderheiten beim ESXi-Server:

- Die Konfiguration erfolgt am Server über eine Umgebung, die an ein BIOS erinnert. Agenten können nur über einen CIM-Provider installiert werden. Die Konfiguration ist lediglich über die grafische Oberfläche oder das Remote CLI (Command Line Interface) möglich.
- Das Remote-Command-Line-Interface kann auf einem Linux- oder Windows-PC oder als virtuelle Maschine installiert werden. Dabei handelt es sich meist um Pearl-Skripten, die eine Verbindung zum ESXi-Host aufnehmen.
- vSphere CLI hat bei der kostenlosen Version nur Lese-, aber keine Schreibberechtigungen.
- Die Installation über KickStart-Skripten (z.B. USB oder CD) ist möglich.

- Booten über SAN wird bei ESXi jetzt auch unterstützt, die Embedded-Version wird nicht installiert und bootet vom Stick.
- SNMP wird nur im lizenzierten Modus unterstützt.
- Im lizenzierten Modus sind Active Directory Integration und Beitritt zur Domäne über GUI und CLI möglich (Einträge im DNS werden dabei nicht gemacht).
- Agenten können nur über einen CIM-Provider installiert werden, ein Teil ist gegebenenfalls vorinstalliert. Es gibt angepasste ESXi-Versionen von diversen Herstellern wie IBM, Fujitsu, HP etc.
- Software-Patches und -Updates verhalten sich wie Firmware-Updates und -Patches. Neue Aktualisierungen beinhalten alle alten.
- VI WebAccess wird auf ESXi nicht unterstützt.
- Der ESXi-Server kann als Teil einer Infrastruktur lizenziert werden, aber auch als Stand-alone eingesetzt werden.
- Der ESXi Embedded wird üblicherweise zusammen mit der Serverhardware ausgeliefert. Einige Hersteller tun dies bereits seit einiger Zeit, darunter Dell, IBM und HP sowie NEC und Fujitsu.

ESXi-Hardwareanforderungen

Zur Verwendung von ESXi sind bestimmte Hardware- und Systemressourcen erforderlich. Hier werde ich nur die wichtigsten bzw. gebräuchlichsten aufzählen. Für eine Gesamtübersicht ziehen Sie bitte die Internetseite von VMware zurate; gerade wenn es neue Updates zu diesem Produkt gibt, könnten auch andere Geräte unterstützt werden. Wenn Sie bereits eine Serverhardware besitzen, können Sie die Kompatibilität mit der Version 5.0 unter www.vmware.com/resources/compatibility nachschlagen.

64-Bit-Prozessor

Der Hypervisor kann nur auf Hardware mit x86-CPU's im 64-Bit-Modus installiert und ausgeführt werden und benötigt mindestens zwei Kerne.

Zu den geeigneten Prozessoren gehören

- alle AMD Opteron-Prozessoren und
- alle Intel Xeon-Prozessoren der Serien 30xx – 33xx, 51xx – 56xx und 71xx – 75xx.

RAM

mindestens 2 GByte RAM

Netzwerkadapter

Ein oder mehrere Ein- oder Zehn-Gigabit-Netzwerkadapter. Die unterstützten Netzwerkadapter umfassen u.a.

- Broadcom NetXtreme 570x Gigabit-Controller und
- Intel PRO 1000-Adapter.

SCSI-Adapter, Fibre-Channel-Adapter oder interner RAID-Controller

Einer oder mehrere der folgenden Controller (alle Kombinationen möglich):

- Die SCSI-Basis-Controller sind Adaptec Ultra-160 und Ultra-320, LSI Logic Fusion-MPT und die meisten NCR/Symbios SCSI-Controller.
- Fibre-Channel, siehe Hardware-Kompatibilitätshandbuch unter <http://www.vmware.com/resources/compatibility>. Dort stehen aktuell 1001 Adapter in der Liste.
- Zu den unterstützten RAID-Adaptoren zählen HP Smart Array, Dell Perc (Adaptec RAID und LSI Mega-RAID) sowie IBM (Adaptec) ServeRAID-Controller.

Installation und Speicherung

Eine SATA- oder SCSI-Festplatte, Fibre-Channel-LUN oder RAID-LUN mit nicht partitioniertem, mindestens 5 GByte großem Bereich gelten als Mindestvoraussetzung für die Installation. In diesem Laufwerk oder RAID-Verbund werden die Dateien für den Hypervisor und gegebenenfalls später die Dateien der virtuellen Maschinen abgelegt. Software-iSCSI über eine normale Netzwerkkarte wird zum Starten oder Installieren von ESXi nicht unterstützt. Nach der Installation kann man dieses aber sehr wohl für die VMs benutzen.

- Unter anderem können die folgenden Festplatten verwendet werden:
- Hardware-iSCSI – eine mit einem iSCSI-Controller verbundene Festplatte, z.B. QLogic qla405x
- Serial Attached SCSI (SAS)
- Serial ATA (SATA) – eine über unterstützte SAS-Controller oder unterstützte On-Board-SATA-Controller verbundene Festplatte

Zu den unterstützten SAS-Controllern gehören folgende:

- LSI1068E (LSISAS3442E)
- LSI1068 (SAS 5)
- IBM ServeRAID 8K SAS-Controller
- Smart Array P400/256-Controller
- Dell PERC 5.0.1-Controller

Zu den unterstützten On-Board-SATA-Controllern gehören die hier:

- Intel ICH9
- Nvidia MCP55
- ServerWorks HT1000

Wenn Sie ESXi auf SATA-Laufwerken installieren wollen, beachten Sie bitte Folgendes:

- Es können nur unterstützte SAS-Controller oder unterstützte On-Board-SATA-Controller verwendet werden.
- Verwenden Sie keine SATA-Festplatten zum Erstellen von VMFS-Datenspeichern, die über mehrere ESXi-Hosts verteilt sind.

- Unterstützte USB-Geräte für die Installation finden Sie ebenfalls online.
- ATA- und IDE-Festplattenlaufwerke – ESXi unterstützt das Installieren und Starten auf einem ATA-Laufwerk oder ATA RAID. Vergewissern Sie sich jedoch, dass Ihr Controller ebenfalls unterstützt wird. IDE-Laufwerke werden für die ESXi-Installation und die VMFS-Erstellung nicht empfohlen.



Beachten Sie für den produktiven Einsatz Ihres ESXi-Servers, dass es spezielle SATA-Laufwerke gibt, die mit »24/7« als für den Dauerbetrieb ausgelegt gekennzeichnet sind, was für handelsübliche SATA-Platten nicht zutrifft.

Sie können sowohl ein normales BIOS als auch ein UEFI-System benutzen. Beachten Sie aber, dass bei einer Änderung nach der Installation das System nicht mehr booten kann.

ESXi 5.0 verwendet das GUID-Partitionstabellenformat (GPT), das Boot-Laufwerke über 2 TByte erlaubt. Es wird nur die erste Festplatte während der Installation formatiert.

ESXi-Hardwareempfehlungen

Vor der Installation des Hypervisor sollten Sie noch einige wichtige Punkte beachten:

- Nehmen Sie für die Installation eine kleine Festplatte, um darauf das Boot-Image zu speichern (mindestens 5 GByte). Nehmen Sie für das VMFS Storage nach der Installation eine weitere große Festplatte, um dort die VMs abzulegen. Aus Performancegründen sollten Sie nicht eine einzige Platte für beides verwenden. Fügen Sie die große Festplatte sicherheitshalber erst nach der Installation hinzu und erstellen Sie eine VMFS-Partition über den vSphere Client – nur so ist sichergestellt, dass ein automatisches Alignment an der 64-K-Grenze gemacht wird. Beachten Sie zum Punkt Alignment auch Kapitel 7, *Storage-Konfiguration*!
- Die CPU-Auslastung ist bei den meisten Systemen eher gering, wichtig ist dabei aber der Prozessorcache. Der Arbeitsspeicher wird dagegen sehr intensiv genutzt. Hier ist mehr gleich besser.
- Sie sollten mindestens zwei separate Ethernet-Adapter für das Management Network und die virtuellen Maschinen haben. Auch hier ist mehr besser – je nachdem, wie viele VMs und sonstige Dienste (wie iSCSI, NFS, vMotion und FT) Sie nutzen wollen. Beachten Sie auch die Hinweise in Kapitel 6, *Netzwerkkonfiguration*.

ESXi interaktiv installieren

Die Installation des ersten VMware-ESXi-Servers wird üblicherweise komplett manuell durchgeführt. Eine automatisierte Installationsroutine kann hinterher implementiert werden (siehe dazu den Abschnitt »Weiteren ESXi-Server über ein Skript installieren« auf Seite 32).

Vor der Installation des ESXi-Servers sollten Sie – vorausgesetzt, Sie wollen nicht vom SAN booten – alle vorhandenen FibreChannel-Anschlüsse und iSCSI-Storages abziehen bzw. trennen, damit Sie nicht durch die womöglich vorhandenen LUNs (Logical Unit Numbers, also Volumes) unnötig durcheinanderkommen. Des Weiteren sollten Sie sich noch vergewissern, dass keine Hardware vorhanden ist, die vom ESXi-Server nicht unterstützt wird. Da es für manche zertifizierte Serverhardware, die Sie auf der oben genannten Webseite bei VMware finden, wichtige Informationen bei der Installation zu beachten gibt, ist ein Besuch dieser Webseite vorher ratsam. Ein weiterer wichtiger Punkt sind die Netzwerkkarten: Mindestens eine ist Pflicht, und bei der Verwendung von vMotion werden sogar drei empfohlen.

ESXi installieren – Schritt für Schritt

Die Installation des VMware Hypervisor kann von einer CD/DVD oder einem vorher vorbereiteten USB-Stick erfolgen. Die Embedded-Version ist schon auf einem Stick auf dem Motherboard und muss nicht nochmals installiert werden. Im Gegenteil: Auf einem Embedded-ESXi *darf* die Installable-Version nicht zusätzlich installiert werden. Eine Installation über die Netzwerkkarte (PXE, Preboot Execution Environment) ist ebenfalls möglich. Stecken Sie den optischen Datenträger in das Laufwerk des Hostsystems ein oder booten Sie ihn vom Stick.

Gehen Sie im Detail folgendermaßen vor:

1. Stellen Sie im BIOS ein, dass der Server von der CD/DVD oder dem Stick gestartet wird. Überprüfen Sie, ob der Virtualisierungsmodus Intel-VT bzw. AMD-V und gegebenenfalls Hyperthreading aktiviert sind. Achten Sie auf die Uhrzeit und das Datum des Systems.
 - a. Starten Sie den Computer neu.
 - b. Drücken Sie die entsprechende Taste, um das BIOS-Setup oder das Startmenü Ihres Computers zu öffnen. Oft ist das eine Funktionstaste (F2, F9 o. Ä.) oder die Entfernen-Taste.
 - c. Legen Sie das CD-/DVD-Laufwerk oder den USB-Stick als erstes Startgerät fest.
 - d. Speichern Sie die Änderungen und verlassen Sie das BIOS.
2. Wenn Sie keine der beiden Möglichkeiten (installieren oder von Festplatte booten) auswählen oder die Enter-Taste betätigen, startet die Installation automatisch nach sieben Sekunden. Ein Laufbalken am oberen Bildschirmrand zeigt den Ladevorgang an.

Es werden erst diverse Installationsmeldungen auf dem Bildschirm angezeigt, bevor die Begrüßungsseite erscheint.
3. Betätigen Sie zum Fortfahren die Taste Enter bzw. Return.
4. Wählen Sie ICH AKZEPTIERE DIE BEDINGUNGEN DER LIZENZVEREINBARUNG, indem Sie die Taste F11 drücken.

Sie können das Produkt nur installieren, wenn Sie der Lizenzvereinbarung zugestimmt haben.

Die Einrichtung der Lizenzinformationen für den Hypervisor erfolgt später. Neu angelegte oder bereits vorhandene virtuelle Maschinen lassen sich bis zur korrekten Eingabe der ESXi-Serverlizenz nicht starten, wenn der Evaluierungsmodus nach 60 Tagen beendet ist. Falls Sie über eine zeitlich begrenzte Lizenz verfügen, werden die virtuellen Maschinen nach Ablauf des gesetzten Zeitraums in den Suspend-Modus geschaltet und können erst nach Eingabe einer gültigen Lizenz wieder gestartet werden.

5. Wählen Sie einen Datenträger aus der Liste und drücken Sie ggf. F1 für weitere Details. Drücken Sie anschließend Enter, um in das nächste Fenster zu gelangen.



Sollte sich auf dem Datenträger eine frühere Installation eines ESXi-Servers befinden, können Sie diesen mit allen Informationen und Einstellungen sowie VMs aktualisieren. Sind andere Daten vorhanden, werden Sie aufgefordert, das Löschen zu bestätigen.

6. Mit den Pfeiltasten können Sie das gewünschte Tastaturlayout auswählen, mit der Bild-hoch-Taste kommen Sie an den Anfang der Liste. Drücken Sie anschließend Enter, um in das nächste Fenster zu gelangen. Das Tastaturlayout kann auch noch nach der Installation geändert werden (passen Sie dann aber bei der Passwordeingabe auf!).
7. Geben Sie zweimal hintereinander ein Passwort mit mindestens sechs Zeichen ein. Es muss nicht, wie bei der Vorgängerversion, komplex sein und darf auch leer sein. Drücken Sie danach Enter.

Das System wird nun ein weiteres Mal nach Geräten und Inkompatibilitäten durchsucht. Sollte ein nicht unterstütztes Gerät gefunden werden oder ein wichtiges Gerät fehlen, wird eine Fehler- oder Warnmeldung angezeigt. Überlegen Sie sich dann, ob Sie diese Meldung für einen produktiven Einsatz ignorieren oder nochmals auf der Webseite von VMware nach kompatibler Hardware Ausschau halten wollen.

8. Nun wird es ernst: Wenn Sie im Fenster CONFIRM INSTALL die Taste F11 drücken, wird die eigentliche Installation gestartet.



Das Installationsprogramm löscht ggf. den gesamten Inhalt des ausgewählten Speichergeräts.

Drücken Sie F11, um die Installation zu starten.

9. Wenn der Laufbalken mit den Prozentangaben bei 100 angelangt ist, werden Sie in einem neuen Fenster (hoffentlich) darauf hingewiesen, dass die Installation SUCCESSFULLY verlaufen ist, wie Abbildung 3-1 zeigt.



Abbildung 3-1: Abschluss der erfolgreichen Installation

10. Nehmen Sie die CD/DVD aus dem Laufwerk oder den USB-Stick aus dem Server und bestätigen Sie mit Enter den Neustart des Systems.
11. Stellen Sie bei Bedarf die Bootreihenfolge wieder um.

Ist der Server wieder hochgefahren, können Sie am Bildschirm die erste Konfiguration vornehmen.

Erste Konfiguration des ESXi-Servers

Sollte in Ihrer Umgebung ein DHCP-Server installiert sein, wird der ESXi-Server wohl von diesem IP-Adressinformationen zugewiesen bekommen. Wenn nicht, wird er sich nach einiger Zeit eine APIPA-Adresse (*Automatic Private IP Address*) aus dem Bereich 169.254.x.y mit der Subnetzmaske 255.255.0.0 nehmen. Beachten Sie, dass damit kein ausgehender Datenverkehr möglich ist. Hat er aber über DHCP eine Adresse bekommen, können Sie die nächsten Schritte auch über den vSphere Client erledigen.

Über die Funktionstaste F12 können Sie, ähnlich wie bei einem BIOS, einige Einstellungen vornehmen, die in den folgenden Abschnitten näher beleuchtet werden. Dafür habe ich die einzelnen Einträge in der Originalsprache als Überschrift gewählt.

Configure Password

Ein Passwort ist zwar nicht unbedingt notwendig, sollte aber gesetzt werden. Hier ist im Gegensatz zur Vorgängerversion kein komplexes Passwort für den User *root* mehr notwendig, wohl aber für alle anderen Benutzer, die Sie nachträglich anlegen. Sie können aber trotzdem für *root* eines wählen, das aus kleinen und großen Buchstaben, Zahlen und Sonderzeichen besteht. Beachten Sie bitte, dass die Tastatur ggf. noch nicht auf das deutsche Tastaturlayout eingestellt ist. Ist Ihr gewähltes Passwort zu kurz oder stimmen Ihre zwei Eingabeversuche nicht überein, bekommen Sie eine Fehlermeldung. Ist es einmal

gesetzt, kommen Sie in diese Konfigurationsseite nur noch mit dem gewählten Passwort. Haben Sie während der Installation schon eines vergeben, können Sie diesen Schritt überspringen.

Die Einstellungen für das notwendige Passwort befinden sich in der Datei *passwd* im Verzeichnis */etc/pam.d*. In der dritten Zeile steht am Ende u.a. der Eintrag `min=8,8,8,7,6`. Dabei bedeutet der erste Eintrag die Minimallänge des Passworts, wenn nur eine Zeichenart verwendet wird. Die zweite Zahl ist die minimale Länge bei Verwendung von zwei der Möglichkeiten, wobei der erste Großbuchstabe nicht zählt (Passwort weist also nur eine Zeichenart auf, Passwort zwei). Der dritte Wert gibt die Minimallänge einer Passphrase aus mindestens drei Wörtern an; der vierte und der fünfte Eintrag beschreiben die Mindestlänge bei drei bzw. vier verwendeten Zeichencodes. Die angegebenen fünf Werte müssen absteigend oder gleich sein.

Um die Passwortlänge zu reduzieren, kann man also z.B. den Eintrag auf `min=6,6,6,6,6` ändern. Zum Ausschalten der Komplexität können Sie zusätzlich noch den Eintrag `enforce=none` anhängen. Die Änderungen können mit dem Editor *vi* vorgenommen werden. Ein anderer Editor wird auf der i-Version nicht angeboten.

Vorgehensweise:

1. Um sich auf der Konsole anmelden zu können, müssen Sie zunächst bei der Konfiguration die »Troubleshooting Mode Options« ändern. Wollen Sie sich direkt am ESXi-Server anmelden, wählen Sie mit den Pfeiltasten den Eintrag `ENABLE ESXi SHELL` aus und drücken Sie Return.
2. Drücken Sie die Tastenkombination `Alt+F1`, um auf die erste Konsole zu kommen.
3. Geben Sie das Passwort des Users *root* ein und drücken Sie erneut die Enter-Taste.
4. Da es hier nur den Editor *vi* gibt, geben Sie an der Position, an der Sie sich befinden, `vi /etc/pam.d/passwd` ein und drücken Sie Enter.
5. Gehen Sie mit den Pfeiltasten in die dritte Zeile und dann nach rechts, bis Sie den Eintrag `... retry=3 min= ...` sehen. Drücken Sie `Einf`g und ändern oder ergänzen Sie den Eintrag wie oben beschrieben ab.
6. Drücken Sie `Esc` und anschließend `:wq` zum Speichern und Verlassen des Editors.
7. Sie brauchen weiter nichts zu veranlassen, denn diese Änderung wirkt bei der nächsten Anmeldung auf der Konsole sofort.

Configure Lockdown Mode

Den Sperrmodus können Sie nur über den vSphere Client auf dem vCenter Server aktivieren. Wenn Sie das tun, kann der Benutzer *root* nicht mehr mit dem vSphere Client oder der Remote CLI (*Command Line Interface*) auf den Server zugreifen. Das geht dann nur noch lokal oder auch über *ssh*, falls dieses eingestellt wurde (siehe weiter unten bei »Troubleshooting Options« auf Seite 29). Das Aktivieren dieses Befehls kann auch

andere Software beeinflussen, z.B. Managementtools. Der vCenter Server greift über den *vpxuser* auf den Host zu, nicht über *root*.

Configure Management Network

Im nun folgenden Untermenü können Sie

- sich die Netzwerkadapter mit ihrem Verbindungsstatus ansehen,
- ein VLAN einrichten (besser über die grafische Oberfläche mit dem vSphere Client),
- unter IP CONFIGURATION zwischen DHCP und statischer IP-Adresse wechseln und IP-Adresse, Subnetzmaske und Default-Gateway eingeben,
- IPv6 aktivieren und konfigurieren, was allerdings einen Neustart erfordert,
- den ersten und gegebenenfalls zweiten DNS-Server sowie einen Namen für den Host eingeben
- und ein weiteres DNS-Suffix angeben.

Restart Management Network

Wie der Name schon sagt, können Sie hier das Management-Netzwerk neu starten. Das kann notwendig sein, wenn man eine neue IP-Adresse vom DHCP-Server haben möchte, eine IP im Netzwerk aus Versehen doppelt vergeben war oder der Remote-Zugriff unterbrochen war. Die Netzwerkeinstellungen werden dann aus den Konfigurationsdateien neu gelesen und die zugehörigen Dienste neu gestartet.

Dabei wird die Verbindung über den vSphere Client oder den vCenter Server unterbrochen und es kann passieren, dass die gerade laufenden virtuellen Maschinen kurzfristig ebenfalls keine Netzwerkverbindung haben.

Bekommt der Host dabei durch DHCP eine neue Identität, müssen Sie sich ggf. am vSphere Client neu anmelden oder den Host über den vCenter Server neu verbinden.

Test Management Network

Um die gemachten Einstellungen zum Standard-Gateway und zum ersten und gegebenenfalls zweiten DNS-Server sowie die Auflösung des Hostnamens zu überprüfen, können Sie diesen Schritt ausführen. Die Adressen, an die ein ping-Signal (ICMP-Paket) geschickt wird, werden vorher nochmals aufgelistet.

Restore Network Settings

Um die Netzwerkeinstellungen zurückzusetzen, kann dieser Punkt ausgewählt werden. Beachten Sie, dass eventuell laufende VMs dabei gestoppt werden und wieder die kompletten Standardeinstellungen (z.B. DHCP, wie direkt nach der Installation des Hosts) genommen werden.

Restore Standard Switch

Dieser Menüpunkt ist nur auswählbar, wenn Sie einen Distributed Virtual Switch über den vCenter Server erstellt haben. Benötigen Sie diesen nicht mehr, können Sie an dieser Stelle den Standardswitch wiederherstellen. Dabei wird der nicht mehr benötigte Netzwerkadapter an diesen Switch gebunden.

Über eine weitere Netzwerkkarte können Sie aber auch mit dem vSphere Client eine neue Verbindung zum Management Network herstellen und dann über die grafische Oberfläche diese Arbeiten durchführen.

Configure Keyboard

Hier lässt sich das Tastaturlayout auf insgesamt 28 verschiedene Einstellungen ändern. Der Eintrag US DEFAULT stellt übrigens die amerikanische Tastatur ein, wogegen es auch die Einstellung UNITED KINGDOM gibt. Suchen Sie sich Ihr Layout aus, aktivieren Sie es mit der Leertaste und bestätigen Sie die Änderung mit Enter.

Troubleshooting Options

Dahinter verbergen sich vier weitere wichtige Optionen, die man bei Bedarf ändern kann. Zwei der Einträge ändern sich, je nachdem, ob sie aktiv sind oder nicht.

Enable / Disable ESXi Shell

Wenn Sie sich über die Kommandozeile der Busybox anmelden wollen, müssen Sie auf diesem Eintrag die Enter-Taste betätigen. Dann ändert sich der Text von ENABLE ESXi SHELL auf DISABLE ESXi SHELL. Wenn dort DISABLE ESXi SHELL steht, wurde also die Shell aktiviert und Sie können sich mit Alt+F1 dort anmelden. Ist die Shell aktiviert, bekommen sie über den vSphere Client nach der Anmeldung einen Hinweis im gelben Kasten darüber auf der ersten Registerkarte ÜBERSICHT.

Enable / Disable SSH

Um sich über das Netzwerk mit einer Remote Secure Shell (wie *putty* oder *WinSCP*) anmelden zu können, muss diese Option aktiviert sein. Achten Sie darauf, dass im rechten Teil des Fensters nach drücken der Enter-Taste der Text auf SSH IS ENABLED wechselt. Auch diese Aktivierung wird über die grafische Oberfläche in einem gelben Balken angezeigt, da sie ggf. einen nicht autorisierten Zugriff ermöglicht.

Modify ESXi Shell timeout

Der Standardwert nach der Installation ist hier auf 0 gesetzt, es gibt also keinen Timeout für die Arbeiten in der Busybox. Sie können hier bis zu 1440 Minuten für den Remote- und lokalen Shellzugriff festlegen. Nach Ablauf der Zeit wird der angemeldete User ausgeloggt.

Restart Management Agent

Diesen Menüpunkt dürfen Sie nicht mit RESTART MANAGEMENT NETWORK (siehe oben) verwechseln. Diese Agenten sind für die Verbindung vom vSphere Client oder dem vCenter Server zuständig und werden bei der Installation des Hosts bereits installiert und ggf. aktiviert. Wenn der Zugriff auf den ESXi-Server nicht mehr möglich ist, können Sie über den Neustart der Agenten versuchen, die Verbindung zurückzusetzen. Dabei werden alle Agenten und Dienste, die im Ordner */etc/init.d* auf dem Host aufgelistet sind, neu gestartet. Üblicherweise handelt es sich um folgende Dämonen, die meist an dem »d« am Ende des Namens zu erkennen sind: *hostd*, *ntpd*, *sfcdbd*, *slpd*, *vobd* und *wsman*.

Dabei wird die Verbindung über den vSphere Client oder auch den vCenter Server unterbrochen und es kann passieren, dass die gerade laufenden virtuellen Maschinen kurzfristig ebenfalls keine Netzwerkverbindung haben.

Das Neustarten der Management-Agenten (ein Agent oder Daemon ist vergleichbar mit Diensten auf einem Windows-Rechner) ist normalerweise nicht notwendig. Es kann aber sein, dass auf der grafischen Oberfläche einmal etwas nicht aktualisiert oder aus einem anderen Grund falsch angezeigt wird. Nach dem Neuankommen mit dem vSphere Client ist das Problem dann meist nicht behoben. Nach einem Neustart der Management-Agenten müsste aber alles wieder richtig und aktuell angezeigt werden.

View System Logs

Insgesamt sechs Logdateien werden zur Ansicht angeboten: *syslog*, *vmkernel*, *config*, *Managemnet Agent hostd*, *VirtualCenter Agent vpxa* und *VMware ESXi Observation log vobd*. Wenn Sie eine der Logdateien ausgewählt haben, wird das unter Linux bekannte Programm *less* für die Ansicht genutzt. Sie können sich mithilfe der Pfeiltasten und den Tasten Bild hoch bzw. Bild herunter die Texte ansehen und mit Q die Ansicht verlassen. Über die Taste H bekommen Sie weitere Tastenkommandos angezeigt, und mit dem Schrägstrich / können Sie in der Logdatei nach Ausdrücken suchen. Sollten Sie später mal Probleme oder lange Wartezeiten beim Server haben, nehmen Sie sich diese Logdateien als Erstes vor, um nach Lösungen zu suchen.

Eine grobe Übersicht über das Verhalten des Servers bekommen Sie auch auf der 12. Konsole. Mit Alt+F12 können Sie sich die letzten Zeilen der *vmkernel*-Logdatei ansehen. Läuft die Anzeige sehr schnell weiter und zeigt immer den gleichen Eintrag an, hat der ESXi ein Problem – das ist häufig bei fehlenden oder nicht mehr verbundenen Festplatten der Fall (z. B. iSCSI).

View Support Information

Auf diesen beiden Seiten sind Einträge zur Lizenz, zu SSL, zur Supportwebseite von VMware, zur BIOS-Version und gegebenenfalls noch weitere zu finden. Über die Tasten Bild hoch bzw. Bild herunter kann man sich die Seiten anzeigen lassen.

Reset System Configuration

Mit dem Auslösen dieses Befehls und einem anschließenden Neustart wird der ESXi-Server wieder fast in den Ursprungszustand vor allen Änderungen zurückgesetzt. Auch die schon erstellten virtuellen Maschinen müssen anschließend neu registriert werden, z.B. über den Datastore-Browser. Selbst das Passwort für den User *root* ist wieder auf »leer« gesetzt. Haben Sie sich also verkonfiguriert und bekommen das anschließende Chaos nicht mehr in den Griff, können Sie es damit versuchen. Meistens funktioniert nach dem Neustart wieder alles, und Sie brauchen den Server nicht neu zu installieren.

Alternative Installationsmöglichkeiten

Anstatt von einer CD/DVD zu booten, haben Sie auch die Möglichkeit, einen Medienpool über die Netzwerkkarte per FTP, HTTP/HTTPS oder NFS zu erreichen. Das funktioniert aber bisher nur über IPv4, nicht über IPv6. Stellen Sie dann im BIOS des Servers PXE (Preboot Execution Environment) als Startmedium ein. Bei beiden Installationsmöglichkeiten gibt es entweder einen Assistenten, der Sie wie oben geschildert durch den Vorgang leitet, oder Sie können jeweils eine Kickstart-Datei (*ks.cfg*, siehe unten) dafür verwenden.

Wenn Sie bisher noch nicht mit der Installation eines Rechners über das Netzwerk zu tun hatten, lohnt sich vermutlich auch nicht der Aufwand, den Sie dafür betreiben müssten: Sie brauchen eine Netzwerkstruktur mit DHCP-Server, einen TFTP-Server (Trivial File Transfer Protocol), ein SYSLINUX-Paket zum Starten des Installationsprogramms und eine Netzwerkfreigabe über NFS, HTTP oder FTP.

Manche Remote-Management-Anwendungen können ebenfalls für die Installation des ESXi-Servers genutzt werden. Dazu gehören HP Integrated Lights-Out (iLO), Dell Remote Access Card (DRAC), IBM Management Module (MM) und Remote Supervisor Adapter II (RSA II). Dabei kann auch ein *ks.cfg*-Skript verwendet werden.

Die Dateien für die Installation und das Skript können sich ebenfalls auf einem USB-Laufwerk befinden, von dem aus dann statt CD/DVD oder Netzwerkkarte installiert wird.

Ein Installationsskript erstellen

Wie bereits oben erwähnt, kann man sich eine Textdatei basteln, die die Antworten auf die Fragen bei der Installation automatisch gibt. Das Vorgehen mit so einer Antwortdatei dürfte vielen von Windows oder Linux bekannt sein. Das Besondere bei dieser Datei ist, dass man damit Fragen beantworten kann, die sonst gar nicht gestellt würden. Man hat also mit dem Skript eine Einflussnahme, die man sonst nicht hätte.

Beispiel 3-1 zeigt, wie eine manuell erstellte *ks.cfg*-Datei für den nächsten ESXi-Server aussehen könnte:

Beispiel 3-1

```
# Lizenzvereinbarung akzeptieren
vmaccepteula
# Kennwort von root, z. B. für den "Tech Support"-Modus
rootpw ganzgeheim
# alle vorhandenen Festplattenpartitionen außer VMFS löschen (optional)
clearpart --alldrives
# Festplattenpartitionen inkl. VMFS löschen und erste Festplatte vorbereiten (optional)
clearpart --alldrives --overwritevmfs
# Installationsanweisung: install, upgrade oder installorupgrade
install --firstdisk # oder install usb oder install remote --server=gfu.dom --dir=/nfs/ESXi50
# Tastaturlayout (optional)
keyboardtype German
# entweder Netzwerkeinstellungen mit DHCP für den ersten gefundenen Adapter ...
network --bootproto=dhcp --device=vmnic0
# ... oder Netzwerkeinstellungen statisch für den dritten gefundenen Adapter
network --bootproto=static --device=vmnic2 --ip=192.168.150.12 --gateway=192.168.150.10 --
nameserver=192.168.150.10 --netmask=255.255.255.0 --hostname=esx2.gfu.dom
# gewünschte VMFS-Partition eintragen (nicht nötig und nur auf zusätzlicher Festplatte anwendbar)
part datastore <Datenspeichername> --firstdisk
# nach dem Abschluss der Installation noch weitere Skripten ausführen, %post kann mehrfach
# verwendet werden (optional)
%post --interpreter=[python|busybox]
```

Wenn Sie in Ihrem Netzwerk DHCP nutzen, können Sie das obige Skript auch für mehrere Rechner nehmen und die jeweiligen Parameter wie Name und IP von diesem beziehen.

Auf der letzten Konsole, die Sie mit Alt+F12 erreichen, können Sie die letzten Zeilen der VMkernel-Logdatei ansehen. Es ist immer eine gute Idee, diese wichtige Logdatei im Auge zu behalten!

Weiteren ESXi-Server über ein Skript installieren

Die obige Kickstartdatei kann man leicht modifiziert auch für den dritten und weitere Hosts nehmen. Ein Beispiel dazu habe ich oben schon aufgeführt, Sie können es sich auch von der Website zum Buch herunterladen.

Sie können die Datei *ks.cfg* für Ihre eigene Installation anpassen und verwenden. Wichtig ist, dass Sie den Namen der Datei (*ks.cfg*) beibehalten, damit sie gefunden wird. Alternativ können Sie aber auch einen zusätzlichen Parameter mit der Tastenkombination Shift+O (»Edit boot options«) angeben, z.B. wenn sich die Datei auf einer CD befindet: *ks=CD-ROM:<Pfad zur Datei ks.cfg>*.

In der ebenfalls auf der Webseite zu findenden PDF-Datei *vsphere-esxi-vcenter-server-50-installation-setup-guide.pdf* von VMware wird der Vorgang mit einigen weiteren Parametern auf Englisch beschrieben. Nehmen Sie diese Datei zur Hand, wenn Sie Probleme mit der Skriptinstallation haben oder weitere Parameter angeben möchten.

Wir starten wieder von der CD, drücken die Taste Tab und tragen z. B. folgenden Eintrag ein:

```
mboot.c32 -c boot.cfg ks=usb
```

Nachdem Sie Return gedrückt haben, erscheint Ihre Auswahl hinter dem Wort *weasel*. Bestätigen Sie wiederum mit Return.

Dabei muss die Datei *ks.cfg* im Root-Verzeichnis sein. Sollte beim Starten das USB-Gerät nicht erkannt werden, stecken Sie es in einen anderen Slot. Der Installer schaut nach zehn Sekunden nochmals nach und findet dann (hoffentlich) den USB-Storage. Es spielt keine Rolle, ob sich noch andere Dateien auf dem Stick befinden, nur im Wurzelverzeichnis muss eine Datei namens *kf.cfg* sein. Drücken Sie dann Return.

Wenn alles fertig ist, drücken Sie zum Neustart Enter, nehmen die CD und den Stick wieder heraus und beobachten den Bootvorgang.

Wenn der ESXi-Serverstart vollendet ist, können Sie sich über den vSphere Client mit ihm verbinden. Sie brauchen eine noch offene Sitzung mit dem ersten ESXi-Host dafür nicht zu beenden.

ESXi-Installation mit Skript von USB

Eine nette Möglichkeit, einen oder mehrere ESXi-Server per Skript zu installieren, bietet ein USB-Stick. Dorthin kann man alle benötigten Daten startfähig übertragen und die Datei *ks.cfg* gleich mit draufpacken. Als Tool habe ich *UNetbootin* verwendet, das man sich aus dem Internet von der Seite <http://unetbootin.sourceforge.net> kostenlos herunterladen kann. Damit man keine zusätzlichen Startparameter angeben muss, kann man nach der Übertragung auf den Stick die Datei *boot.cfg* ändern und die eigene *ks.cfg*-Datei dort eintragen. Damit erreicht man eine benutzerdefinierte, vollständig automatisch ablaufende Installation.

In der Datei *boot.cfg* steht eine Zeile, die folgendermaßen aussieht:

```
kernelopt=runweasel
```

Ändern Sie diese Zeile für Ihren USB-Stick wie folgt ab:

```
kernelopt=ks=usb
```

Starten Sie anschließend Ihren Server vom Stick.



Sollte die Installation mit dem Skript nicht funktionieren und Sie bekommen eine Fehlermeldung wie *cannot find kickstart file*, versuchen Sie es nochmals und geben die Datei in Großbuchstaben an: *ks=cdrom:/KS.CFG*.

Über den vCenter Server gibt es noch eine weitere Möglichkeit, die Installation mehrerer ESXi-Hosts automatisiert zu erledigen. Nähere Informationen darüber finden Sie in Kapitel 11.

Den ersten ESXi-Host verwalten

Sie verwalten Hosts mit dem vSphere Client.

Jetzt können Sie sich über die Webseite des Servers weitere Informationen holen, den vSphere Client installieren (notwendig) und von dort aus die restlichen Schritte konfigurieren. Verbinden Sie sich über einen Browser mit Ihrem neuen ESXi-Server, wählen Sie HERUNTERLADEN DES VSPHERE CLIENTS und installieren Sie ihn über das Internet.



Wenn Ihre Ländereinstellung nicht auf Deutsch eingestellt ist, bekommen Sie dementsprechend eine andere Sprache angezeigt.

Statt den vSphere Client über die Webseite des Hosts herunterzuladen, der wiederum auf die VMware-Webseite zeigt, können Sie diesen entweder vorher schon von dort als ausführbare Datei beziehen (*VMware-viclient-all-5.0.0-455964.exe*) oder den Client von der vCenter Server-DVD nehmen, falls Sie sie besitzen.

Hardwareanforderungen für den vSphere Client

Folgende Voraussetzungen müssen hardwareseitig für den vSphere Client erfüllt sein:

- CPU: eine CPU
- Prozessor: 266-MHz- oder schnellerer Intel- oder AMD-Prozessor (500 MHz empfohlen)
- Arbeitsspeicher: 256 MByte RAM
- Netzwerk: Gigabit-Verbindung empfohlen
- Festplattenspeicher: 1 GByte freier Festplattenspeicher für eine Komplettinstallation mit den folgenden Komponenten:
 - Microsoft .NET 3.5 SP1
 - Microsoft Visual J#
 - vSphere Client 5.0
- Sie müssen weiterhin über 400 MByte freien Speicherplatz auf dem Laufwerk mit dem *%temp%*-Verzeichnis verfügen.
- Wenn alle erforderlichen Komponenten installiert sind, werden 300 MByte auf dem Laufwerk mit dem *%temp%*-Verzeichnis und 450 MByte für den vSphere Client 5.0 benötigt.

Softwareanforderungen für den vSphere Client

Stellen Sie sicher, dass der vSphere Client von Ihrem Betriebssystem unterstützt wird. Er benötigt das Microsoft .NET- Framework 3.5 SP1. Wenn dieses Framework nicht auf Ihrem System installiert ist, wird es vom Installationsprogramm des vSphere Clients installiert.

Falls Sie Probleme mit der Installation des vSphere Clients haben, können Sie auch die DVD des vCenter Servers nutzen – das sollte funktionieren. In den Unterverzeichnissen des vCenter-Installationsordners befinden sich auch alle oben erwähnten notwendigen Komponenten wie .NET und Visual J# von Microsoft. In Abbildung 3-2 sehen Sie den Startbildschirm zur Installation des Clients.



Abbildung 3-2: Installation des vSphere Clients

Haben Sie bereits einen älteren Client auf Ihrem Rechner installiert, wird ein neuer Unterordner mit der Version 5.0 erstellt, der nur die notwendigen DLL-Dateien und die länderspezifischen Unterordner enthält.

Akzeptieren Sie den Standardinstallationspeicherort und klicken Sie auf WEITER oder klicken Sie auf ÄNDERN, um einen anderen Speicherort auszuwählen.

Kurze Zeit später (falls Sie Microsoft .NET 3.5 SP1 und Microsoft Visual J# schon installiert hatten, sonst dauert es länger) ist die Installation abgeschlossen, und auf Ihrem Desktop befindet sich ein zusätzliches Icon.



Sollte sich bei Ihrem Computer längere Zeit nichts tun, starten Sie die Installation nicht neu! Schauen Sie erst im Task-Manager nach, ob die Anwendung vielleicht doch noch läuft. Gegebenenfalls brauchen Sie gerade bei der .NET-Installation reichlich Geduld.

Stellen Sie anschließend eine Verbindung zum Host mit dem vSphere Client her, indem Sie die IP-Adresse oder den Namen des ESXi-Servers eingeben. Beachten Sie, dass sich der ESXi-Server nicht selbstständig im DNS einträgt – das müssen Sie manuell tun. Weiterhin sollten Sie vorher – falls noch nicht geschehen – die Reverse-Lookup-Zone im DNS erstellen.

Als Benutzernamen wählen Sie *root* (das ist der Administrator oder Superuser) mit dem Passwort, das Sie bei der Installation gewählt haben (siehe Abbildung 3-3).



Abbildung 3-3: Direkte Anmeldung am ESXi-Host

Bevor eine Verbindung zustande kommt, wird noch eine Sicherheitswarnung für das Zertifikat ausgegeben, die Sie zu diesem Zeitpunkt ignorieren können. Diese Warnung wird angezeigt, weil der vSphere Client ein vom ESXi-Host signiertes Zertifikat erkannt hat (Standardeinstellung). Bei sehr sicheren Umgebungen empfiehlt VMware Zertifikate, die von einem vertrauenswürdigen Drittanbieter generiert werden. Sie können natürlich auch Ihre eigenen Zertifikate generieren und anschließend einspielen.



Sollte die Verbindung nicht klappen, suchen Sie zuerst nach den Einstellungen in Ihrer Firewall (vom Betriebssystem oder der Antivirensoftware). Nähere Informationen über den Grund der nicht erfolgten Verbindung können Sie auch in den Logdateien des vSphere Clients unter `C:\Benutzer\<Name>\AppData\Local\VMware\vpv` finden.

Den vSphere Client konfigurieren

Zum vSphere Client können unter anderem noch einige Parameter eingegeben werden, die die tägliche Arbeit ein bisschen vereinfachen. Das Laufzeitverhalten des Clients kann allerdings nicht lokal, sondern erst nach einer Verbindung eingestellt werden.

Wenn Sie die englische Version bevorzugen, können Sie den Eigenschaften des Icons noch den Parameter `-locale en_us` hinzufügen. Möchten Sie sich eine Verknüpfung mit immer demselben ESXi-Server auf den Desktop legen, funktioniert auch der Parameter `-s <esxi-server-name>` oder `-s <IP-Adresse>`, vorausgesetzt, Sie haben den Server im DNS eingetragen oder Ihre `hosts`-Datei angepasst (bei Windows unter `C:\Windows\System32\drivers\etc\hosts`).

Beispiel: <Pfad>"VpxClient.exe" -locale en_us -s esx1.cssv.de

Auch der Benutzername und das Passwort lassen sich mit `-user root` und `-password uvwxyz` hier voreinstellen. Haben Sie alle Optionen angegeben, brauchen Sie anschließend nicht einmal mehr auf VERBINDEN zu klicken. Sie sollten das Passwort allerdings aus Sicherheitsgründen möglichst nicht mit angeben.

Bei den Parametern ist jeweils auch die Kurzform möglich, also statt `-user` nur `-u` oder statt `-password` nur `-p`. Nur bei der Sprache funktioniert `-l` nicht. Haben Sie ein Betriebssystem mit einer anderen Sprache als Deutsch installiert und möchten lieber Ihre Muttersprache angezeigt bekommen, dann geben Sie hinter `-locale` `de_de` an.

Der vSphere Client unter Windows 7

Sollte der vSphere Client unter Microsoft Windows 7 vor allem im Vollbildschirm sehr träge wirken, liegt das an der Einstellung der Aero-Umgebung. Mit den folgenden Einstellungen wird die CPU- und Grafikkartenbelastung deutlich reduziert, aber auch die Aero-Umgebung zur Laufzeit des Clients komplett abgeschaltet:

1. Schließen Sie ggf. alle Fenster des vSphere Clients.
2. Klicken Sie mit der rechten Maustaste auf das Symbol des vSphere Clients und wählen Sie aus dem Kontextmenü **EIGENSCHAFTEN**.
3. Wählen Sie die Registerkarte **KOMPATIBILITÄT** und setzen Sie das Häkchen bei **DESKTOPGESTALTUNG DEAKTIVIEREN**.
4. Klicken Sie auf **OK** und starten Sie den Client neu, um sich mit dem ESXi-Server neu zu verbinden.

Clienteeinstellungen bearbeiten

Nachdem Sie sich mit dem ESXi-Server verbunden haben, finden Sie – wie in Abbildung 3-4 dargestellt – die weiteren Einstellungen zum vSphere Client im Menü unter **BEARBEITEN** → **CLIENTEINSTELLUNGEN**.

In diesem Fenster sind drei Registerkarten untergebracht. Auf der ersten haben wir vier Abschnitte, die das Laufzeitverhalten des Clients steuern. Die ersten beiden Abschnitte sind selbsterklärend, im dritten geht es um Meldungen, die Sie weggeklickt haben, weil Sie sie nicht mehr sehen wollten. Die Hinweise können zurückgesetzt werden, so dass Sie wieder alle Meldungen erhalten.

Im vierten Abschnitt lassen sich die mit der Zeit nervigen Registerkarten **ERSTE SCHRITTE** abschalten – ansonsten bekommen Sie nach dem Wegklicken einer Karte bei jeder neuen Gelegenheit wieder eine angezeigt. Wenn Sie hier das Häkchen herausnehmen, wird das lokal auf Ihrem Rechner gespeichert und gilt für alle weiteren ESXi-Server, mit denen Sie sich verbinden (auch später beim vCenter Server).



Abbildung 3-4: Clienteneinstellungen nach dem Verbinden

Die Einstellungen auf der zweiten Karte betreffen drei verschiedene Listen:

1. Die Größe der Liste von AUFGABEN UND EREIGNISSE (zulässiger Wert zwischen 10 und 1.000).
2. Ob in der BESTANDSLISTE (INVENTORY) nur die Informationen zu den virtuellen Maschinen und ESXi-Servern wie angezeigt aktualisiert oder die herausgefilterten Infos ebenfalls aktualisiert werden sollen.
3. Ob die VMs in der Bestandsliste überhaupt angezeigt werden sollen oder nur die Hosts.

Auf der dritten Registerkarte finden Sie nur einen Eintrag, der für große Umgebungen interessant ist: die maximale Anzahl an angeforderten Topologieelementen. Diese Einstellung betrifft erst Umgebungen mit einem vCenter Server, über den die virtuellen Maschinen, ESXi-Server, Netzwerke und Storages grafisch angezeigt werden können. Wenn Sie versuchen, eine Zuordnung anzuzeigen, die über mehr Container als den eingetragenen Grenzwert (standardmäßig 300) verfügt, erhalten Sie eine Meldung mit der Möglichkeit, die Anzeige der Grafik abubrechen oder damit fortzufahren.

Fehlermeldung über Logdateien

Sollten Sie bei Ihrem neu installierten Host eine Fehlermeldung bekommen, dass die Logdateien nicht geschrieben werden können, müssen Sie den Syslog-Dienst korrekt einstellen. Das können Sie mit dem vSphere Client auf der Oberfläche des ESXi-Hosts erledigen:

1. Gehen Sie auf die Registerkarte KONFIGURATION des Servers.
2. Klicken Sie unter SOFTWARE auf ERWEITERTE EINSTELLUNGEN. Es öffnet sich ein weiteres Fenster.
3. Wählen Sie im linken Teil des Fensters den Eintrag SYSLOG aus und erweitern Sie die Anzeige, indem Sie auf das Pluszeichen + klicken.
4. Unter dem Punkt GLOBAL können Einstellungen erreicht werden, die für die untergeordneten Punkte zählen. Da die Beschreibungen der Einträge sehr schön und aussagekräftig sind, wiederhole ich sie hier nicht.
5. Unter Syslog.global.LogDir kann ein Speicherort und Verzeichnis für die Logdateien angegeben werden, das z.B. so aussehen könnte: [datastore1] /var/log/.

Sie können aber auch z.B. ein NFS-Laufwerk dafür angeben. Wollen Sie so ein Laufwerk für alle ESXi-Hosts verwenden, dann können Sie beim nächsten Punkt Syslog.global.logDirUnique das Häkchen setzen. Es werden dann automatisch je ein Verzeichnis mit dem Namen des Hosts erstellt und die Dateien dort abgelegt.

Vergessen Sie aber nicht, diese Einstellung dann auch bei jedem Host zu machen.

Nun haben Sie mindestens den ersten ESXi-Server aufgesetzt. Dieser bildet die Grundlage für das weitere Vorgehen, also die Installation von VMs, gegebenenfalls das Aufsetzen eines vCenter Servers usw.

In diesem Kapitel haben Sie alles Notwendige über den ESXi-Server erfahren sowie über die Installationsmöglichkeiten, die Aufgaben und Arbeiten des Hypervisor und die Installation des vSphere Clients, den wir für den Zugriff auf den ESXi-Server und später gegebenenfalls für den vCenter Server benötigen.

Im nächsten Kapitel wird es spannender, denn da gehe ich sehr detailliert auf die Erstellung unserer ersten virtuellen Maschine mit allen Optionen und Fallstricken ein.

Die virtuelle Maschine

Nachdem ich Ihnen in den bisherigen Kapiteln das notwendige Vorwissen für die Erstellung einer virtuellen Maschine vermittelt habe, kommen wir nun zum eigentlich interessantesten Punkt, nämlich wie man eine VM richtig anlegt. Beim Anlegen der VM wird der Grundstein für die in der Maschine vorhandene Hardware gelegt. Ein nachträglicher Austausch ist immer mit Risiken verbunden – deshalb ist dieses Kapitel so wichtig und umfangreich! Auf den nächsten Seiten werden Sie alles über die Erstellung virtueller Maschinen erfahren.

Was nun noch fehlt, ist der innerhalb der Virtualisierungssoftware – also mit dem vSphere Client – einzuschlagende Weg. Dafür wird auf der grafischen Oberfläche ein Assistent bereitgestellt, der über verschiedene Wege erreichbar ist.

Woraus besteht nun eine virtuelle Maschine? Welche Dateien bilden dieses Konstrukt auf der VMFS-Partition? Auch diese Fragen suchen nach Antworten, die insbesondere beim Sichern oder Klonen der virtuellen Maschine Gold wert sind, denn es müssen z.B. beim Kopieren oder beim Backup nicht alle Dateien im Verzeichnis der VM mitgenommen werden.

Weiterhin ist nach dem Erstellungsprozess in den seltensten Fällen die virtuelle Maschine schon fertig aufgesetzt. Um ein besseres Handling für Maus- und Tastaturfunktionen zu erreichen und mehr Performance für die VM zu bekommen, müssen noch die VMware Tools mit den Treibern und Agenten installiert werden. Auch dabei können sich Fehler einschleichen, die einem später das Leben schwer machen können. Im Folgenden wird auch dieser wichtige Punkt detailliert beschrieben.

Eine virtuelle Maschine erstellen

Es gibt verschiedene Möglichkeiten, den Erstellungsvorgang für virtuelle Maschinen zu starten. Sie können im Menü DATEI → NEU eine neue virtuelle Maschine erstellen, eine

virtuelle Maschine anhand eines Templates bereitstellen, eine Maschine importieren oder konvertieren und eine virtuelle Maschine aus einer vorhandenen virtuellen Maschine klonen. Einiges davon ist erst über den vCenter Server möglich, um den wir uns in Kapitel 10 ausführlich kümmern.

Je nachdem, für welche Möglichkeit Sie sich entscheiden, variieren die Bildschirmdarstellungen leicht, da sie genau auf den ausgewählten Prozess abgestimmt sind. Alle nicht zutreffenden Optionen für Ihre Auswahl sind auch nicht anwählbar. Zum Beispiel ist KLONEN im Menü deaktiviert, wenn im Inventar keine virtuelle Maschine vorhanden ist oder der Fokus nicht auf einer steht. In allen Fällen ist jedoch die größtmögliche Anzahl von Optionen gegeben, um optimale Flexibilität für Ihre Auswahl zu gewährleisten.

ISO-Image einspielen

Da Sie mit Sicherheit mehrere virtuelle Maschinen mit dem gleichen Betriebssystem auf dem ESXi Server installieren wollen, empfiehlt es sich, eine ISO-Datei von der CD oder DVD zu erstellen und sie auf das VMFS-Volumen zu legen. Von dort aus hat jede VM Zugriff auf die Dateien, und die Installation geht dann wesentlich schneller.

1. Melden Sie sich mit dem vSphere Client am ESXi Server an, klicken Sie auf das Symbol BESTANDSLISTE (INVENTORY) und navigieren Sie dann zur Registerkarte ÜBERSICHT (SUMMARY).
2. Auf der rechten Seite des Bildschirms sehen Sie im Feld DATENSPEICHER (DATASTORE) den Eintrag des VMFS-Volumes. Klicken Sie mit der rechten Maustaste darauf und wählen Sie DATENSPEICHER DURCHSUCHEN (BROWSE DATASTORE). Es öffnet sich ein weiteres Fenster, das in Abbildung 4-1 zu sehen ist.

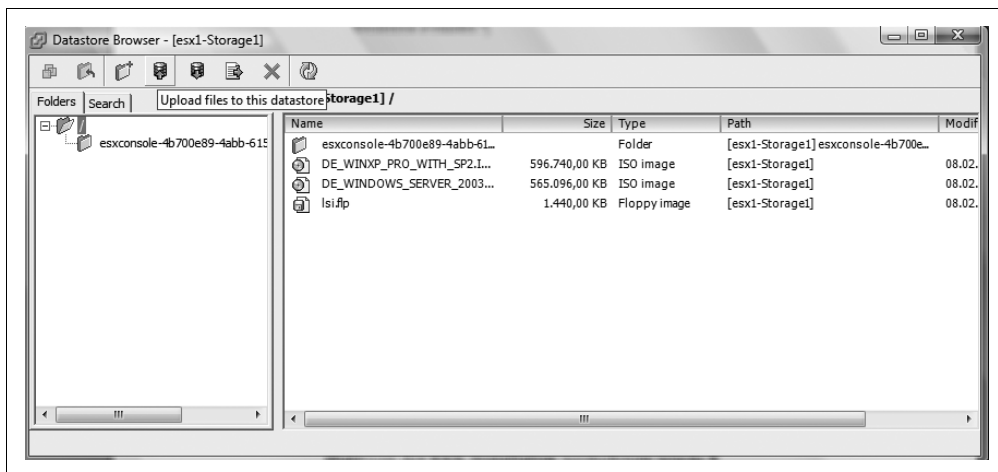


Abbildung 4-1: Dateien hochladen

- Über das vierte Symbol von links (DATEIEN HOCHLADEN – UPLOAD FILES TO THIS DATASTORE) können Sie z. B. eine ISO-Datei oder einen Ordner hier einspielen.



Es gibt auf dem Storage einen weiteren Ordner namens *VMImages*, in dem die VMware Tools und einige Floppy-Images liegen; der Ordner ist z. B. über *ssh* erreichbar und wird hier nicht angezeigt. Sie sollten Ihre Dateien nicht in diesen Ordner legen, weil er im *root*-Verzeichnis »/« gemountet ist und sonst Speicherplatz von der ESXi-Installation wegnehmen würde.

- Ist der Uploadvorgang abgeschlossen, wird die Datei im Datastore-Browser angezeigt. Schließen Sie das Fenster wieder.

Benutzerdefinierte VMs erstellen

Da die Erstellung einer virtuellen Maschine im benutzerdefinierten Pfad im Assistenten alle möglichen Optionen und die meiste Flexibilität bietet, beschreibe ich in diesem Abschnitt diese Vorgehensweise zur Erstellung einer neuen virtuellen Maschine. Wenn Sie im Assistenten das Häkchen bei BENUTZERDEFINIERT setzen, sehen Sie auf der linken Hälfte des Fensters einige zusätzliche Optionen, die bei TYPISCH nicht vorhanden sind.



Wenn Sie den Eintrag TYPISCH wählen, werden einige virtuelle Maschinen nicht so konfiguriert, wie es eigentlich sinnvoll wäre. Beispielsweise hätten Sie unter Windows XP 32 Bit einen IDE-Adapter statt SCSI und eine Netzwerkkarte (flexibel ^= AMD PCNet Adapter), die eher für 100 MBit als für 1 GBit tauglich ist.

Erst wenn Sie auf BEENDEN klicken, wird die Maschine erstellt. Drücken Sie vorher irgendwann auf ABBRECHEN, wird nichts gespeichert.

So erstellen Sie eine neue virtuelle Maschine über den benutzerdefinierten Pfad:

- Klicken Sie im vSphere Client in der Navigationsleiste auf BESTANDSLISTE und erweitern Sie die Liste bei Bedarf, um Ihre schon erstellten VMs zu sehen.
- Wählen Sie in der BESTANDSLISTE den verwalteten ESXi Server aus, dem Sie die neue virtuelle Maschine hinzufügen möchten.
- Wählen Sie DATEI → NEU → VIRTUELLE MASCHINE oder über das Kontextmenü NEUE VIRTUELLE MASCHINE ...

Der Assistent zur Erstellung einer neuen virtuellen Maschine wird angezeigt. Das Menü im linken Teil des Fensters weicht von dem im Assistenten für die normale Konfiguration der virtuellen Maschine ab, wenn Sie auf BENUTZERDEFINIERT klicken.

- Wählen Sie die Schaltfläche WEITER.
- Geben Sie einen aussagekräftigen Namen für eine virtuelle Maschine ein und klicken Sie auf WEITER.

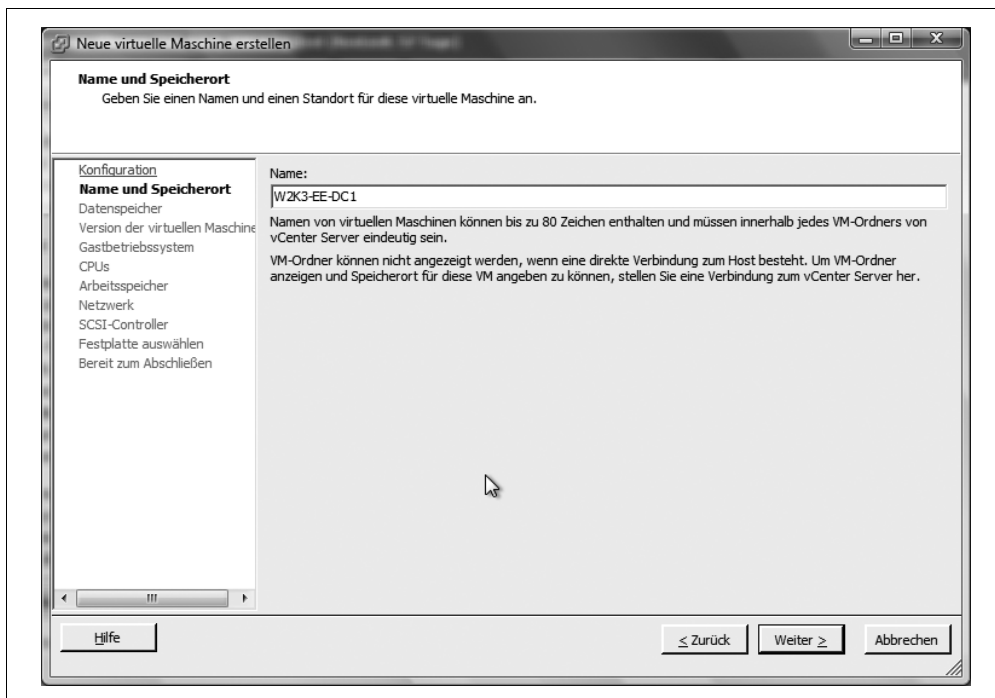


Abbildung 4-2: Eine neue virtuelle Maschine erstellen

Der Name der virtuellen Maschine, den Sie wie in Abbildung 4-2 dargestellt im Feld NAME eingeben, wird anschließend im Inventar des vSphere Clients angezeigt. Er wird auch als Name der Dateien der virtuellen Maschine und seines Verzeichnisses verwendet. Der Name kann bis zu 80 Zeichen lang sein und alphanumerische Zeichen sowie Unterstriche (_) und Bindestriche (-) enthalten. Dieser Name muss im gesamten Datacenter und innerhalb des Ordners eindeutig sein (Groß- und Kleinschreibung werden dabei nicht berücksichtigt). Er hat nichts mit dem Namen innerhalb des zu installierenden Betriebssystems zu tun, sollte aber der Übersicht zuliebe dementsprechend gewählt werden.

6. Wählen Sie einen Storage aus (siehe Abbildung 4-3), in dem Sie die Dateien der virtuellen Maschine speichern möchten, und klicken Sie auf WEITER.

Wählen Sie einen Datastore aus, der für die virtuelle Maschine und alle zugehörigen Dateien der virtuellen Festplatte groß genug ist. Für ESXi Server wird der Datastore auf diesem Server konfiguriert, einschließlich VMFS-, NAS- und iSCSI-Volumes. Den Haken bei SPEICHER-DRS können Sie erst setzen, wenn Sie sich über den vCenter Server anmelden – dazu später mehr in Kapitel 10.

7. Wählen Sie gegebenenfalls die Version der Maschine aus, um Kompatibilität zu einer älteren Version zu erreichen. Voreingestellt ist die Version 8, die auch neuere Hardware und einige andere zusätzliche Features zur Verfügung stellt. Die Auswahl ist abhängig von den Versionen der ESX Server im Cluster.

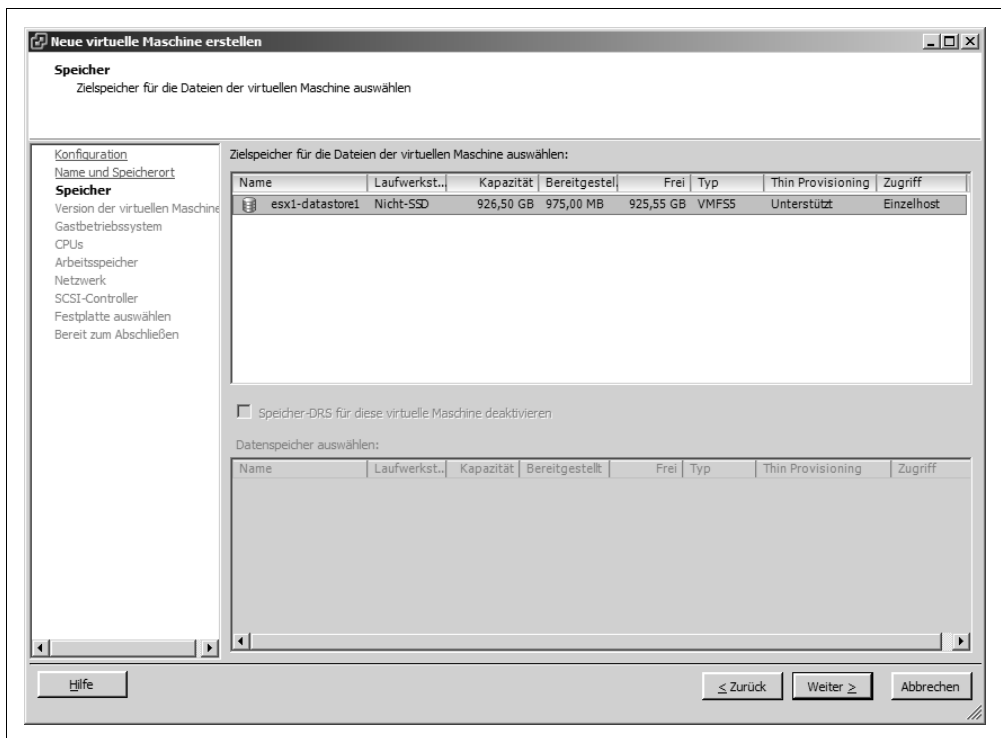


Abbildung 4-3: Den Speicherort der VM aussuchen



Wenn Sie die Hardwareversion der VM später ändern möchten oder eine ältere VM importiert haben, müssen Sie die VM ausschalten und im Abschnitt STATUS der VM auf VIRTUELLE MASCHINE AKTUALISIEREN klicken. Vergessen Sie nicht, die aktuelle Version der VMware Tools möglichst vor dem Ausschalten zu installieren. Von einer neueren Version auf eine ältere zurückzugehen, ist über den vSphere Client nicht möglich – wohl aber über die Kommandozeile (siehe Kapitel 18).

8. Wählen Sie unter GAST-BETRIEBSSYSTEM die Betriebssystemfamilie (WINDOWS, LINUX oder ANDERE, siehe Abbildung 4-4) aus und dann im Pull-down-Menü die zu installierende Version. Von der hier getroffenen Auswahl sind einige weitere Optionen und später die Installation der VMware Tools abhängig. So werden z.B. für bestimmte Betriebssysteme unterschiedliche Netzwerkkarten angeboten, es wird mehr oder weniger Arbeitsspeicher empfohlen, verschiedenartige SCSI-Controller werden vorgeschlagen usw.

Unter der Option ANDERE finden Sie z.B. Apple Mac OS X, FreeBSD, IBM OS/2, Novell NetWare, Solaris und UNIX. Ist Ihr gewünschtes Betriebssystem nicht dabei, nehmen Sie das, das ihm am nächsten kommt.

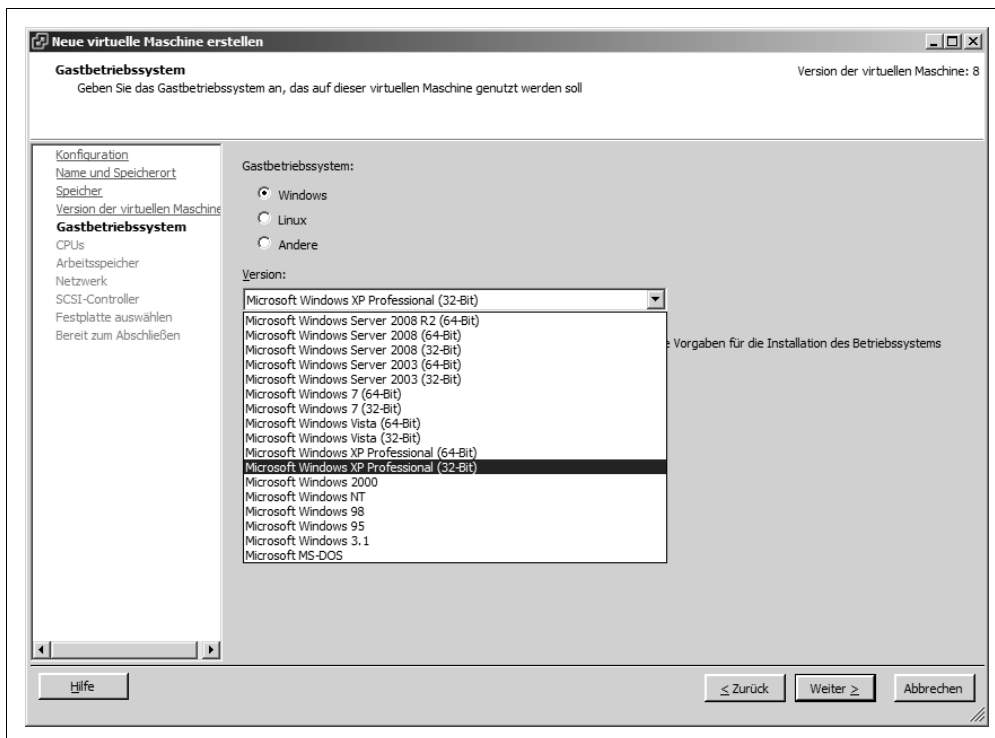


Abbildung 4-4: Auswahl der Betriebssysteme

Vom Assistenten wird das Gastbetriebssystem später nicht installiert, dafür sind Sie selbst verantwortlich. Der Assistent zur Erstellung einer neuen virtuellen Maschine wählt anhand dieser Informationen die richtigen Standardwerte aus, z.B. den benötigten Festplattenspeicher, die unterstützten Netzwerkkarten und SCSI-Controller usw. (Verlassen Sie sich aber nicht unbedingt darauf, denn der empfohlene Arbeitsspeicher berücksichtigt nicht eventuelle Aufgaben oder zu installierende Programme.)

9. Klicken Sie auf WEITER.
10. Wählen Sie im nächsten Fenster die Anzahl der virtuellen CPU-Sockel und die Kerne pro Sockel für Ihre Maschine und klicken Sie auf WEITER.



Die Seite ANZAHL DER VIRTUELLEN CPUS wird nicht angezeigt, wenn der Server nur einen einzelnen Prozessor besitzt oder das Gastbetriebssystem SMP nicht unterstützt (z.B. NetWare und Windows NT 4.0). Sie können der VM nicht mehr Kerne geben, als Ihr Host insgesamt hat oder Ihre Lizenz erlaubt. Die obige und untere Anzeige wird ggf. auf den maximal möglichen Wert zurückgesetzt.

Wenn Sie später eine Anwendung innerhalb der VM installieren, die mehrere Prozessoren unterstützt, wählen Sie bei diesem Schritt besser mehrere CPUs. Braucht Ihre Software nur einen Prozessor, nehmen Sie hier auch

nur einen. Möchten Sie eine Vorlage (Template) generieren, nehmen Sie besser zwei Prozessoren. Hinterher ist es einfacher, auf einen, vier oder gar 32 Prozessoren umzustellen!

11. Konfigurieren Sie die Speichergröße der virtuellen Maschine, indem Sie die Anzahl der MBytes oder GBytes auswählen.

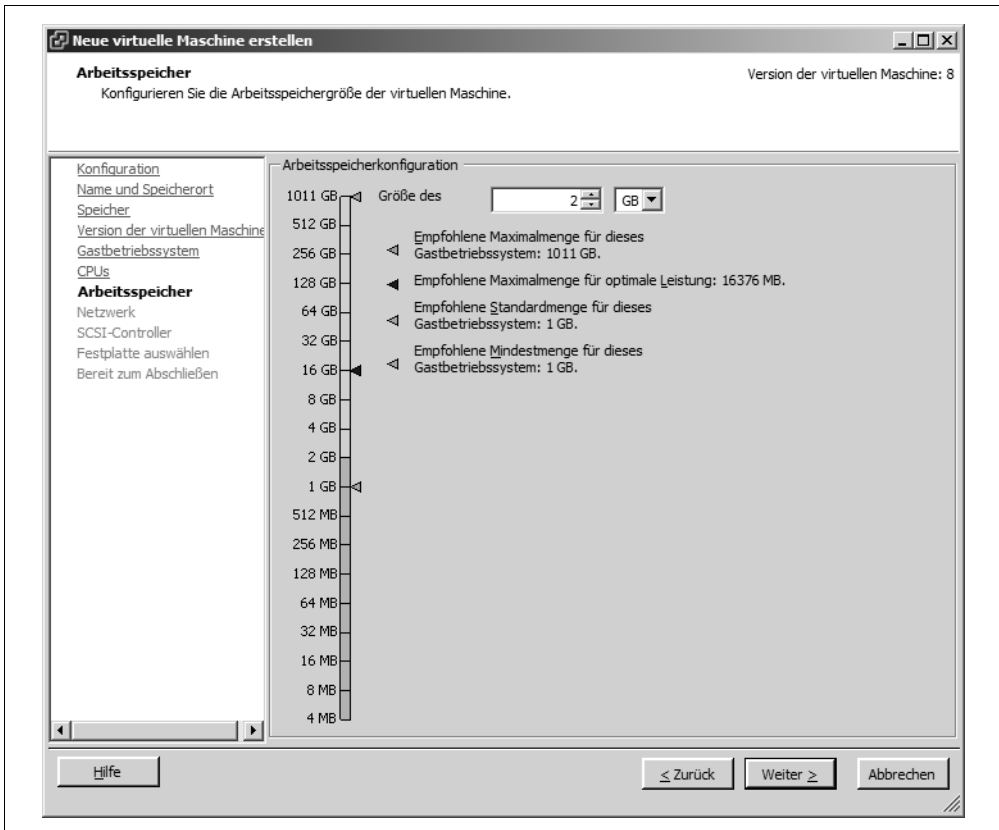


Abbildung 4-5: Arbeitsspeicherempfehlungen für die VM

Die empfohlenen Mindest- und Höchstwerte hängen vom Gastbetriebssystem ab. Unabhängig von diesem beträgt die minimale Speichergröße 4 MByte wenn die VM ein gewöhnliches BIOS hat, bei (U)EFI ist der Mindestwert 96 MB. Die Einstellung wird anhand des ausgewählten Betriebssystems automatisch vorgenommen und ist teilweise – abhängig vom gewählten OS – unter den Optionen der VM nachträglich änderbar. Der Höchstwert hängt vom Server ab, liegt jedoch bei ESXi Server 5.0 bei 1.011 GByte. Haben Sie die Version 7 der VM gewählt, können Sie maximal 255 GByte vergeben.

Die Speichergröße muss ein Vielfaches von 4 MByte sein. Es ist auch möglich, die Werte in MByte anzugeben. Nur bei der Version *Enterprise Plus* gibt es keine Beschränkungen bezüglich des maximalen ESXi Server-Speicherausbaus. Abbildung 4-5 zeigt beispielhaft die Voreinstellungen für Mac OS X 10.6 (64 Bit).



Sie können übrigens auf die Werte links von der Skala mit der Maus klicken, um der Maschine z.B. 1, 2 oder 4 GByte zuzuordnen. Achten Sie bei Microsoft-Betriebssystemen bis einschließlich Server 2003 auf die Zweierpotenzen.

12. Klicken Sie auf WEITER.
13. Wählen Sie die Netzwerke bzw. Portgruppen der VMs (Portgruppen sind Unterteilungen der Switches, zu ihnen kommen wir in Kapitel 6) auf den virtuellen Switches aus, mit denen Sie eine Verbindung herstellen möchten, sowie die entsprechenden Optionen wie die Anzahl der NICs (*Network Interface Cards*) für Verbindungen und die Namen der Netzwerke. Legen Sie fest, ob die Verbindung beim Einschalten hergestellt werden soll.

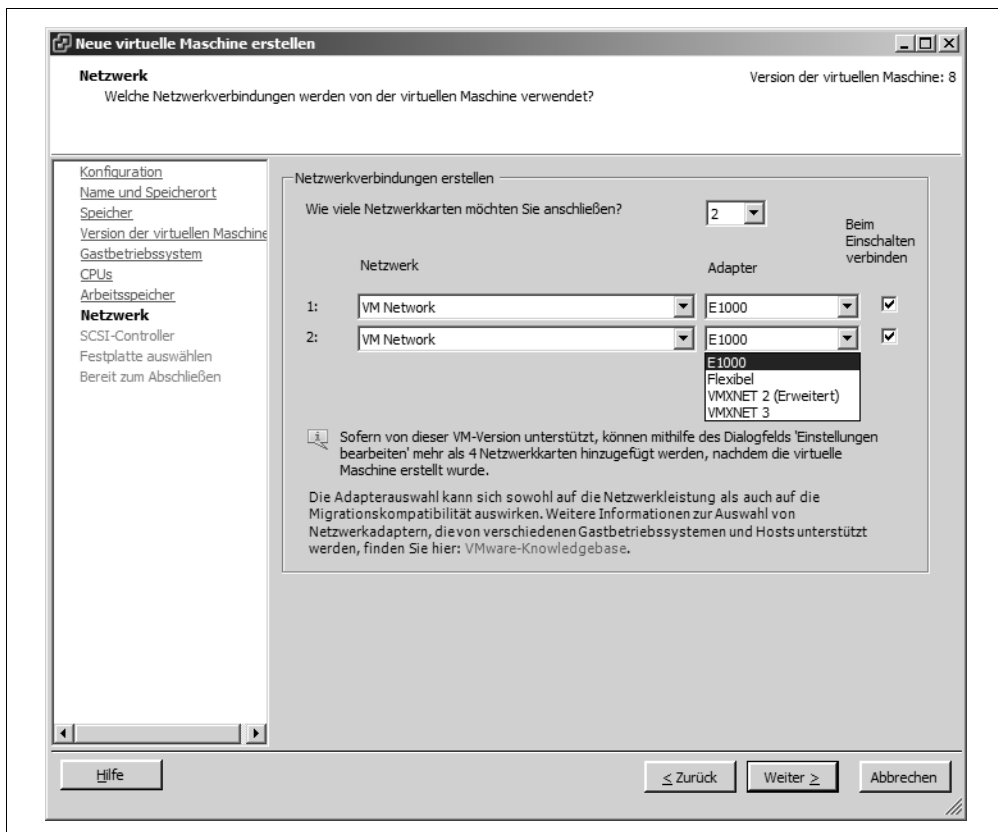


Abbildung 4-6: Auswahl der Netzwerkkarten



Die Auswahl hängt vom ausgewählten Betriebssystem ab (siehe Abbildung 4-6). Nehmen Sie möglichst nicht mehr den Adapter *Flexibel*, weil seine Performance im Netzwerk mit GBit-Ethernet sehr schlecht ist (siehe Tabelle 4-3 Unterstützte Netzwerkkarten).

Adaptertypen

Der *IDE-Adapter* ist immer *ATAPI* und wird immer für optische Laufwerke wie CD oder DVD genutzt. Der Standard-E/A-Adaptertyp Ihres Gastbetriebssystems ist bereits ausgewählt.

Ältere Gastbetriebssysteme verwenden standardmäßig den *BusLogic- oder IDE-Adapter*.

Der LSI Logic-Adapter verfügt über eine verbesserte Leistung, funktioniert besser mit SCSI-Geräten, die keine Festplatten sind, und ist als Treiber z. B. in Windows Server 2003 enthalten. Die Auswahl des SCSI-Controllers hat keinen Einfluss darauf, ob Sie als virtuelle Festplatte eine IDE- oder eine SCSI-Festplatte verwenden. Beim SCSI-Adapter können Sie zwischen BusLogic Parallel, LSI Logic Parallel, LSI Logic-SAS und VMware Paravirtual wählen. Die SAS-Option (Serial Attached SCSI) ist für virtuelle Maschinen ab der Hardwareversion 7 und 8 verfügbar.



Wenn Sie eine virtuelle Maschine mit LSI Logic erstellen und eine zusätzliche virtuelle Festplatte hinzufügen, die BusLogic-Adapter verwendet, wird die virtuelle Maschine von der zusätzlichen Festplatte gebootet, also dem BusLogic-Gerät.

Sie können den Treiber auch von der LSI Logic-Website herunterladen oder z. B. die FLP-Datei von der Website zum Buch nehmen.

Paravirtuelle SCSI-Adapter (PVSCSI-Adapter) sind Hochleistungsspeicheradapter, die einen höheren Durchsatz und eine geringere CPU-Auslastung liefern können. PVSCSI-Adapter sind am besten für Umgebungen geeignet, die E/A-intensive Anwendungen ausführen (besonders SAN-Umgebungen). PVSCSI-Adapter sollten nicht als startfähige Festplatte genommen werden, da es hinterher zu Problemen kommen kann.

Als Voraussetzung für die Nutzung empfehle ich eine vorhandene virtuelle Maschine, auf der ein Gastbetriebssystem und die VMware Tools mit PVSCSI-Treibern installiert sind. Die virtuelle Maschine sollte mit einem primären SCSI-Adapter konfiguriert werden, um eine Festplatte zu unterstützen, auf der das Betriebssystem installiert ist, und kann dann als Datenplatte einen paravirtuellen Adapter nutzen.

Wie in Abbildung 4-7 zu sehen ist, werden im Pull-down-Menü NETZWERK die Portgruppen aufgelistet, die für die Verwendung durch die virtuelle Maschine auf dem Server konfiguriert sind. Wenn für die virtuellen Maschinen keine Portgruppen konfiguriert sind, wird ein Dialogfeld mit einem Warnhinweis angezeigt und Sie kön-

nen keine virtuellen Netzwerkkarten konfigurieren. Die Portgruppe *VM Network* wird bei der Installation des ESXi Servers üblicherweise automatisch angelegt.

Die Menge an Netzwerkkarten, die Sie hier auswählen können, ist auf vier begrenzt. Je nach ausgewähltem Betriebssystem können Sie nach der Erstellung der VM aber noch weitere Karten hinzufügen.

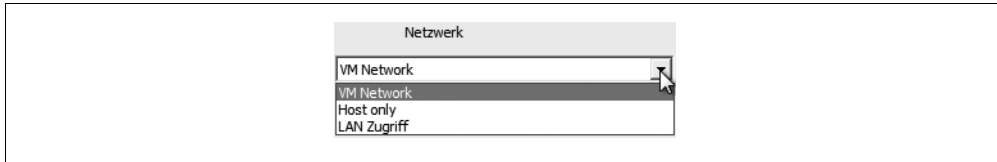


Abbildung 4-7: Auswahl der VM-Portgruppen

14. Klicken Sie auf WEITER.
15. Wählen Sie den SCSI-Adaptertyp aus, den Sie mit der virtuellen Maschine verwenden möchten. Beachten Sie die Hinweise im Kasten »Adaptertypen«.
16. Wählen Sie den Typ der Festplatte aus und klicken Sie auf WEITER.

Sie können Daten zu virtuellen Maschinen auf einer neuen virtuellen Festplatte, einer vorhandenen virtuellen Festplatte oder einer zugeordneten SAN-LUN (*Storage Area Network Logical Unit Number*) speichern.

Eine virtuelle Festplatte besteht aus einer oder mehreren Dateien im Dateisystem, die dem Gastbetriebssystem als einzelne Festplatte angezeigt werden (siehe Abbildung 4-8). Diese Festplatten können zwischen den einzelnen ESXi Servern über einen vCenter Server mittels Storage vMotion verschoben werden.

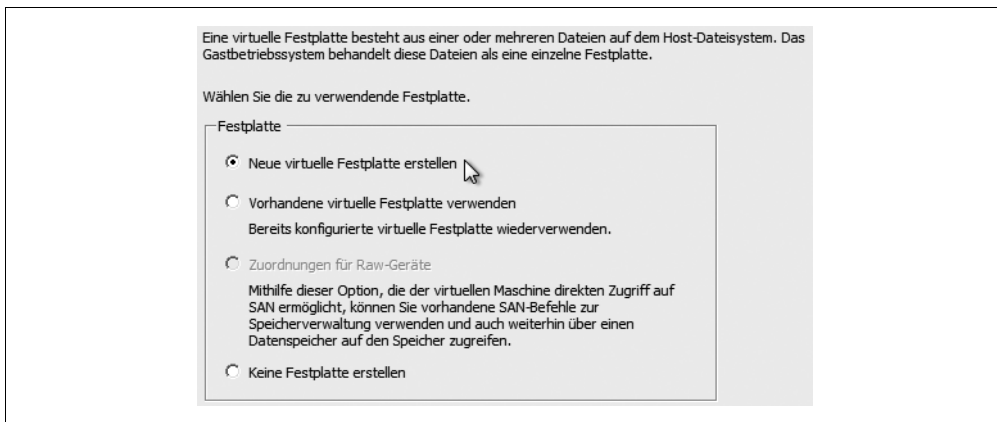


Abbildung 4-8: Auswahlmöglichkeiten bei virtuellen Festplatten

Durch Zuordnung einer SAN-LUN erhält die virtuelle Maschine direkten Zugriff auf dieses SAN, wodurch Sie vorhandene SAN-Befehle für die Speicherverwaltung der Festplatte verwenden können – das nennt sich *Raw Device Mapping* (RDM).

17. Wenn Sie eine neue virtuelle Festplatte erstellen möchten, müssen Sie ihre Größe festlegen, einen Datastore-Speicherort für sie angeben und auf WEITER klicken.

The screenshot shows a VMware virtual disk creation wizard with three main sections:

- Kapazität**: A section for setting the disk size. It includes a text input field for "Festplattengröße:" containing the value "40", and a dropdown menu for the unit, currently set to "GB". The dropdown menu is open, showing options: "MB", "GB" (selected), and "TB".
- Festplattenbereitstellung**: A section for choosing the provisioning type. It contains three radio button options: "Thick-Provision Lazy-Zeroed" (selected), "Thick-Provision Eager-Zeroed", and "Thin-Bereitstellung".
- Speicherort**: A section for selecting the storage location. It contains two radio button options: "Gemeinsam mit virtueller Maschine speichern" (selected) and "Datenspeicher oder Datenspeicher-Cluster angeben:". Below the second option is a text input field and a "Durchsuchen..." button.

Abbildung 4-9: Typ und Größe der Festplatte festlegen

Wie Sie in Abbildung 4-9 sehen, können Sie die Festplattengröße in MByte, GByte oder TByte angeben. Die Standardeinstellung wird je nach gewähltem Betriebssystem angezeigt. Der verfügbare Speicherplatz auf dem ausgewählten VMFS-Volume wird aufgelistet, wenn Sie manuell einen Datenspeicher auswählen. Sie können Festplatten von 1 MByte bis 16 TByte (16.384 GByte) konfigurieren, wobei Sie auch Werte für MByte oder GByte in ganzen Zahlen oder auch mit Komma angeben können. Die virtuelle Festplatte sollte für das Gastbetriebssystem und die gesamte zu installierende Software groß genug sein. Berücksichtigen Sie auch das zukünftige Anwachsen der Daten.

Ein Partitionieren innerhalb des Betriebssystems ist natürlich möglich, aber ich empfehle Ihnen, für weitere Laufwerke lieber zusätzliche virtuelle Festplatten zu nehmen, weil Sie damit viel flexibler sind. Nachträglich lässt sich das übrigens teilweise über den VMware Converter erledigen. Sie können später über den Dialog EIGENSCHAFTEN DER VIRTUELLEN MASCHINE zusätzliche virtuelle Festplatten hinzufügen.

Das für Ihre Bedürfnisse am besten geeignete Festplattenformat können Sie dem Kasten »Festplattenformate« entnehmen.

Sie können eine virtuelle Festplatte in demselben Datastore wie die virtuelle Maschine verwenden oder einen anderen Storage auswählen. Über DURCHSUCHEN können Sie ein anderes Volume auswählen.

18. Klicken Sie auf WEITER und wählen Sie einen virtuellen SCSI-Anschluss für das Laufwerk. Üblicherweise ist das SCSI (0:0), was bedeutet, dass die Platte an den ersten SCSI-Adapter und mit der ID 0 angeschlossen wird. Lassen Sie den Modus der Festplatte zunächst unberücksichtigt – dazu kommen wir später im Abschnitt »Festplattengröße und -modus«. Wählen Sie aus Performancegründen möglichst nicht IDE.

19. Es werden eine Zusammenfassung der ausgewählten Hardwarekomponenten und das zu installierende Betriebssystem angezeigt. Überprüfen Sie Ihre Angaben, gehen Sie gegebenenfalls zurück, um etwas zu ändern, und klicken Sie anschließend auf **BEENDEN**.
20. (Optional:) Falls Sie das Häkchen bei **EINSTELLUNGEN DER VIRTUELLEN ...** gesetzt haben, heißt die Beenden-Schaltfläche »Fortfahren«. Sie bekommen dabei die ausgewählte Hardware vor der eigentlichen Erstellung der VM nochmals angezeigt und können dort weitere Änderungen vornehmen.

Festplattenformate

Thin-Bereitstellung

Dieses Format können Sie verwenden, um Speicherplatz zu sparen. Dabei wird nur so viel Platz bereitgestellt, wie das Gastbetriebssystem tatsächlich braucht. Der Umfang kann aber trotzdem natürlich nicht größer sein als der des Volumes.



Das Format »Thin-Bereitstellung« können Sie für die Festplatte der VM nicht benutzen, wenn Sie Clusterlösungen einrichten wollen. Auch Fehlertoleranz (*Fault Tolerance*) wird dann nicht unterstützt. Die Festplatte kann später auf ihre maximale Kapazität anwachsen und den gesamten für sie bereitgestellten Speicherplatz in Anspruch nehmen. Außerdem können Sie die Festplatte manuell in das Thick-Format konvertieren. Beachten Sie auch, dass die Performance beim Wachsen der Festplatte leiden kann.

Thick-Provision Lazy-Zeroed

Das ist das Standardformat für virtuelle Festplatten. Die Festplatte in diesem Format belegt von Anfang an den gesamten Speicherplatz. Es wird kein Auffüllen der Blöcke mit Nullen durchgeführt. Eine Umwandlung vom Thick- in das Thin-Format gibt es nur beim Storage vMotion oder über die Kommandozeile.

Thick-Provision Eager-Zeroed

Dieses Festplattenformat sollten Sie auswählen, wenn diese virtuelle Maschine später im Modus *Fault Tolerance* (FT, gespiegelte VMs) laufen soll. Beim Auswählen von FT kann das aber auch nachträglich erledigt werden. Darauf gehe ich später in Kapitel 10 noch detailliert ein. Bei diesem Modus wird die gesamte Festplatte mit Nullen gefüllt bzw. überschrieben. Dieser Vorgang dauert deutlich länger als die beiden anderen Möglichkeiten.

Jetzt haben wir die Erstellung der ersten virtuellen Maschine abgeschlossen. In Abbildung 4-10 sehen Sie ein Beispiel für die Übersicht der gewählten Einstellungen. Bevor Sie die neue virtuelle Maschine einschalten, müssen Sie die virtuelle Festplatte partitionieren, formatieren und ein Gastbetriebssystem sowie die VMware Tools installieren. Die Partitio-

nierungs- und Formatierungsschritte führt das Installationsprogramm des Betriebssystems normalerweise selbst durch.

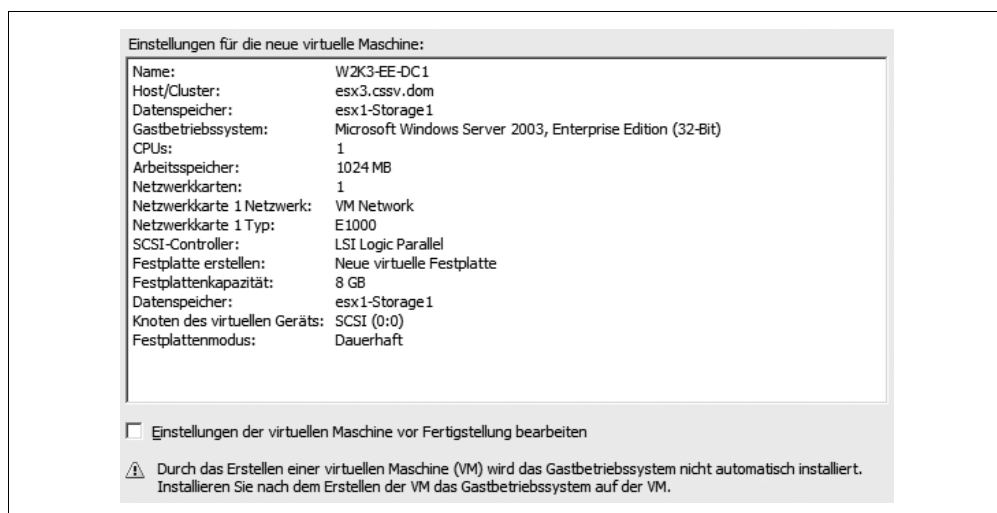


Abbildung 4-10: Übersicht der gewählten Einstellungen

In der Statuszeile am unteren Rand sehen Sie den Prozess der Erstellung der Maschine (Abbildung 4-11). Wenn dieser Prozess abgeschlossen ist, steht unter *Status* ABGESCHLOSSEN.

Kürzlich bearbeitete Aufgaben

Name	Ziel	Status	Angeforderte St...	Zeit der Fertigstell...
 Virtuelle Maschine erstellen	 192.168.50.111	 Abgeschlossen	18.12.11 14:03:30	18.12.11 14:03:31
 Virtuelle Maschine neu konfigurieren	 vm-XP-1	 Abgeschlossen	18.12.11 14:00:21	18.12.11 14:00:25
 Virtuelle Maschine erstellen	 192.168.50.111	 Abgeschlossen	18.12.11 13:58:42	18.12.11 13:58:43
 Aufgaben				

Abbildung 4-11: Status der Erstellung einer VM

Betriebssystem installieren

Ihre erste virtuelle Maschine unter dem ESXi Server ist jetzt in der Standardkonfiguration angelegt. Ob diese allerdings schon Ihren Anforderungen entspricht, sei dahingestellt. Auf jeden Fall muss noch ein Datenträger, meist CD oder DVD, mit dem Installationsprogramm angeschlossen werden. Sie können natürlich auch die Installation über die Netzwerkkarte mit PXE (*Preboot Execution Environment*) vornehmen.

1. Dazu klicken Sie am besten mit der rechten Maustaste in der BESTANDSLISTE (INVENTORY) auf den Namen der VM und wählen aus dem Kontextmenü EINSTELLUNGEN

BEARBEITEN (EDIT SETTINGS) aus. In dem nun offenen Fenster sehen Sie die Hardware der Maschine, wie Sie sie angelegt haben.

2. Wählen Sie den Eintrag CD-/DVD-LAUFWERK 1 aus.
3. Klicken Sie auf DATENSPEICHER-ISO-DATEI und dann auf DURCHSUCHEN, um die vorher kopierte Datei auszuwählen. In diesem Fenster sehen Sie die angelegte VMFS-Partition (ESX1-DATASTORE1) und den oben erwähnten Ordner *vmimages*, in dem sich u.a. die VMware Tools befinden.
4. Klicken Sie doppelt auf ESX1-DATASTORE1, dann auf die ISO-Datei (siehe Abbildung 4-12) und dann auf OK.

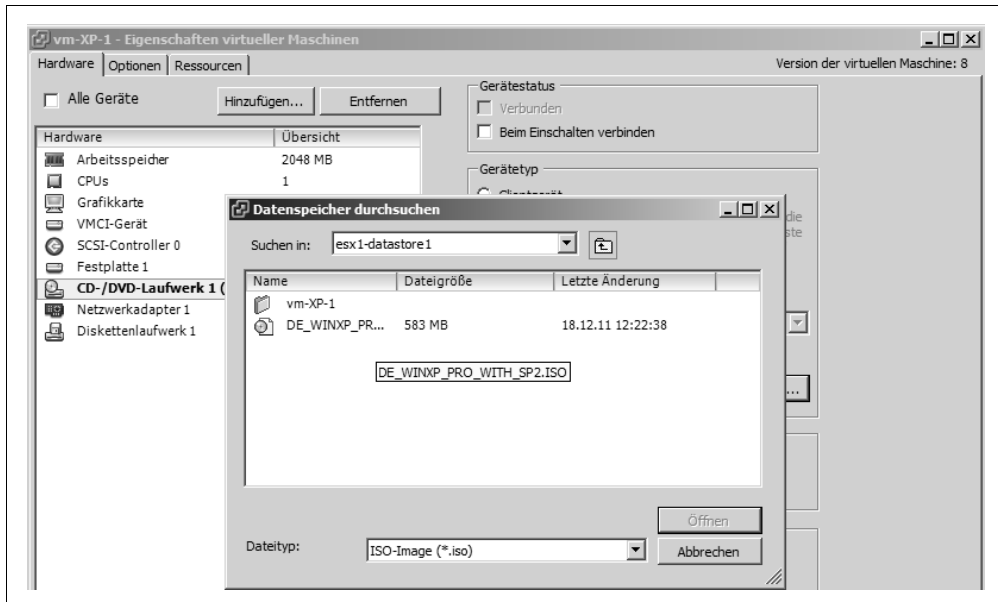


Abbildung 4-12: Installationsmedium zuweisen

5. Unter GERÄTESTATUS müssen Sie noch das Häkchen bei BEIM EINSCHALTEN VERBINDEN setzen, damit das Image für die virtuelle Maschine bereitgestellt wird.
6. Klicken Sie anschließend auf OK.

Jetzt können Sie Ihre VM einschalten und z.B. über die Registerkarte KONSOLE den Installationsvorgang mitverfolgen. Ich bevorzuge es, in der Symbolleiste des vSphere Clients das Icon mit dem Monitor auszuwählen, damit ich ein neues Fenster für meine Maschine bekomme.

Bevor Sie jetzt weitermachen, beachten Sie bitte die folgenden wichtigen Hinweise:

- Unter Umständen müssen Sie die Bootreihenfolge im BIOS oder EFI der virtuellen Maschine ändern, damit die virtuelle Maschine zunächst versucht, vom CD-/DVD-

Gerät zu booten, bevor sie damit beginnt, über andere Startgeräte zu booten. Drücken Sie dazu die Taste F2, wenn Sie beim Hochfahren der virtuellen Maschine das BIOS oder EFI sehen. Falls Sie das nicht schaffen, setzen Sie das Häkchen unter EIGENSCHAFTEN DER VM → REGISTERKARTE OPTIONEN → VMWARE TOOLS zum automatischen Aufruf des BIOS oder EFI-Setup.

- Sind Eingaben innerhalb des Fensters notwendig, z.B. Lizenz-Key, Name der Firma o. Ä., müssen Sie mit der Maus in das Fenster klicken, damit es den Fokus bekommt. Aus der virtuellen Maschine kommen Sie wieder heraus, indem Sie die Tastenkombination Strg+Alt kurz drücken.
- Falls Sie Windows installieren und zur Anmeldung die Aufforderung DRÜCKEN SIE STRG+ALT+ENTF sehen, sollten Sie stattdessen die Tastenkombination Strg+Alt+Einfgr drücken oder über das Menü auf VM klicken, dann auf GAST und dann STRG+ALT+ENTF SENDEN anklicken.
- Sollte eine Meldung erscheinen, die Sie darüber informiert, dass die MKS (Mouse, Keyboard, Screen) nicht verbunden werden kann, stimmt etwas nicht mit der Namensauflösung von Host oder vCenter Server. Konfigurieren Sie DNS oder die Hosts-Datei auf Ihrem Rechner richtig, damit die Namensauflösung funktioniert.

VMware Tools installieren

Die VMware Tools bestehen aus einer Reihe von Dienstprogrammen und Agenten, die die Performance des Gastbetriebssystems der virtuellen Maschine und die Verwaltung der virtuellen Maschine verbessern. Die Installation von VMware Tools im Gastbetriebssystem ist unerlässlich. Zwar kann das Gastbetriebssystem ohne VMware Tools ausgeführt werden, doch müssen Sie dann auf wichtige Funktionen und einige Bequemlichkeit verzichten.

Bei der Installation der VMware Tools installieren Sie gleichzeitig Folgendes:

- Den *VMware Tools-Dienst* (oder *vmware-guestd* bei Wahl von Linux als Gastbetriebssystem)
- Eine Reihe von *VMware-Gerätetreibern* einschließlich eines SVGA-Bildschirmtreibers, des Netzwerktreibers (z.B. *vmxnet*) für einige Gastbetriebssysteme, des BusLogic- oder LSI Logic-SCSI-Treibers für einige Gastbetriebssysteme, des Speichersteuerungstreibers (*vmmemctl.exe*) zur effizienten Speichertzuteilung zwischen virtuellen Maschinen, des Synchronisierungstreibers zur Stilllegung von I/O für Backups oder Snapshots und des VMware-Maustreibers
- Die *VMware Tools-Systemsteuerung*, über die Sie Einstellungen ändern sowie zugewiesene virtuelle Geräte anschließen und abtrennen können
- Eine Reihe von Skripten, die Sie beim Automatisieren von Vorgängen im Gastbetriebssystem unterstützen. Die Skripten werden bei Betriebszustandswechseln der virtuellen Maschine ausgeführt.

- Eine Komponente, die das Kopieren und Einfügen von Text zwischen dem Gast- und dem Betriebssystem auf einem verwalteten Server in Microsoft Windows-Gastbetriebssystemen unterstützt. Die Option zum Kopieren und Einfügen wird in Linux-Gastbetriebssystemen nicht unterstützt.

Konfigurieren Sie das Gastbetriebssystem, bevor Sie die VMware Tools installieren oder neu installieren. Auf diese Weise können die Tools und Treiber die korrekte Maus- und weitere Hardwarekonfigurationen erkennen und berücksichtigen.

Einschränkungen

Für VMware Tools unter ESXi gelten folgende Einschränkungen:

- Das Verkleinern von Festplatten (*Shrinking*) wird zwar nicht unterstützt, aber in manchen Betriebssystemen können Sie es innerhalb der VM anwählen. Das ist z.B. praktisch, wenn Sie aus Ihrer VM eine OVF-Vorlage (*Open Virtualization Format*, offenes Virtualisierungsformat) machen wollen, damit der Export nicht zu groß wird.
- Unter Windows NT funktionieren die Standardskripten für *Suspend* (Anhalten) und *Resume* (Wiederaufnehmen) nicht.
- Die Installation des Maustreibers schlägt in früheren Linux-Versionen als 4.2.0 für die grafische Oberfläche (X) fehl.



Erst wenn Sie die Tools installiert haben, können Sie die Schaltflächen für das Herunterfahren und Neustarten nutzen, denn dieses wird über Agenten im virtuellen Betriebssystem ausgelöst. Der Suspend-Modus funktioniert auch vorher. Wenn Sie das Gastbetriebssystem also ohne Tools herunterfahren möchten, müssen Sie das innerhalb des Fensters im Gast-OS manuell tun oder über das Menü.

- Die Tools von VMware lassen sich in einem laufenden Gastsystem über den Menüpunkt VM → GAST → VMWARE TOOLS INSTALLIEREN oder BESTANDSLISTE → VIRTUELLE MASCHINE → GAST → INSTALL VMWARE TOOLS installieren. Ob die Tools schon auf dem Betriebssystem installiert sind, wird jeweils in der ÜBERSICHT (siehe Abbildung 4-13) angezeigt sowie im Fenster des Windows-Gastsystems links neben der Uhr (abschaltbar!).



Ich empfehle dringend die Installation der Tools, weil sie die Handhabung von Maus und Tastatur wesentlich vereinfachen (die sogenannte *Grab-Funktion*) und ein paar weitere Features mitbringen, die nachfolgend beschrieben werden.

1. Klicken Sie in der Menüleiste des Remote-Console-Fensters auf VM → GAST → VMWARE TOOLS INSTALLIEREN. Gegebenenfalls müssen Sie Strg+Alt drücken, um mit der Maus aus dem Fenster herauszukommen und das Menü zu erreichen.

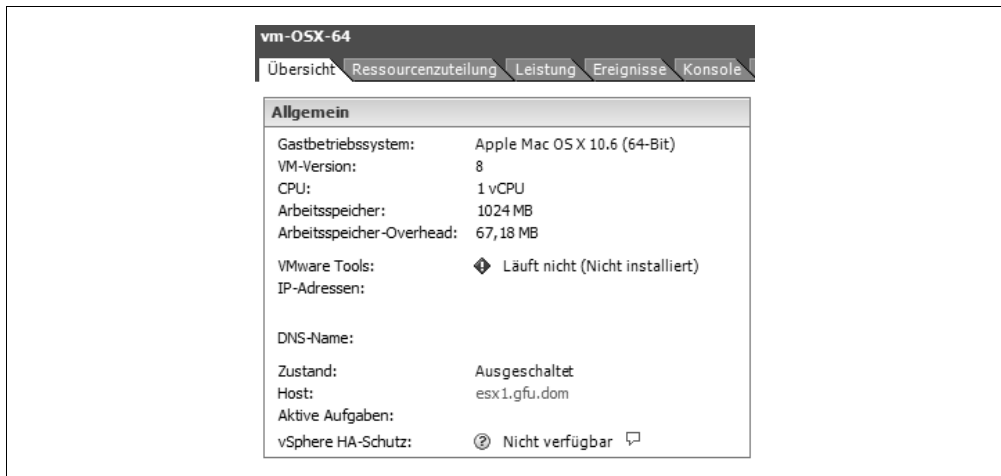


Abbildung 4-13: VMware Tools nicht installiert

Beachten Sie den Hinweis, der in Abbildung 4-14 dargestellt wird, dass die Tools nur im laufenden Gastbetriebssystem installiert werden können.



Abbildung 4-14: Installation der VMware Tools

1. Klicken Sie auf die Schaltfläche OK und im Fenster des Assistenten auf WEITER.
2. Je nachdem, ob diese VM auch unter anderen VMware-Produkten wie der Workstation oder dem VMware Server laufen soll, wählen Sie TYPISCH oder VOLLSTÄNDIG aus. Unter BENUTZERDEFINIERT können bestimmte Einstellungen geändert werden, z. B. der Speicherort innerhalb der VM (siehe Abbildung 4-15). Auch können Sie sich die einzelnen Komponenten ansehen und die jeweilige Funktionsbeschreibung anzeigen lassen (siehe Tabelle 4-1).
3. Je nach installiertem Betriebssystem muss gegebenenfalls noch der Microsoft-Hinweis für nicht zertifizierte Treiber bestätigt werden.
4. Klicken Sie anschließend auf BEENDEN und starten Sie die virtuelle Maschine (gegebenenfalls) neu.



Abbildung 4-15: Benutzerdefinierte Installation der Tools

Tabelle 4-1: Funktionsbeschreibung der VMware Tools

Funktion	Beschreibung	Bemerkung
Toolbox	Dienstprogramme zur Erweiterung des Funktionsumfangs dieser virtuellen Maschine	Die Toolbox enthält den VMware Tray neben der Uhr in der Symbolleiste, der in der Systemsteuerung als CPL-Datei liegt, sowie den Dienst <i>VMware Tools Service</i> , der u. a. einen Heartbeat an den Host sendet.
Protokollierung der WMI-Leistung	Leistungsüberwachung zwischen der Gast-SDK-API und der WMI-Umgebung aktivieren	Erstellt unter Start → Programme → VMware → einen Eintrag für die Statistikprotokollierung als Systemmonitor
VMware-Gerätetreiber	Treiber zur Verbesserung der Leistung der virtuellen Maschine	Enthält Treiber für spezielle Hardware, die über den ESXi Server zur Verfügung gestellt wird
Treiber für Aufnahme/Wiedergabe	Treiber zur Aktivierung von Aufnahme und Wiedergabe virtueller Maschinen	Treiber für Backups und Snapshots
Paravirtuelles SCSI	Treiber zur Verbesserung der Leistung der paravirtuellen SCSI-Geräte	Paravirtuelle Adapter sollten nicht als Bootfestplatte genommen werden, obwohl VMware im Ordner <i>VMImages</i> Floppy-Images für Windows-Betriebssysteme bereithält. Nutzen Sie Festplatten an so einem Adapter z. B. für ein SAN als zweite oder weitere Festplatte.
Virtuelles Drucken	Ermöglicht das automatische Drucken auf den Druckern des Host-computers	Bei der typischen Installation der Tools ist dieser Treiber nicht ausgewählt. Er bringt aber auch nicht allzu viel, da meistens Netzwerkdrucker für die VMs genutzt werden.
Treiber für Speichersteuerung	Treiber zur erweiterten Speicherverwaltung für diese virtuelle Maschine	Der Hintergrundprozess <i>vmmemctl.exe</i> wird über die erweiterten Einstellungen des ESXi Hosts gesteuert. Mit ihm kann der Speicherbedarf in der VM besser kontrolliert werden und in Grenzsituationen mehr RAM für andere VMs bereitgestellt werden. Bei Web- und Terminalservern sollten Sie diesen Treiber deaktivieren, weil diese sehr plötzlich sehr viel Speicher haben wollen.

Tabelle 4-1: Funktionsbeschreibung der VMware Tools (Fortsetzung)

Funktion	Beschreibung	Bemerkung
Maustreiber	Treiber zur Verbesserung der Leistung der virtuellen Maus	Die Tastenkombination Strg+Alt ist nach der Installation nicht mehr notwendig und die Performance der Maus erheblich verbessert.
Treiber für Dateisystem-synchronisierung	Treiber zur Synchronisation des Dateisystems zur Vorbereitung auf Sicherungen	Auch dieser Treiber wird bei Backups, Suspend und Snapshots gebraucht. Damit sind kurzfristig keine E/A-Vorgänge möglich. (Nur bis Windows 2003.)
SCSI-Treiber	Treiber zur Verbesserung der Leistung virtueller SCSI-Geräte	Notwendige angepasste Treiber für SCSI-Geräte. Installieren Sie möglichst keine anderen SCSI-Treiber des Herstellers, z. B. LSIlogic.
SVGA-Treiber	Treiber zur Verbesserung der Leistung der virtuellen Grafikkarte	Ab Windows 7 bzw. 2008 gibt es bessere Treiber (WDDM), die leider nicht immer installiert werden. Schauen Sie nach dem Neustart im Gerätemanager nach und installieren Sie sie nachträglich. Die Treiber finden Sie unter <code>C:\Program Files\Common Files\VMware\Drivers</code> .
Audiotreiber	Treiber zur Bereitstellung von Ton für virtuelle Soundkarten	Soundkarten werden unter ESXi nicht unterstützt. Über RDP kann man sie aber nutzen (siehe VMware KB1004839). Nur für 64-Bit-OS und Windows ab Vista.
VMXNet-Netzwerk-kartentreiber	Treiber zur Verbesserung der Leistung der virtuellen Netzwerkkarte	Treiber für VMXNet2 (erweitert). Siehe Abbildung 4-6.
VMXNet3-Netzwerk-kartentreiber	Treiber zur Verbesserung der Leistung der virtuellen Netzwerkkarte (ndis5/6)	Treiber für VMXNet3. Siehe Tabelle 4-3 und VMware KB 1001805.
VSS-Unterstützung	VSS-Unterstützung für Windows-Gastbetriebssysteme	Ebenfalls für Backups und Snapshots. Damit gibt es allerdings manchmal Probleme wie das, dass keine Snapshots erstellt oder übernommen werden können. Bei Problemen sollten Sie diesen Treiber deinstallieren. (Erst ab Vista.)
VMCI-Treiber	Treiber, über den virtuelle Maschinen mit Anwendungen auf dem Host und mithilfe von Datagrammen und gemeinsam genutztem Speicher mit anderen virtuellen Maschinen kommunizieren können	Das <i>VMware Communication Interface</i> muss in den Einstellungen zur VM zusätzlich aktiviert werden. Einige Anwendungen unter Windows erlauben die schnelle Kommunikation über den RAM des ESXi Hosts mit bis zu 9 GBit/s.
Ordnerfreigaben	Ermöglicht die gemeinsame Nutzung von Dateien auf dieser virtuellen Maschine und dem Hostcomputer	Die Ordnerfreigaben funktionieren nur unter den Workstation- und Player-Versionen von VMware! Bei Terminalservern sollten sie nicht ausgewählt werden. Wenn Sie einen Terminalserver als virtuelle Maschine einrichten wollen, sollten Sie bei den VMware Tools die benutzerdefinierte Einstellung wählen und den Treiber für die Speichersteuerung sowie die Ordnerfreigaben deaktivieren, sonst kann es zu Problemen damit kommen.
Wyse Multimedia-Unterstützung	Treiber zur Verbesserung der Multimedialeistung auf dem Remote-Desktop	Dient nur bei Wyse-Stationen zur besseren Videoleistung und nur bei XP und 2003.
LSI	LSI PCI Fusion-MPT Miniport Driver	Treiber für LSIlogic SCSI-Adapter bei Windows XP
BootCamp	Treiber für Mac BootCamp	Nur bei Mac-Rechnern verfügbar.

Grafikbeschleunigung bei Microsoft-Servern

Bei Microsofts Serverbetriebssystemen ist die Hardwarebeschleunigung der Grafikkarte auf das Minimum eingestellt. Das sollten Sie wie folgt ändern:

- Klicken Sie mit der rechten Maustaste auf den Desktop und wählen Sie EIGENSCHAFTEN.
- Navigieren Sie zur letzten Registerkarte EINSTELLUNGEN und klicken Sie auf die Schaltfläche ERWEITERT.
- Wählen Sie die Registerkarte PROBLEMBEHANDLUNG und schieben Sie den Regler bei HARDWAREBESCHLEUNIGUNG ganz nach rechts.
- Schließen Sie die Fenster.

Treiberproblem bei Windows 7 und Server 2008

Ab Windows Vista, also auch bei Windows 7 und 2008, gibt es eine neue Grafikkarte mit Aero-Unterstützung (VMware SVGA 3D). Leider werden die Treiber nicht immer ordnungsgemäß installiert. Schauen Sie nach dem Neustart in den Gerätemanager und aktualisieren Sie ggf. den Treiber. Die notwendigen Dateien finden Sie unter *C:\Programme\Common Files\VMware\Drivers*. Wählen Sie möglichst die WDDM-Treiber oder lassen Sie Windows selbst in den Unterverzeichnissen suchen. Befinden sich die Dateien nicht in diesem Ordner, dann schauen Sie auf dem vCenter Server (2008 R2) im gleichen Pfad nach. Kopieren Sie die Verzeichnisse von hier oder einer anderen VM und versuchen Sie die Installation erneut.

Achten Sie darauf, dass Sie für die VM die Hardwareversion 7 oder 8 nutzen.



Die VMware Tools werden als CD-Image mitgeliefert und befinden sich im Verzeichnis */vmimages/tools* auf dem ESXi Server. Bei der Installation der Tools und Treiber wird das ISO-Image in der VM gemountet, und unter Microsoft-Betriebssystemen wird ein Autostart ausgeführt. Bei anderen OS (z.B. Linux) findet kein Autostart statt. Dort liegen die Tools als *tar.gz*-Datei vor und die Installation muss manuell durchgeführt werden. Beachten Sie unter Linux die Hinweise zum automatischen Starten der Tools nach dem Neustart der Maschine!

Sollten Sie feststellen, dass Maus und Tastatur in den virtuellen Maschinen für einige Sekunden nicht reagieren, wenn eine CD gewechselt wird, liegt das nicht an Ihnen, sondern an der Virtualisierungssoftware.

Nach dem Neustart der VM können Sie die Auflösung des Desktops anpassen, denn erst jetzt wird die Grafikkarte komplett unterstützt. Auch die Tastenkombination Strg+Alt

für den Fokus (also z.B. für den Mauszeiger) brauchen Sie jetzt nicht mehr zu drücken – das geschieht nun automatisch, wenn Sie das Fenster verlassen bzw. in es zurückkehren.

Wollen Sie eine VM vom VMware Server oder Workstation bzw. einer älteren Version von VMware ESX übernehmen, sollten Sie die VMware Tools in der aktuellen Version, sprich der des aktuellen Systems, installieren. Es ist übrigens kein Problem, wenn Ihre VMware ESX-Farm aus Servern verschiedener Versionen besteht. Installieren Sie einfach die VMware Tools der aktuellsten Version in den entsprechenden VMs, denn sie sind abwärtskompatibel.

VMware Tools anpassen

Wie bereits oben erwähnt, werden die Tools auf dem Gastbetriebssystem in der Ordnerstruktur installiert und beim Systemstart als Dienst bzw. Daemon mitgeladen. Unter Windows befinden sich insgesamt bis zu vier neue Dienste mit dem Starttyp AUTOMATISCH in der Auflistung. Falls das Icon des VMware Tools ausgeblendet wurde, findet man in der Systemsteuerung ein zusätzliches Icon, über das die Tools wieder erreichbar sind.

Nun kommen wir zu den Einstellungen, die man bei Bedarf verändern kann.

Zeitsynchronisierung zwischen Host und Gast

Möchten Sie die Zeit zwischen dem ESXi Server und den Gastbetriebssystemen synchronisieren (einmal pro Minute), sollten Sie zunächst den ESXi Server dafür einrichten, falls es noch nicht während der Installation geschehen ist.

Als IP-Adresse können Sie dann z.B. einen Zeitserver aus dem Internet angeben oder besser den PDC-Emulator der Active-Directory-Domäne.

Über die grafische Oberfläche erreichen Sie das, indem Sie auf den ESXi Server klicken, das Register KONFIGURATION auswählen und dann im Abschnitt SOFTWARE auf UHRZEITKONFIGURATION klicken. Rechts oben im Fenster sehen Sie den Link EIGENSCHAFTEN, dem Sie bitte anklicken.

Dann öffnet sich das Fenster aus Abbildung 4-16, in dem Sie über die Schaltfläche OPTIONEN und den Eintrag NTP-EINSTELLUNGEN einen NTP-Server hinzufügen können. Dabei wird der NTP-Port in der Firewall automatisch geöffnet. Anschließend sollten Sie den NTP-Dienst aktivieren (nicht neu starten!), indem Sie das Kästchen NTP-CLIENT AKTIVIERT auswählen und auf OK klicken.



Bedenken Sie, dass in einer Windows 2000-Domäne (oder neuer) der PDC-Emulator die Aufgabe der Zeitsynchronisierung für die gesamte Domäne übernimmt. Synchronisieren Sie alle Server und Clients auf jeden Fall mit der Domäne. Bei Rechnern, die nicht in regelmäßigen Abständen neu gestartet werden, sollten Sie gegebenenfalls einen geplanten Task z.B. als Batch-Datei hinterlegen, der die Zeit einmal pro Tag mit der Domäne synchronisiert:

```
net time /Domain /set /yes
```



Der VMware Tools-Dienst aktualisiert das Datum und die Uhrzeit im Gastbetriebssystem mit der Servicekonsole auch in Reaktion auf verschiedene Systemereignisse (beispielsweise beim Resume). Diese Option können Sie nur in der Konfigurationsdatei (.vmx) deaktivieren, indem Sie Folgendes einstellen:

```
time.synchronize.resume.disk = FALSE
```

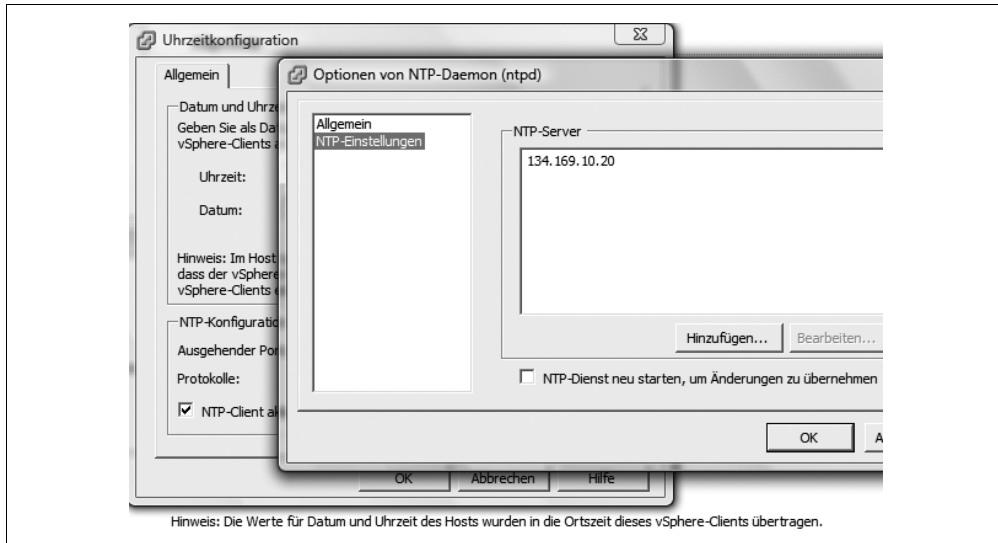


Abbildung 4-16: NTP-Einstellungen festlegen

Empfehlung zur Zeitsynchronisierung

Alle Domänenmitglieder müssen die Zeit vom PDC-Emulator haben. Bei der Anmeldung des Computers in der Domäne bekommt dieser ein Kerberosticket mit Datum und Uhrzeit, die er weiterführen muss. Weicht die Zeit mehr als fünf Minuten nach oben oder unten ab, verliert das Ticket seine Gültigkeit und die Zugriffsrechte sind obsolet. Auf dem Server geöffnete Dateien lassen sich beispielsweise nicht mehr dort sichern.

Der PDC-Emulator selbst sollte eine unabhängige Zeitquelle zur Synchronisierung haben – das kann eine Funkuhr, ein Internetdienst oder etwas Ähnliches sein.

Da jede VM beim Starten, Aufwecken aus dem Suspend-Modus etc. zunächst die Zeitinformationen des jeweiligen ESXi Servers erhält, sollten Sie diesen – wie oben beschrieben – ebenfalls mit dem zuständigen Domänencontroller per NTP abgleichen. Die komplette Synchronisation mit dem Host kann nur in der Konfigurationsdatei (.vmx) zur VM abgeschaltet werden. Ggf. müssen folgende Einträge ergänzt werden, wobei FALSE jeweils abschaltet und TRUE wieder einschaltet:

```
tools.syncTime = "FALSE"  
time.synchronize.continue = "FALSE"  
time.synchronize.restore = "FALSE"
```

```
time.synchronize.resume.disk = "FALSE"  
time.synchronize.shrink = "FALSE"  
time.synchronize.tools.startup = "FALSE"
```

Ist Ihre VM nicht in einer Domäne, können Sie bei den VMware Tools oder in den Einstellungen der VM die Zeitsynchronisierung mit dem ESXi Server aktivieren. Die Tools in der VM aktualisieren dann automatisch mit dem Host jede Minute einmal. Wollen Sie das für Windows-Gäste per Skript erledigen, können Sie das Programm *VMwareToolboxCmd.exe* im Verzeichnis *C:\Programme\VMware\VMware Tools* oder auch *C:\Program Files\VMware\VMware Tools* mit dem Parameter *timesync disable* abstellen bzw. mit *enable* aktivieren.



Beachten Sie bitte, dass lokale Dienste in der VM die Zeit genauer behandeln als der Agent von VMware. Dazu gehören *W32Time* unter Windows und *NTP* bei Linux. Auf gar keinen Fall sollten Sie mehr als einen Zeitdienst aktivieren.

Weitere Optionen

Auf dieser Registerkarte können Sie die VMware Tools in der Taskleiste anzeigen lassen oder diese Funktion abschalten und eine Benachrichtigung erhalten, wenn es neue Versionen der VMware Tools gibt. Das kann z.B. durch ein Update des ESXi Servers vorkommen. Um das Symbol wieder neben der Uhr anzeigen zu lassen, öffnen Sie die Systemsteuerung und klicken doppelt auf den Eintrag *VMWARE TOOLS*. Setzen Sie zum Anzeigen wieder das Häkchen.

Registerkarte »Geräte«

Auf der Registerkarte *GERÄTE* können Sie eine Liste aller entfernbaren Geräte (z.B. Disketten- und DVD-ROM-Laufwerke) anzeigen, die für die virtuelle Maschine verfügbar sind. Außerdem wird angezeigt, ob diese angeschlossen oder getrennt sind. Alle aufgelisteten Geräte können angeschlossen oder getrennt werden, indem das Häkchen gesetzt oder entfernt wird. Diese Option ist nicht immer verfügbar.

Hierbei haben Sie auch die Möglichkeit, die Netzwerkkarte kurzfristig vom LAN zu trennen. Wenn Sie das Häkchen herausnehmen und auf *ÜBERNEHMEN* klicken, zeigt der Gast *NETZWERKKABEL NICHT ANGESCHLOSSEN* an. Übrigens: Mit Remote-Desktop sollten Sie das nicht versuchen.

Registerkarte »Skripts«

Über die VMware Tools können Sie bei Änderungen des Betriebsstatus der virtuellen Maschine (d.h. beim Einschalten, Ausschalten, Anhalten oder Fortsetzen der virtuellen Maschine) Skripten ausführen lassen. Es ist jeweils ein Standardskript für jede Betriebsstatusänderung vorgesehen. Diese Skripten befinden sich beim Windows-Gastbetriebssystem unter *C:\Programme\VMware\VMware Tools* und sind in Tabelle 4-2 aufgeführt.

Tabelle 4-2: Skripten für die VMware Tools

Aufgabe	Standardskript
Anhalten des Gastbetriebssystems	<i>suspend-vm-default.bat</i>
Wiederaufnehmen des Gastbetriebssystems	<i>resume-vm-default.bat</i>
Herunterfahren des Gastbetriebssystems	<i>poweroff-vm-default.bat</i>
Einschalten des Gastbetriebssystems	<i>poweron-vm-default.bat</i>

Wenn Sie ein anderes Skript als Standardskript verwenden möchten, klicken Sie in dem Fenster, das in Abbildung 4-17 dargestellt ist, auf BENUTZERDEFINIERTES SKRIPT und dann auf DURCHSUCHEN und wählen Ihr eigenes aus.

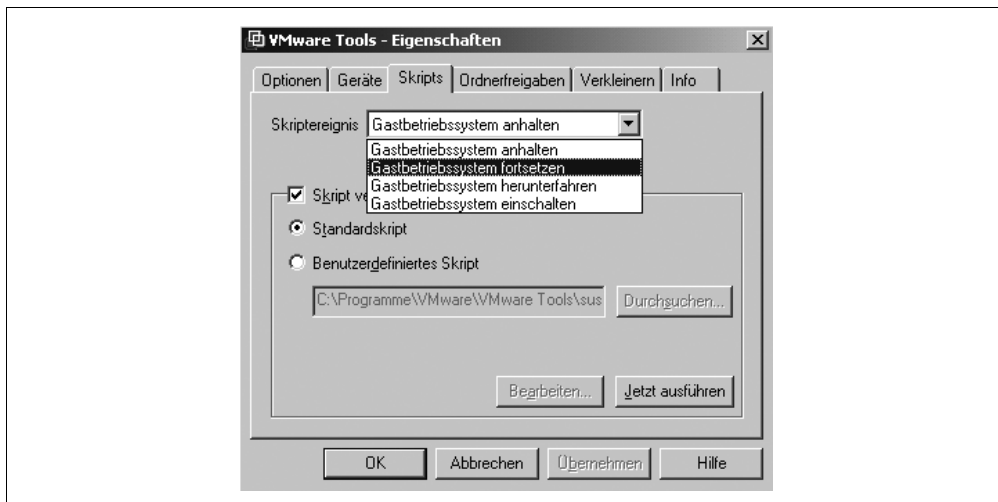


Abbildung 4-17: Skripten der VMware Tools

Anschließend können Sie es bearbeiten oder ausführen, um es zu testen.

1. Zum Bearbeiten klicken Sie auf die gleichnamige Schaltfläche, damit das Skript in Ihrem Standardeditor geöffnet wird. Nehmen Sie dort alle notwendigen Änderungen vor.
2. Klicken Sie zum Testen auf JETZT AUSFÜHREN.
3. Um die Ausführung der Skripten zu verhindern, deaktivieren Sie das jeweilige Kontrollkästchen bei SKRIPT VERWENDEN.
4. Klicken Sie auf ÜBERNEHMEN, um Ihre Einstellungen zu speichern.



Die Standardskripten werden beim Update der Tools überschrieben. Sie sollten sich also besser Ihre eigenen Batch-Dateien anlegen.



Die Standardskripten für Suspend und Resume beinhalten jeweils einen Befehl für die Netzwerkkonfiguration. Beim Suspend werden die vom DHCP-Server erhaltenen Adressinformationen zurückgegeben, und beim Resume wird eine neue Adresse angefordert. Meistens ist das in einer produktiven Umgebung nicht gewollt.

Registerkarte »Verkleinern«

Über die Einstellungen auf dieser Karte können Daten, die sich auf der Festplatte der VM befinden, in den vorderen Teil geschoben werden, damit hinterher eine dynamisch angelegte Festplattendatei verkleinert werden kann. Unter ESXi können die *.vmdk*-Dateien abhängig vom Gastbetriebssystem nur vorbereitet werden, um hinterher z.B. einen kleineren Export zu erhalten. Auch diese Option steht nicht immer zur Verfügung.

Registerkarte »Info«

Die Registerkarte INFO enthält u.a. Informationen über VMware Tools, z.B. die Version und die Build-Nummer (die übrigens mit der angezeigten Nummer des ESXi Servers in etwa übereinstimmen sollten).

Eine neue Funktion befindet sich in der VM unter START → PROGRAMME → VMWARE: Dort können Sie sich die Statistikprotokollierung der virtuellen Maschine ansehen. Die Darstellung erinnert stark an das Perfmancetool von Microsoft.

Automatische Upgrades für VMware Tools

Ab dem ESX Server 3.0.1 können VMware Tools und virtuelle Hardware gleichzeitig für mehrere virtuelle Maschinen aufgerüstet werden, ohne von der Konsole für die virtuelle Maschine aus mit dieser kommunizieren zu müssen. Diese Funktion ermöglicht Upgrades von früheren Releases von VMware Tools und virtueller Hardware für eine oder mehrere virtuelle Maschinen. Der Anwender, der das Upgrade ausführt, muss über die entsprechende Berechtigung verfügen.

Für Massenumgrades von VMware Tools gelten folgende Einschränkungen:

- Es können nur virtuelle Maschinen aufgerüstet werden, die vom vCenter Server 2.0.1 oder höher verwaltet werden.
- Massen-Upgrades sind nur für Linux und Microsoft Windows 2000 und höher verfügbar.
- FreeBSD, Netware und Windows NT werden nicht unterstützt.
- Bei der virtuellen Festplatte muss es sich um eine Datei auf einem VMFS-3- oder -5-Volume handeln.
- Virtuelle Maschinen müssen ausgeschaltet sein.

Vorgehensweise:

- Öffnen Sie das »Eigenschaften Dialogfeld« für die zu aktualisierende virtuelle Maschine.
- Wählen Sie OPTIONEN → VMWARE TOOLS.
- Wählen Sie unter ERWEITERT die Option TOOLS VOR JEDEM EINSCHALTVORGANG PRÜFEN UND AKTUALISIEREN.
- Klicken Sie auf OK.

Beim nächsten Einschalten der virtuellen Maschine wird eine Überprüfung auf eine neuere Version der VMware Tools durchgeführt. Wenn eine neuere Version auf dem ESXi Server vorhanden ist, wird diese installiert und das Gastbetriebssystem bei Bedarf neu gestartet. Überlegen Sie sich bitte vor der Änderung, wie sinnvoll diese Vorgehensweise für produktive Systeme ist.

Unbeaufsichtigte Installation der Tools

Wie ich oben in Tabelle 4-1 detailliert beschrieben habe, gibt es bei der einen oder anderen virtuellen Maschine Komponenten in den VMware Tools, die zu Problemen führen können. Auch wenn Sie für eine Menge von VMs während deren Benutzung ein Upgrade planen, soll der PC vielleicht nicht sofort neu gestartet werden oder der User soll von einer im Hintergrund ablaufenden Installation erst gar nichts mitbekommen. Für diese Zwecke können Sie die in der ISO-Datei vorhandene Datei *setup.exe* (32 oder 64 Bit) nehmen und eine administrative Installation der Tools erwirken. Damit bekommen Sie ein MSI-Paket, das über den Windows Installer genutzt werden kann.

Die jeweiligen Komponenten, die als Parameter ausgeschlossen werden sollen, finden Sie z.B. bei einer Testmaschine mit bereits installierten Tools durch folgenden Befehl:

```
D:\Setup.exe /s /v"/qn /1*v ""C:\vmtools.log""
```

Dabei passiert Folgendes:

- D:\ wird als CD/DVD-Laufwerk angenommen.
- /s blendet den Initialisierungsdialog aus.
- /v bietet zusätzliche Parameter für *setup.exe*
- /qn bedeutet keine Meldungen oder Fenster auf der Oberfläche.
- /1* gibt den Pfad und die Datei für das Loggen an.
- /v ist der ausführliche Logmodus.

In der dann erstellten Logdatei suchen Sie nach SetNO_UNINSTALL_ und finden dann unter anderem Werte wie diese:

AUDIO, AUDIO2008, BUSLOGIC, HGFS, MEMCTL, MOUSE usw.

Die meisten Einträge sind selbsterklärend. Bei HGFS handelt es sich um die Ordnerfreigaben, BUSLOGIC ist für den SCSI-Treiber und MEMCTL für den Speichertreiber.

Um eine Anpassung für die Installation nutzen zu können, empfiehlt sich eine Freigabe auf einem Rechner, auf den die VMs zugreifen können. Darin können Sie eine administrative Installation erwirken und bekommen somit die MSI-Datei. Geben Sie z.B. folgenden Befehl bei Ihrer Testmaschine ein:

```
D:\Setup.exe /a "C:\Freigabe"
```

Um *Setup64.exe* aufrufen zu können, brauchen Sie ein 64-Bit-Windows. In der Freigabe bereits vorhandene Dateien bleiben dabei erhalten. Nun können Sie mit der Installation verschiedene Werte übergeben. Wollen Sie z.B. alle Komponenten installieren und nur die Ordnerfreigaben (unter vSphere nicht empfohlen) und den BusLogic-Treiber (nicht empfohlen, wenn LSI genutzt wird) herausnehmen, sähe der Aufruf so aus:

```
msiexec /i ""\\Server\Freigabe\VMware Tools.msi" ADDLOCAL=ALL REMOVE=Hgfs,Buslogic /qn /l* "C:\vmtools.log" /norestart"
```

Dabei steht alles in einer Zeile, die Sie auch als BAT- oder CMD-Datei ausführen können. Groß- und Kleinschreibung muss beachtet werden.

Noch einfacher geht es über die Liste der virtuellen Maschinen. Klicken Sie die erste VM in der Liste an, halten Sie die Strg-Taste gedrückt und wählen Sie dann alle VMs aus, die Sie aktualisieren wollen. Klicken Sie dann mit der rechten Maustaste auf Ihre Auswahl und wählen Sie aus dem Kontextmenü GAST → VMWARE TOOLS INSTALLIEREN/AKTUALISIEREN aus. Im folgenden Fenster (siehe Abbildung 4-18) können Sie für das Setupprogramm die Startparameter unter ERWEITERTE OPTIONEN mit angeben.



Abbildung 4-18: VMware Tools aktualisieren

Änderungen bei den VMware Tools unter Windows können problemlos über die grafische Oberfläche erledigt werden – bei Linux geht das häufig nur über die Kommandozeile. Möchten Sie beispielsweise die Ordnerfreigaben unter Linux deinstallieren, so gehen Sie auf der Kommandozeile zu dem Ordner, in dem Sie die tar.gz-Datei entpackt haben. Rufen Sie das Perl-Skript mit folgenden Parametern auf:

```
vmware-install.pl --clobber-kernel-modules=vmhgfs
```

Möchten Sie die Treiber für den vmxnet3-Adapter de- und dann neu installieren, funktioniert das mit folgendem Aufruf:

```
vmware-install.pl --clobber-kernel-modules=vmxnet3
```

Dem Skript können auch mehrere Parameter mit Komma getrennt übergeben werden:

```
vmware-install.pl --clobber-kernel-modules=pvscsi,vmblock,vmci, vmhgfs,vsock,vmxnet,vmxnet3
```

Um alle Pfadangaben automatisch zu bestätigen, kann -d mit angegeben werden.

VMware hat noch andere Methoden parat, um die Installation für Linux-Betriebssysteme einfacher zu machen. Auf deren Website findet sich eine Beschreibung für die Installation von »Operating System Specific Packages« unter folgender URL: <http://packages.vmware.com/tools/docs/manuals/osp-esxi-50-install-guide.pdf>. Die Pakete kann man sich unter <http://www.vmware.com/download/packages.html> herunterladen.

Manuelle Änderung der VMware Tools

Änderungen bei den VMware Tools unter Windows können problemlos über die grafische Oberfläche erledigt werden – bei Linux geht das nur über die Kommandozeile. Möchten Sie beispielsweise die Ordnerfreigaben unter Linux deinstallieren, so gehen Sie auf der Kommandozeile zu dem Ordner, in dem Sie die tar.gz-Datei entpackt haben. Rufen Sie das Perl-Skript mit folgenden Parametern auf: *vmware-install.pl --clobber-kernel-modules=vmhgfs*. Möchten Sie die Treiber für den *vmxnet3*-Adapter de- und dann neu installieren, funktioniert das mit folgendem Aufruf: *vmware-install.pl --clobber-kernel-modules=vmxnet3*. Dem Skript können auch mehrere Parameter mit Komma getrennt übergeben werden: *vmware-install.pl --clobber-kernel-modules=pvscsi,vmblock,vmci,vmhgfs,vsock,vmxnet,vmxnet3*. Um alle Pfadangaben automatisch zu bestätigen kann »-d« mit angegeben werden. VMware hat noch andere Methoden parat, um die Installation für Linux-Betriebssysteme einfacher zu machen. Auf deren Webseite findet sich eine Beschreibung für die Installation von »Operating System Specific Packages« unter folgender URL: <http://packages.vmware.com/tools/docs/manuals/osp-esxi-50-install-guide.pdf>. Die Pakete kann man sich unter <http://www.vmware.com/download/packages.html> herunterladen.

Virtuelle Maschinen optimieren

Über die Methoden und Faktoren, die die virtuelle Infrastruktur zur Verbesserung der Performance zur Verfügung stellt, erfahren Sie mehr in den Kapiteln 10 und 18. Innerhalb

der virtuellen Maschine kann aber ebenfalls einiges erreicht werden, um die Ressourcen besser verteilen zu können.

Optimierung über den vSphere Client

Ob man mit dem vSphere Client auf den ESXi Server-Host oder den vCenter Server zugreift, ist bei den folgenden Optimierungen egal. Beachten Sie zunächst folgende Faktoren:

- Stellen Sie bei der Erstellung virtueller Maschinen sicher, ihre Größe – genau wie bei physischen Maschinen – dem tatsächlichen Bedarf anzupassen. Überkonfigurierte virtuelle Maschinen verschwenden gemeinsam nutzbare Ressourcen.
- Deaktivieren Sie zugunsten der besseren Performance sämtliche nicht verwendeten Geräte wie COM-Ports, LPT-Ports, Diskettenlaufwerke, CD-ROMs, USB-Adapter usw. Diese Geräte werden nämlich auch dann regelmäßig vom (Windows-)Gastbetriebssystem abgefragt, wenn sie nicht verwendet werden. Durch dieses unproduktive Abfragen werden gemeinsam nutzbare CPU- und RAM-Ressourcen verschwendet. Entfernen Sie die nicht benötigten Geräte gegebenenfalls auch im BIOS der VM.
- Installieren Sie die VMware Tools. Sie unterstützen Sie beim Erreichen einer besseren Performance, können zu einer effizienteren CPU- und RAM-Nutzung führen und enthalten Treiber zum Abrufen von Festplatten-, Netzwerk- und Speicherressourcen.

Optimierung innerhalb der VM

Optimieren Sie – genau wie beim physikalischen System – das Betriebssystem der virtuellen Maschine durch Register, Swap-Bereiche usw. und passen Sie die Größe an. Deaktivieren Sie unnötige Programme und Dienste wie Bildschirmschoner und optischen Schnickschnack. Unnötige Programme und Dienste verschwenden gemeinsam nutzbare Ressourcen. Aktualisieren Sie das Gastbetriebssystem stets durch aktuelle Patches und Servicepacks. Falls Sie als Gastbetriebssystem Microsoft Windows verwenden, überprüfen Sie, ob es in der Wissensbasis von Microsoft Artikel über bekannte Probleme mit dem Betriebssystem gibt.

Beobachten Sie den Graphen für den Host, den Ressourcenpool bzw. den Cluster, wie in Abbildung 4-19 beispielhaft gezeigt ist. Stellen Sie diesen gegebenenfalls auf eine andere Ansicht um oder exportieren Sie die Daten nach Excel, um eine Langzeitübersicht zu bekommen. Der Host speichert die Daten nur für einen Tag, während der vCenter Server eine Datenbank dafür hat, in der die Daten für Monate und Jahre erhalten bleiben können.



Beachten Sie auch, dass sich auf der linken Seite die Prozentzahlen auf den Graphen beziehen und nicht auf die Gesamtkapazität! Bewegen Sie den Mauszeiger über die dargestellten Linien, um die tatsächliche Last zu sehen (siehe Abbildung 4-20).

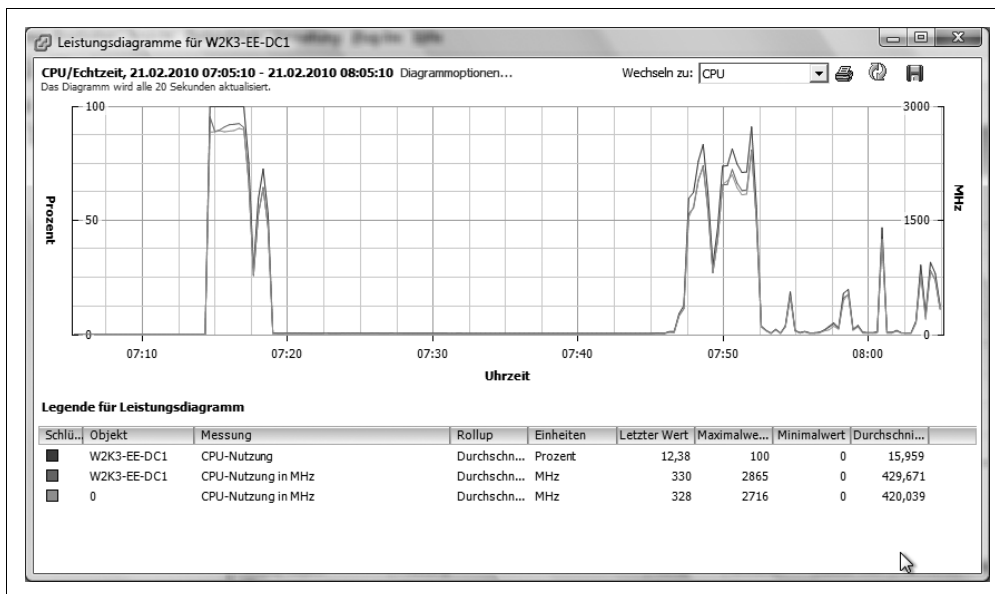


Abbildung 4-19: Leistungsdiagramm der VM

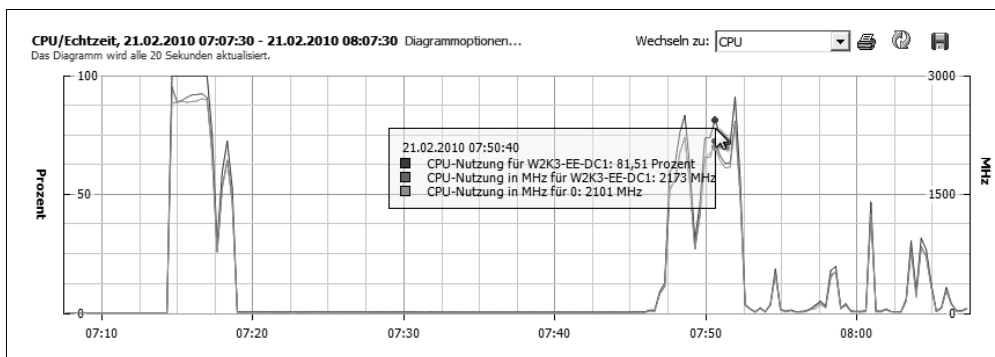


Abbildung 4-20: Diagrammskalen interpretieren

Empfehlung für VM-Optimierung

Hier noch einmal gebündelt die wichtigsten Optimierungsmöglichkeiten für die virtuelle Maschine:

- VM-Hardwareeinstellungen
 - Floppylaufwerk in den Einstellungen und im BIOS der VM entfernen
 - CD/DVD nicht verbunden, noch besser: Clientgerät
 - Grafikkarte der VM auf *Einstellungen automatisch erkennen* setzen

- VM-Ressourcen
 - CPU-Reservierungen vermeiden
 - CPU-Grenzwerte nur bei DOS oder NetWare einschalten
 - RAM-Reservierungen vermeiden
 - RAM-Grenzwerte nicht einstellen, das Häkchen bei *Unbegrenzt* muss gesetzt bleiben
 - Festplattengrenzwert: IOPs nur im Notfall etwas eintragen
- VM-BIOS
 - Legacy-Diskette A/B: *disabled*
 - Floppy disk controller: *disabled*
 - LPT und COM: *disabled*
 - Local Bus IDE Adapter: nur primary oder secondary, je nach Anschluss des CD/DVD-Laufwerks
 - Boot von HD
- VM-Betriebssystem (Beispiel Windows)
 - Anzeigeauflösung nur 16-Bit-Farben
 - Hardwarebeschleunigung der Grafikkarte auf Maximum
 - kein Hintergrundbild
 - Bildschirmschoner aus oder nur schwarz
 - Darstellung für optimale Performance
 - unnötige Dienste abschalten
 - Autostart und Registry-RUN-Zweige überprüfen

Vermeiden Sie aus Performancegründen – wenn möglich – die »Thin-Bereitstellung« bei Festplatten und lassen Sie Snapshots nur so lange wie eben nötig anwachsen.

Das sind allgemein gefasste Empfehlungen. Wenn Sie in der VM beispielsweise ein Diskettenlaufwerk oder einen LPT-/COM-Anschluss benötigen, schalten Sie diesen natürlich nicht ab.



Nach der Konvertierung einer physikalischen in eine virtuelle Maschine sollten Sie die nicht mehr vorhandene Hardware nach der Installation der VMware Tools deinstallieren. Geben Sie in einer DOS-Box unter Windows Folgendes ein:

```
set devmgr_show_nonpresent_devices=1
devmgmt.msc
```

Schalten Sie anschließend unter ANSICHT die ausgeblendeten Geräte ein und deinstallieren Sie die nicht mehr vorhandenen (grau dargestellten) – mit Ausnahme des RAS-Adapters und des gesamten Zweigs NICHT-PNP-GERÄTE.



Mit dem kostenlosen Tool *bginfo* von Bryce Cogswell (ehemals Sysinternals, jetzt Microsoft) können Sie auf einem Windows-Betriebssystem Einstellungen wie den Namen der Maschine, den angemeldeten Benutzer, die IP-Adresse usw. auf dem Desktop anzeigen lassen, wie in Abbildung 4-21 gezeigt ist. Sie finden dieses nützliche Tool auch auf der Website zum Buch.

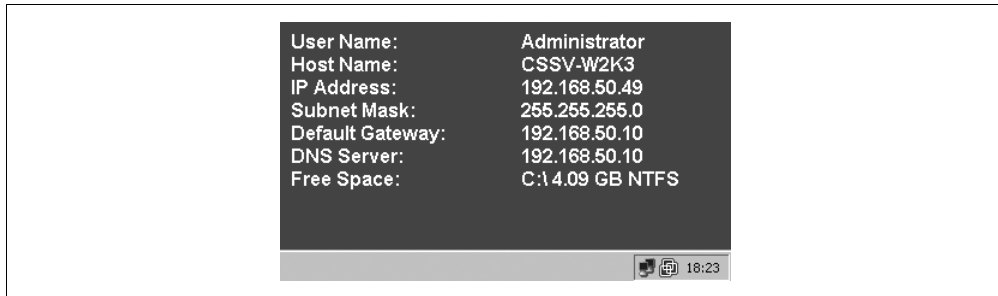


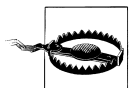
Abbildung 4-21: Anzeige über *bginfo*

Gasthardware ändern

Auch wenn eine virtuelle Maschine über längere Zeit problemlos läuft, kann es vorkommen, dass nach der Installation einer neuen Anwendung zu wenig Hauptspeicher vorhanden ist. Oder die Festplatte wurde bei der Erstellung zu klein gewählt, ein anderes DVD-Laufwerk muss verbunden werden, usw.

Über den VMware vSphere Client können Sie das auf einem einzelnen ESXi Server oder über den vCenter Server erledigen. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine und wählen Sie aus dem Kontextmenü **EINSTELLUNGEN BEARBEITEN** aus. Das ist nur eine Möglichkeit, um zu dem in Abbildung 4-22 gezeigten Fenster zu kommen.

In dieser Ansicht können Sie dann über **HINZUFÜGEN** neue Hardware hinzufügen, über den Button **ENTFERNEN** etwas löschen oder die Konfiguration der einzelnen Geräte in der rechten Fensterhälfte ändern.



Die virtuelle Maschine muss für die meisten Hardwareänderungen ausgeschaltet sein, nur Änderungen wie der Inhalt der CD-/DVD-ROM- und Diskettenlaufwerke, aber auch der aktive Netzwerkanschluss können während der Laufzeit angepasst werden.



VMware unterstützt das Hinzufügen von RAM und das Ändern der CPU-Anzahl im Betrieb (**OPTIONEN** → **SPEICHER** → **CPU-HOTPLUG**), jedoch nicht alle Gastbetriebssysteme! Gegebenenfalls steht diese Möglichkeit nur zur Verfügung, wenn Sie sie zur VM unter **OPTIONEN** extra eingestellt haben.

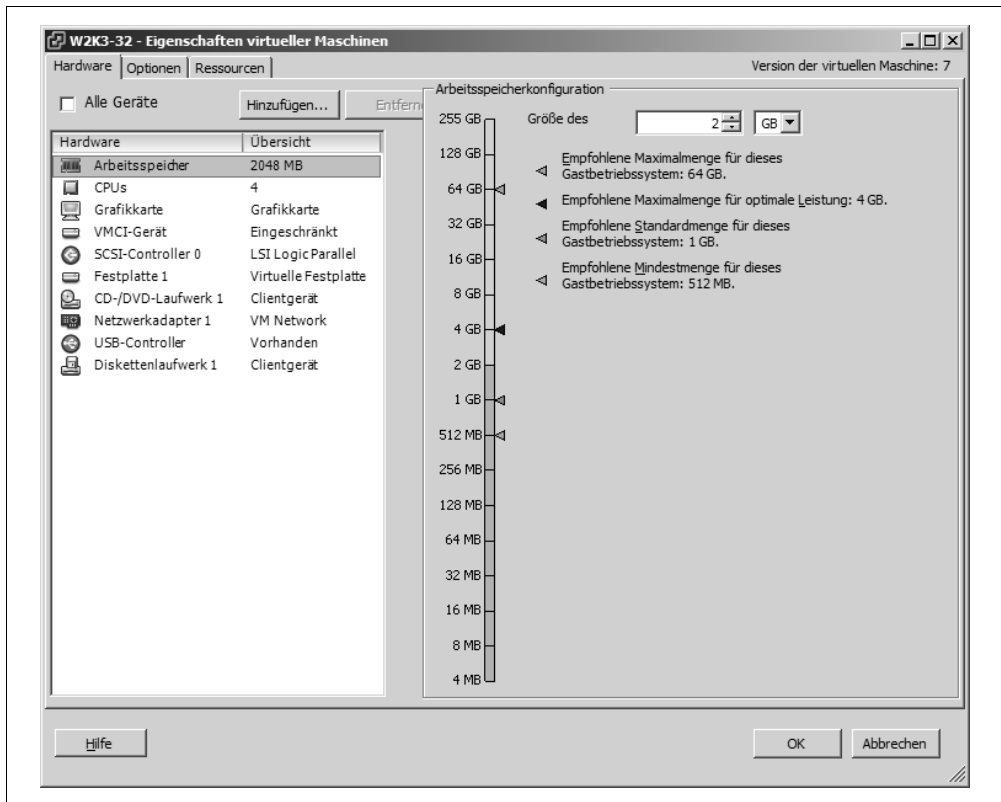


Abbildung 4-22: Gasthardware ändern

Alle Änderungen, die hier vorgenommen werden können, spreche ich hier nochmals an. Dabei werde ich auch Optionen erwähnen, die nicht bei jeder VM auftauchen. Je nach gewähltem Betriebssystem werden bestimmte Geräte und Auswahlmöglichkeiten angezeigt oder eben nicht.

Arbeitsspeicher

Die am häufigsten vorkommende Konfigurationsänderung innerhalb Ihrer virtuellen Maschinen wird wohl den Arbeitsspeicher betreffen.

Die virtuelle Maschine muss meistens heruntergefahren sein, um diese Änderung durchführen zu können. Danach klicken Sie auf **EINSTELLUNGEN BEARBEITEN** und dann auf **ARBEITSSPEICHER** (siehe Abbildung 4-23) und können dort einfach die Menge des zugewiesenen Hauptspeichers anpassen.

Je nach ausgewähltem Betriebssystem werden die farbigen Dreiecke unterschiedlich positioniert – links die Einstellungen zu Windows XP 32 Bit, rechts zu Windows 2003 Enterprise Edition.



Die maximale Menge an Arbeitsspeicher für die virtuellen Maschinen hängt nicht vom tatsächlichen physischen RAM des Hosts ab. Was dieser nicht zur Verfügung stellen kann, wird als Auslagerungsdatei im Verzeichnis der virtuellen Maschine genutzt. Die Erfahrungen aus der Praxis haben gezeigt, dass eine VM deutlich langsamer wird, wenn RAM ausgelagert werden muss.



Beim Einschalten der VM wird immer eine Auslagerungsdatei in der Größe des zugewiesenen RAMs angelegt (.vswp-Datei). Berücksichtigen Sie das auch bei der Größe des zur Verfügung stehenden Volumes.

Wenn Sie eine VM noch in der Hardwareversion 4 oder 7 haben, können Sie dieser maximal 255 GByte RAM geben. Erst ab der Version 8 sind 1.011 GByte RAM auswählbar.

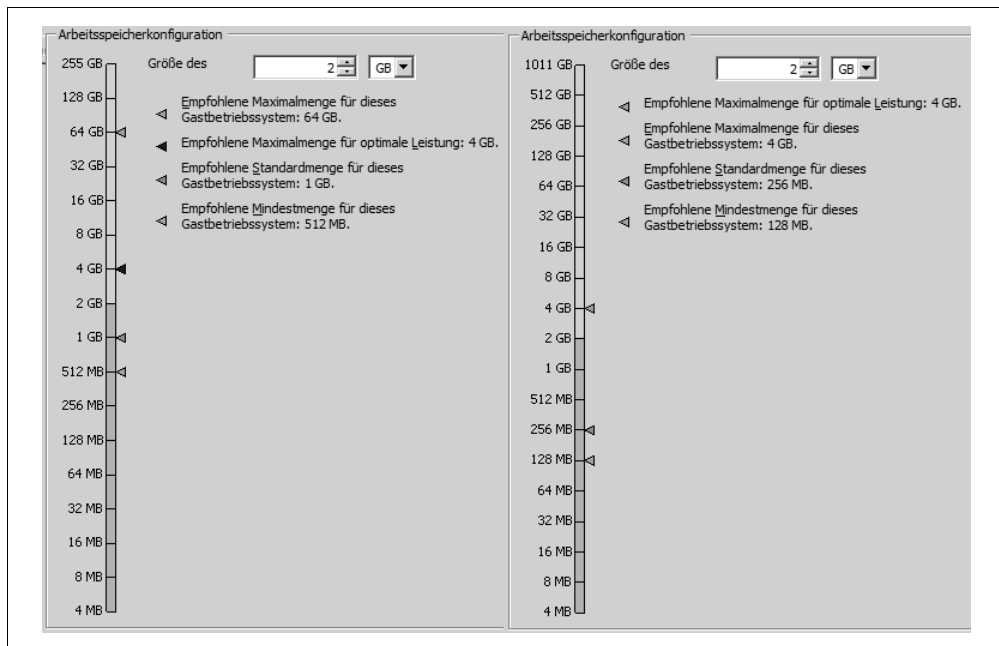


Abbildung 4-23: Vergleich des RAMs verschiedener Betriebssysteme

Anzahl der Prozessoren

Zu Sinn und Unsinn von Mehrprozessormaschinen habe ich schon ein paar Worte gesagt, als es um die Erstellung der ersten Maschine ging. Beachten Sie auch die Hinweise von VMware bei der Änderung dieses Punkts (siehe Abbildung 4-24).

Die Seite ANZAHL DER VIRTUELLEN CPUS wird nicht angezeigt, wenn der Server nur einen einzelnen Prozessor besitzt oder das Gastbetriebssystem SMP (*Symmetrisches Multiprocessing*) nicht unterstützt (z. B. NetWare und Windows NT 4.0).

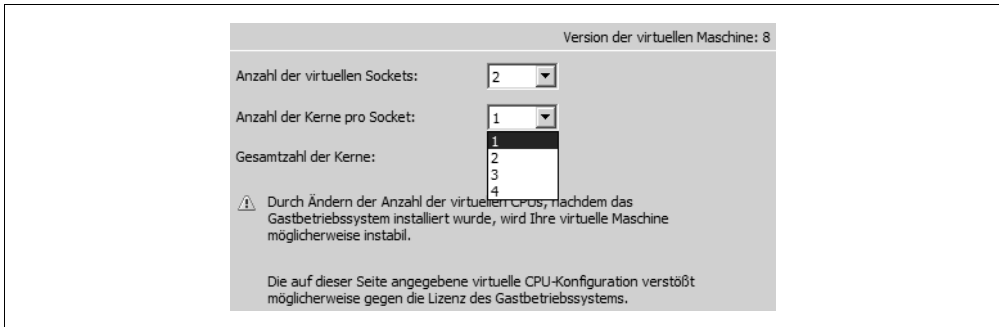


Abbildung 4-24: Auswahl der Prozessoranzahl

Falls Sie sich hier nicht entscheiden können, bedenken Sie Folgendes: Bei den meisten Betriebssystemen ist es einfacher, nachträglich Prozessoren wegzunehmen, als von einem auf mehrere CPUs zu erhöhen. Gerade bei Windows ist diese Vorgehensweise ratsam, weil es besser mit einer CPU auf einer installierten Mehrprozessor-HAL (*Hardware Abstraction Layer*) zurechtkommt als umgekehrt.

Wenn Sie später eine Anwendung innerhalb der VM installieren, die mehrere Prozessoren unterstützt, wählen Sie bei diesem Schritt besser mehrere CPUs. Braucht Ihre Software nur einen Prozessor, nehmen Sie hier nur einen. Möchten Sie eine Vorlage (Template) generieren, nehmen Sie besser zwei Prozessoren. Wie bereits oben erwähnt, ist es hinterher einfacher, auf einen, vier oder gar 32 Prozessoren umzustellen.

Da viele Anwendungen und teilweise auch Betriebssysteme nach den Prozessoren lizenziert werden, haben Sie hier sehr schön die Möglichkeit, nur einen Prozessor zu nutzen, der aber 16 oder mehr Kerne hat. Von der Geschwindigkeit her werden Sie den Unterschied nicht merken.



Die maximale Menge an CPUs für die virtuelle Maschine hängt nicht nur vom Host ab. VMware reduziert die Möglichkeit der CPU-Anzahl auch je nach ausgewähltem Betriebssystem bei Anzahl der Sockel und Kerne.

Grafikkarteneinstellungen

Seit Version 4.0 des ESXi Servers ist es (theoretisch) möglich, für die virtuelle Maschine mehrere Monitore (bis zu zehn bei 4.0, keine bei 4.1, maximal vier bei 5.0) zu übergeben. Der notwendige Arbeitsspeicher ist dabei aber nicht zwingend zehnmal größer als für eine Anzeige. Sie können dafür maximal 128 MByte zur Verfügung stellen. Die physische Grafikkarte des Hosts spielt dabei keine Rolle. Sehr schön ist der »Videoarbeitsspeicher-Rechner«, der die gewählte Auflösung, Bittiefe und Anzahl der Anzeigen direkt in das Feld »Gesamtmenge an Videoarbeitsspeicher« übernimmt. Bei manchen Betriebssystemen ist das Kästchen für die 3-D-Unterstützung anwählbar, z.B. bei Windows 7 und 8 (32 und 64 Bit).

Das Problem der Vorgängerversionen erscheint zunächst gelöst zu sein: Nach dem Start der VM können Sie in den Eigenschaften der Anzeige tatsächlich einen bis drei weitere Monitore sehen. Leider lassen sie sich nicht aktivieren oder über den vSphere Client anzeigen!

Möchten Sie trotzdem mehrere Monitore in der VM haben, können Sie das Problem mit der Remote-Desktop-Verbindung (*mstsc*) umgehen – vorausgesetzt, Sie haben zwei oder mehr Monitore mit der gleichen Auflösung:

1. Überprüfen Sie die Version Ihres RDC (*Remote Desktop Client*), indem Sie START → AUSFÜHREN → MSTSC wählen und in der oberen linken Ecke mit der Maus auf den kleinen Monitor klicken.
2. Wählen Sie INFO aus. Sie benötigen die Version 6.0 oder höher.
3. Gehen Sie erneut auf START → AUSFÜHREN und geben Sie *mstsc /span* ein.
4. Geben Sie den Namen Ihrer VM ein und melden Sie sich an.

Die maximale Auflösung beträgt dabei 4.096 x 2.048 Punkte, es geht nur horizontal, und der Desktop der VM überlagert dann beide physischen Monitore. Das bedeutet, dass auf dem linken Monitor der Start-Button ist und auf dem rechten die Uhr.



Nur wenn der Video-RAM auf AUTOMATISCH eingestellt ist, können Sie die Gestauföslung an die FenstergröÖe angleichen. Die automatische GröÖÖen Anpassung des Fensters funktioniert leider in vielen Fällen sonst nicht.

VMCI-Gerät

Einige Betriebssysteme unterstützen das *VMware-Kommunikations-Interface* (VMCI). Darüber können sich die konfigurierten Maschinen mit dem und über den Hypervisor direkt unterhalten, z.B. um Daten austauschen. Voraussetzung ist, dass die VMs auf demselben ESXi Server laufen. Beachten Sie aber bitte den Hinweis von VMware bezüglich der Sicherheit (siehe Abbildung 4-25).

⚠ Um die größtmögliche Sicherheit zu wahren, aktivieren Sie nur dann VMCI zwischen VMs, wenn dies unbedingt erforderlich ist.

Abbildung 4-25: VMCI einschalten

Seit der Workstation-Version 6 von VMware wird ein SDK (*Software Development Kit*) unterstützt, das die Kommunikation ermöglicht. Die dabei zu erreichende Geschwindigkeit liegt laut Hersteller bei bis zu 10 GBit/s, wobei eine Unterhaltung über das Netzwerk mit der Netzwerkkarte *vmxnet3* schon über 2 GBit/s liefern kann.

Laufwerke

Sowohl DVD-/CD-ROM- als auch Diskettenlaufwerke unterstützen die physischen Laufwerke des Hosts, aber auch Imagedateien (ISO/FLP), mit denen Sie besser arbeiten soll-

ten. Diese Imagedateien sollten aber lokal auf dem ESXi Server (VMFS-Dateisystem) oder im SAN liegen. Alle virtuellen Maschinen teilen sich die Geräte, und alle können z.B. eine einliegende CD-ROM sehen und darauf zugreifen. Der Geschwindigkeitsvorteil von Imagedateien ist enorm, da sie auf der physikalischen Festplatte des Wirtsystems oder im SAN liegen und damit eine deutlich bessere Zugriffszeit haben als ein CD-ROM- oder Diskettenlaufwerk. Weiterhin ist die Handhabung deutlich komfortabler, da Sie die Image-datei einfach während des Betriebs der virtuellen Maschine austauschen können. Die DVD-/CD-ROM-Images sind immer im ISO-Format anzulegen, die Diskettenlaufwerke arbeiten mit dem FLP-Format.

Auch das optische Laufwerk der Station, über die man sich angemeldet hat, kann für den Datenaustausch verwendet werden (siehe Abbildung 4-26).

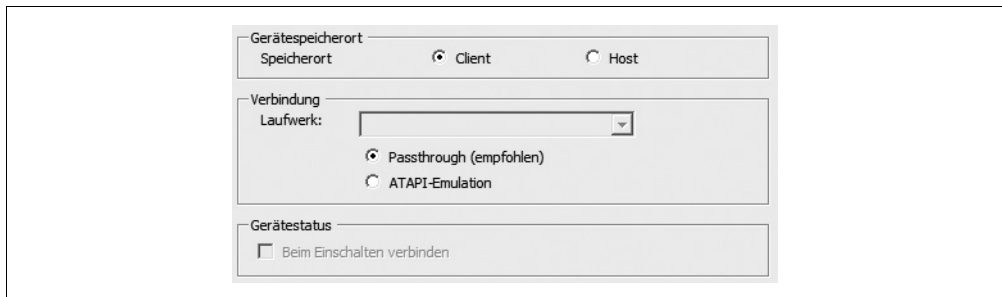


Abbildung 4-26: Auswahl des optischen Laufwerks



Sie sollten Autorun unter Microsoft Windows-Gastsystemen deaktivieren und das optische und Diskettenlaufwerk nur dann mit der virtuellen Maschine verbinden, wenn es wirklich notwendig ist. Wird bei aktiviertem Autorun eine Scheibe ins Laufwerk gelegt, läuft sie im schlimmsten Fall bei allen virtuellen Maschinen gleichzeitig an. Wie bereits oben unter »Performance« erwähnt, sollte man die verbundenen Laufwerke innerhalb der virtuellen Maschine trennen, da bei einem Neustart die Maschine unter Umständen stehen bleibt und auf dem Medium nach dem Bootsektor sucht.

Beim Diskettenlaufwerk haben Sie ebenfalls die Möglichkeit, eine neue Floppydatei im Storage des Hosts zu erstellen und gegebenenfalls Treiber darauf zu platzieren, um diese dann später einer anderen Maschine zur Verfügung zu stellen.

SCSI-Controller

Wenn Sie ein Sharing einer SCSI-Platte benötigen, um z.B. eine *Quorumfestplatte* anzuhängen, können Sie hier für die gemeinsame Verwendung des SCSI-Busses sorgen. Ich empfehle, den beteiligten VMs lieber einen neuen Adapter hinzuzufügen, als den Adapter der Bootplatte zu verwenden. Beachten Sie dabei, dass je nach Auswahl alle beteiligten Maschinen auf dem gleichen Host laufen müssen. Möchten Sie aber ein Cluster aus virtu-

ellen und physischen Maschinen erstellen, müssen Sie RDM (*Raw Device Mapping*) verwenden.

Festplattengröße und -modus

Bei Festplatten kann nicht nur die Größe nachträglich geändert werden, es können auch zwei verschiedene Modi gesetzt werden, die für manche Situationen interessante Möglichkeiten bieten.

Festplattengröße

Sie können die Größe der Festplatte nach oben hin verändern. Dadurch wird aber nur die Platte der VM vergrößert. Die VM sieht dann eine größere Festplatte, die vorher erstellte Partition hat aber immer noch die gleiche Größe. Haben Sie also eine virtuelle Festplatte mit 8 GByte erstellt, das Betriebssystem installiert und anschließend die Größe auf 16 GByte geändert, sieht die VM eine 16-GByte-Platte mit einer primären Partition und 8 GByte ungenutzten Speicher dahinter.

Ich empfehle Ihnen, der VM eine neue Festplatte zu geben oder innerhalb der VM ein Partitionierungstool einzusetzen, um den Platz nutzen zu können. Achten Sie auf die Besonderheiten bei NTFS bezüglich der MFT (*Master File Table*). Auch der VMware Converter kann beim Import die Festplattengröße korrekt anpassen. Sie können auch eine bereits installierte ESXi-VM auf einen anderen Host importieren und zu kleine Platten vergrößern und verkleinern sowie Partitionen in Laufwerke umändern. Ab Windows Vista, also auch bei Windows 7 und Server 2008, können Sie die Partitionen im Festplattenmanager selber vergrößern. Das sollten Sie einem Tool auf jeden Fall vorziehen.

Modus »Dauerhaft«

Die virtuelle Festplatte wird in diesem Fall wie eine normale Festplatte behandelt und alle Änderungen werden sofort auf der Festplatte weggeschrieben, auch bei Snapshots (gegebenenfalls dann nicht anwählbar!).

Über die Kommandozeile kann die Festplatte im laufenden Betrieb in einen anderen Modus geschaltet werden, um beispielsweise Backups zu machen. Bei Neuanlage einer Festplatte befindet sich diese standardmäßig im dauerhaften Modus. Auf die Leistungsfähigkeit dieser Zugriffsart sollte man nicht verzichten und nur bei Bedarf und kurzzeitig auf andere Zugriffsarten umschalten.

Den Modus UNABHÄNGIG – DAUERHAFT können Sie auch bei Backups nutzen, wenn Sie diese Platten nicht sichern wollen, z. B. über Data Recovery.

Modus »Nicht-dauerhaft«

Die virtuelle Festplatte (und nur diese – nicht gegebenenfalls weitere der Maschine) befindet sich bei ihrer Auswahl, wie in Abbildung 4-27 dargestellt, im schreibgeschützten

Modus, und alle Änderungen werden ohne Rückfrage beim Herunterfahren und Ausschalten verworfen. Dieses Verwerfen geschieht nur beim Ausschalten der virtuellen Maschine, nicht bei einem Neustart. Dieser Festplattenmodus ist besonders in Schulungsräumen oder Testumgebungen interessant, wenn man nicht will, dass Änderungen bestehen bleiben. Gerade im Fall einer Schulung könnten Sie die virtuellen Maschinen komplett installieren und dann den Festplattenmodus auf »nicht-dauerhaft« bzw. *non-persistent* umschalten. Die Teilnehmer können anschließend machen, was sie wollen, denn nach dem Abschalten der virtuellen Maschinen ist alles wieder im Ursprungszustand.

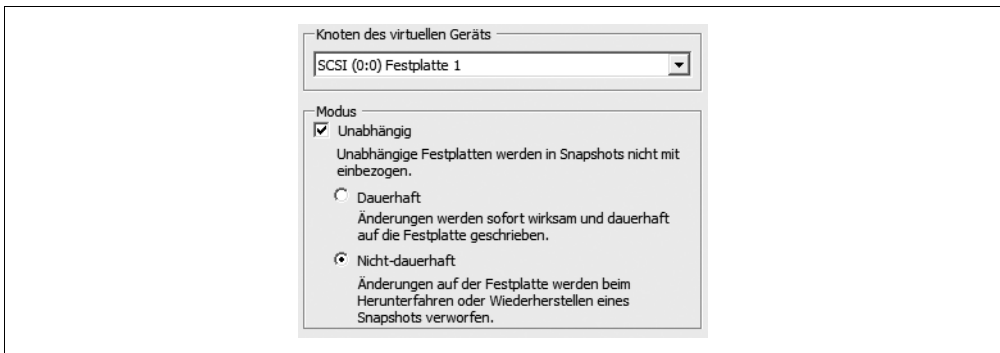


Abbildung 4-27: Unabhängiger Festplattenmodus



Es ist auch eine gute Idee, die Festplatte einer fertigen Maschine in den nicht-dauerhaften Modus umzuschalten und eine zweite Maschine zu erstellen und auf die Festplatte der ersten ebenfalls im nicht-dauerhaften Modus zugreifen zu lassen. Das funktioniert auch mit mehreren Maschinen, z. B. zum Testen verschiedener Konfigurationen.

Wenn Sie eine dynamisch wachsende Festplatte in eine Platte fester Größe ändern wollen, können Sie das über das Kontextmenü im Datastore-Browser erledigen (siehe Abbildung 4-28). Diesen Vorgang können Sie anschließend nicht mehr abbrechen.

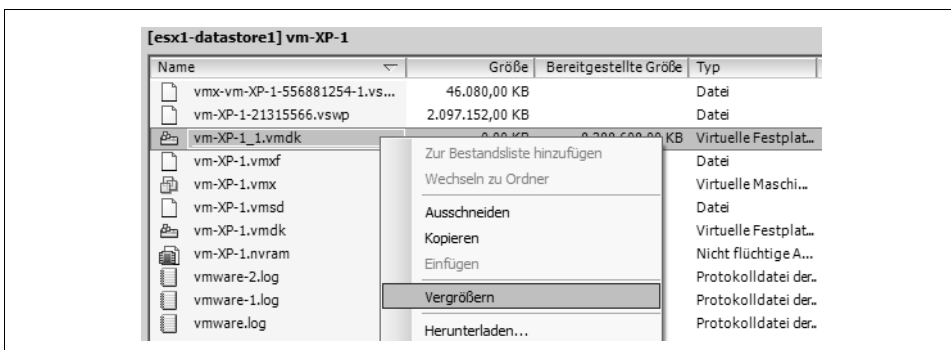


Abbildung 4-28: Festplatte vergrößern

Gasthardware hinzufügen

Nun wollen wir ein zusätzliches Gerät anschließen. Im Dialog können Sie sich nach einem Klick auf HINZUFÜGEN (siehe Abbildung 4-29) zwischen verschiedenen Geräten entscheiden. Zur Wahl stehen die bereits behandelten Festplatten, Netzwerkkarten usw., aber auch mehr oder weniger exotische Geräte wie SCSI-Scanner oder -Streamer.

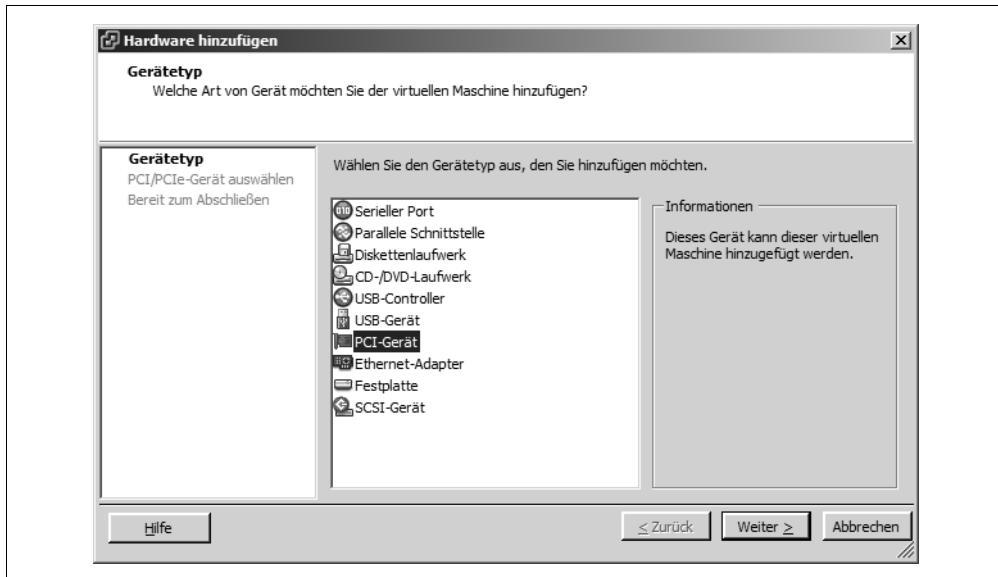


Abbildung 4-29: Hardwareauswahl bei der VM

Serielle und parallele Schnittstellen

Eher selten wird man bei VMs diese Hardware hinzufügen wollen. Nur bei manchen Linux-Systemen und unter Windows NT können hier interessante Konstellationen genutzt werden.

Besonderheiten beim Parallelport

In Abbildung 4-30 sehen Sie die Möglichkeit, eine Datei als Ausgabe für einen Parallelport direkt mit einer VM zu verbinden:

1. Klicken Sie auf die Registerkarte **HARDWARE**.
2. Klicken Sie unter **HARDWARE** auf **HINZUFÜGEN**, dann auf **PARALLELE SCHNITTSTELLE** und schließlich auf **WEITER**.
3. Wählen Sie die physische Schnittstelle des Hosts, falls vorhanden, oder **AUSGABE IN DATEI**. Diese Datei können Sie später z.B. auf einen Drucker kopieren (binär, also

z.B. copy Datei.prn LPT1 /b). Oder wählen Sie die Schnittstelle aus der Pull-down-Liste aus.

4. Aktivieren oder deaktivieren Sie das Kontrollkästchen bei BEIM EINSCHALTEN VERBINDEN, je nachdem, ob das Gerät mit der Schnittstelle beim Einschalten angebunden werden soll oder nicht. Die Voreinstellung ist BEIM EINSCHALTEN VERBINDEN.
5. Klicken Sie auf OK, um Ihre Änderungen zu speichern.

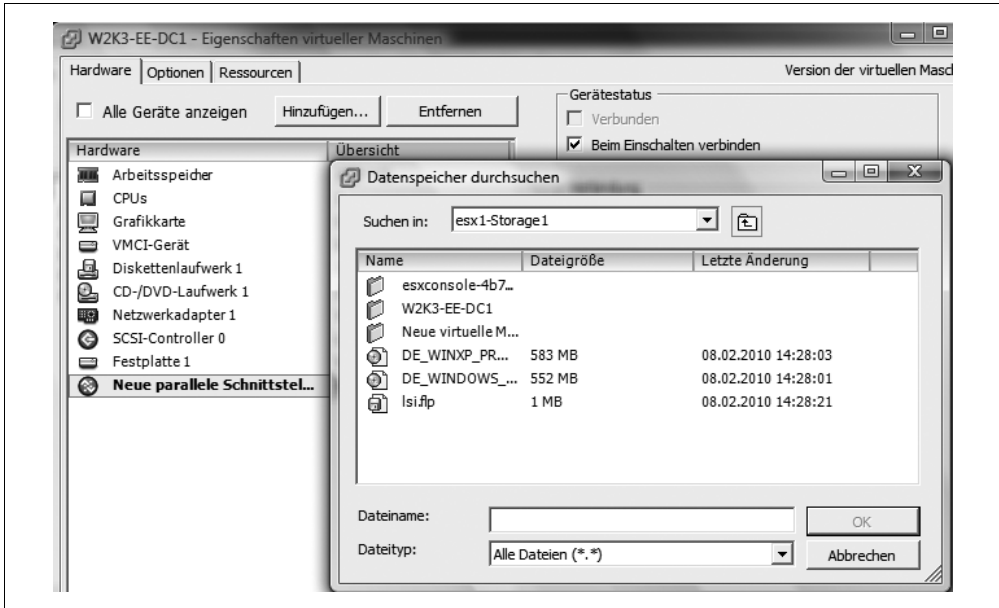


Abbildung 4-30: Schnittstellenkonfiguration

Besonderheiten beim seriellen Port

Abbildung 4-31 zeigt die vier Einstellungsmöglichkeiten beim seriellen Port:

- Wenn Sie die PHYSISCHE SERIELLE SCHNITTSTELLE AUF DEM HOST VERWENDEN möchten, wählen Sie im anschließenden Pull-down-Menü die Schnittstelle auf dem ESXi Server aus, die für diesen seriellen Anschluss verwendet werden soll.
- Wenn Sie die Option AUSGABE IN DATEI aktiviert haben, müssen Sie anschließend einen Namen für die Datei auf dem Speicherort angeben.
- Mit der Option MIT DER NAMED PIPE VERBINDEN erstellen Sie einen Kommunikationskanal, der von mehreren VMs genutzt werden kann. Geben Sie im Feld PIPE-NAME einen beliebigen Namen ein.
- ÜBER NETZWERK VERBINDEN bietet die Möglichkeit, auch weit entfernte Geräte über einen seriellen Port anzuschließen. Dafür benötigen Sie ggf. einen sogenannten Konzentrador.

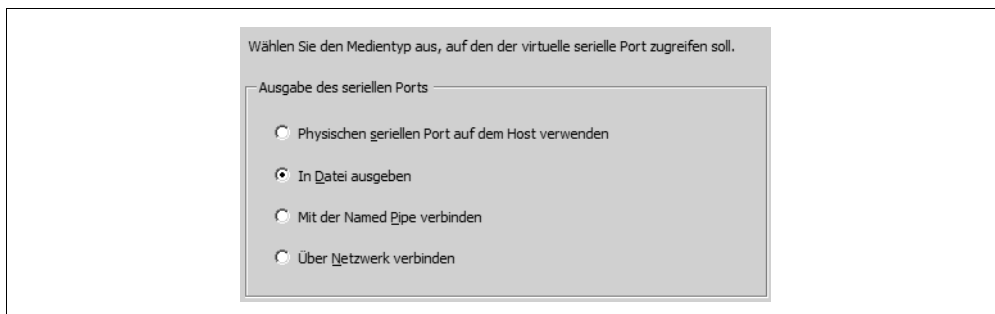


Abbildung 4-31: Bis zu vier Möglichkeiten bei seriellen Ports

Für einen Linux-Rechner geben Sie beim Namen `/tmp/<socket>` oder einen anderen UNIX-Socket-Namen Ihrer Wahl ein. Entscheiden Sie sich dann, ob Sie zwei virtuelle Maschinen miteinander oder eine virtuelle Maschine mit einer Anwendung auf dem Server verbinden wollen, wie in Abbildung 4-32 zu sehen ist.

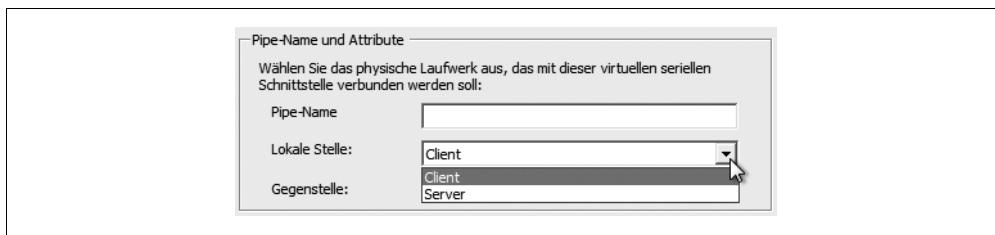


Abbildung 4-32: Serielle Schnittstelle hinzufügen

Wenn Sie zwei virtuelle Maschinen miteinander verbinden, müssen Sie den gleichen Kommunikationskanal auf der zweiten virtuellen Maschinen einrichten: Einer ist dann die **LOKALE STELLE**, der andere die **GEGENSTELLE**. Stellen Sie dann noch **SERVER** und **EINE VIRTUELLE MASCHINE** auf dem einen und **CLIENT** und **EINE VIRTUELLE MASCHINE** auf dem anderen ein.

Falls Sie sich mit einem Prozess verbinden lassen wollen, stellen Sie bei **LOKALE STELLE** die Option **SERVER** oder **CLIENT** ein und bei **GEGENSTELLE** dann **EIN PROZESS**.

Standardmäßig ist die serielle Schnittstelle verbunden, sobald Sie die virtuelle Maschine einschalten. Sie können das Kontrollkästchen **BEIM EINSCHALTEN VERBINDEN** deaktivieren. Bis zu vier serielle Schnittstellen werden bei VMs unterstützt und können auch nachträglich geändert werden.

Beachten Sie auch noch die Optionen bezüglich des E/A-Modus. Möchten Sie diese serielle Schnittstelle im Interrupt- oder im Poll-Modus betreiben? Der Poll-Modus ist vor allem für Entwickler vorgesehen, die Debugging-Werkzeuge über einen seriellen Anschluss verwenden. Im Poll-Modus wird der Prozessor des ESXi Servers unverhältnismäßig stark beansprucht. Dadurch verlangsamen sich der Host und auch die anderen virtuellen Maschinen auf ihm.

USB-Controller

Seit der 4er-Version des ESXi Servers steht ein USB-Controller für die VMs zur Verfügung. Weitere Einstellungen oder Konfigurationen sind hier nicht möglich, d.h. das angezeigte Auswahlfeld bringt nur dann etwas, wenn der Host oder physische PC auch USB 3.0 unterstützt. Innerhalb des Betriebssystems der VM steht dann ein USB-Hostcontroller mit maximal 15 Anschlüssen bereit (siehe Abbildung 4-33), bei USB 3.0 gibt es einen zusätzlichen Hostcontroller. Beide lassen sich übrigens auch im laufenden Betrieb hinzufügen, und die Geräte sollten automatisch verbunden werden.

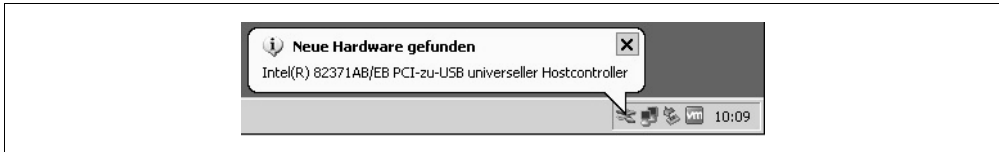


Abbildung 4-33: USB in der VM

Mittlerweile muss das USB-Gerät nicht mehr unbedingt mit dem Host verbunden sein, sondern das Durchreichen vom lokalen Arbeitsplatz über den vSphere Client in die VM ist ebenfalls möglich. Dafür wird am lokalen PC ein VMware USB Device installiert; angesteckte Geräte kann man über ein zusätzliches Icon in der Symbolleiste mit der VM verbinden. Das funktioniert auch mit den meisten Dongles, Websticks, USB-Festplatten etc. Rufen Sie anschließend die Eigenschaften der VM auf, steht das verbundene USB-Gerät mit in der Liste.



Ein USB-CD-/DVD-Laufwerk auf dem Host kann der VM nur als SCSI-Gerät hinzugefügt werden.



Gespiegelte VMs (Fault Tolerance) können nicht mit USB-Geräten des Clients versorgt werden.

Über eine Remote-Desktopverbindung können Sie lokale Ressourcen, also auch USB-Sticks, der virtuellen Maschine zur Verfügung stellen. USB-Dongles, Scanner, Drucker und andere Geräte können auch über einen USB-Device-Server angebunden werden. Da wäre z.B. der Digitus DN-13009, ein 4-Port-USB-Hub mit 100-MBit-Ethernet-Anbindung, oder der »myUTN-50« von SEH mit zwei Ports. Die Firma SILEX bietet sogar GBit-Verbindungen für USB im LAN an, und AnywhereUSB hält ebenfalls eine Netzwerklösung für USB bereit.

Ethernet-Adapter hinzufügen

Wenn Sie einer virtuellen Maschine einen Ethernet-Adapter hinzufügen, wählen Sie den Adaptertyp und die Netzwerkbezeichnung (den virtuellen Switch bzw. die Portgruppe) aus und geben an, ob das Gerät beim Einschalten der virtuellen Maschine verbunden werden soll.

1. Starten Sie den Assistenten zum Hinzufügen von Hardware.

2. Wählen Sie ETHERNET-ADAPTER und klicken Sie auf WEITER.
3. Wählen Sie im Abschnitt ADAPTERTYP einen Typ aus.
4. Wählen Sie im Fenster NETZWERKVERBINDUNG eine bereits vorhandene Portgruppe mit einer angegebenen Bezeichnung oder ein Legacy-Netzwerk aus.
5. Wenn die virtuelle Netzwerkkarte (*Network Interface Card*, NIC) beim Einschalten der virtuellen Maschine verbunden werden soll, wählen Sie BEIM EINSCHALTEN VERBINDEN.
6. Klicken Sie auf WEITER.
7. Überprüfen Sie Ihre Auswahl und klicken Sie auf BEENDEN.
8. Wenn Sie einen DISTRIBUTED VIRTUAL SWITCH haben, können Sie zwischen der Standard- und der erweiterten Ansicht umschalten und einen bestimmten Port für die NIC festlegen.
9. Weiterhin können Sie der VM eine beliebige MAC-Adresse zuweisen oder eine automatisch generierte nehmen.

Typen von Netzwerkadaptern

Wenn Sie eine virtuelle Maschine konfigurieren, können Sie Netzwerkadapter hinzufügen und den Adaptertyp festlegen. Welche Typen von Netzwerkadaptern verfügbar sind, ist abhängig

- von der Version der virtuellen Maschine, die vom Host abhängig ist, auf dem sie erstellt oder zuletzt aktualisiert wurde,
- davon, ob die virtuelle Maschine vom aktuellen Host auf die neueste Version aktualisiert wurde, und
- vom Gastbetriebssystem.

Die folgenden Netzwerkadapertypen werden unterstützt:

Tabelle 4-3: Unterstützte virtuelle Netzwerkkarten

Adaptertyp	Bemerkung
Vlance	Eine emulierte Version des AMD PCnet-Adapters, eine ältere 10-MBit/s-NIC, die von den meisten 32-Bit-Betriebssystemen außer Windows Vista und neuer unterstützt wird. Es brauchen keine VMware Tools installiert zu werden.
vmxnet	Hierfür gibt es keine physische Entsprechung einer NIC. Die Tools müssen installiert werden, damit der Adapter funktioniert.
flexibel	Wird auf virtuellen Maschinen unterstützt, die unter ESXi Server 3.0 oder höher erstellt wurden und ein 32-Bit-Gastbetriebssystem ausführen. Der flexible Adapter fungiert als Vlance-Adapter, wenn die VMware Tools nicht auf der virtuellen Maschine installiert wurden. Sind die VMware Tools installiert, arbeitet der Adapter als vmxnet-Treiber.
e1000	Emuliert die Funktionsweise einer Intel-LAN-Pro-GBit-Netzwerkkarte. Hierbei handelt es sich um den standardmäßigen Adaptertyp für virtuelle Maschinen, die ein 64-Bit-Gastbetriebssystem ausführen.
VMXNet 2 (erweitert)	Eine aktualisierte Version des vmxnet-Geräts mit verbesserter Leistung (wie Jumbo-Frames). Für diesen Adaptertyp ist die Installation der VMware Tools auf der virtuellen Maschine erforderlich. Der Adapter wird erst bei neueren OS unterstützt.

Tabelle 4-3: Unterstützte virtuelle Netzwerkkarten (Fortsetzung)

Adapterttyp	Bemerkung
VMXNet 3	vmxnet-Gerät der nächsten Generation mit verbesserter Leistung und erweiterten Netzwerkfunktionen. VMware Tools müssen dafür auf der virtuellen Maschine installiert sein, und die virtuelle Maschine muss die Hardwareversion 7 oder höher verwenden. Der Adapter wird erst bei neueren OS unterstützt.

Netzwerkadapter auf Legacy-VMs

Wenn Ihre virtuelle Maschine auf ESX Server 3.0 oder einer höheren Version erstellt wurde und ein 32-Bit-Gastbetriebssystem ausführt, ist der standardmäßige Adapterttyp *flexibel*. Der flexible Adapter fungiert als *Vlance*-Adapter, wenn der Adaptertreiber der Standardtreiber des Gastbetriebssystems ist. Der flexible Adapter fungiert als *vmxnet*-Adapter, wenn der *vmxnet*-Treiber als Bestandteil der VMware Tools-Installation auf der virtuellen Maschine installiert wurde.

Führt Ihre virtuelle Maschine ein 64-Bit-Gastbetriebssystem aus, ist der standardmäßige Adapterttyp *e1000*. Wenn Sie eine virtuelle Maschine von einem 32-Bit- auf ein 64-Bit-Gastbetriebssystem umstellen (oder umgekehrt), müssen Sie den vorhandenen Netzwerkadapter entfernen und durch einen neuen ersetzen, ansonsten wird die virtuelle Maschine gegebenenfalls nicht eingeschaltet.

Bei einem Hardware-Upgrade auf einer virtuellen Legacy-Maschine gilt für diese Maschine nach erfolgtem Upgrade folgender Adapterttyp:

- War der Adapterttyp zuvor *Vlance*, ist der Adapterttyp der virtuellen Maschine nach dem Upgrade *flexibel*. Dieser Adapter funktioniert genau wie ein *Vlance*-Adapter. Möchten Sie eine deutlich bessere Leistung erzielen, müssen Sie lediglich die VMware Tools auf der virtuellen Maschine installieren, wie es im vorangegangenen Schritt beschrieben wurde.
- Falls der Adapterttyp zuvor *vmxnet* war, ist der Adapterttyp der virtuellen Maschine nach dem Upgrade weiterhin *vmxnet*. Sie können diesen Adapterttyp jedoch nicht – wie im Fall einer virtuellen Legacy-Maschine – in *Vlance* ändern.



Wenn Sie eine physische Maschine importieren oder eine VM hardwaremäßig hochstufen, sollten Sie einen höheren Netzwerkadapter benutzen, um die Leistung zu verbessern.

SCSI-Gerät hinzufügen

Sie können an ESXi Server angeschlossene SCSI-Hardware – aber keine Festplatten – über den Assistenten der virtuellen Maschine hinzufügen:

1. Wählen Sie Ihre VM aus und klicken Sie auf EINSTELLUNGEN BEARBEITEN.
2. Klicken Sie auf die Schaltfläche HINZUFÜGEN und wählen Sie SCSI-GERÄT unter GERÄTETYP aus. Klicken Sie auf WEITER.

3. Wählen Sie unter VERBINDUNG im Drop-down-Menü das physische Gerät aus, das Sie verwenden möchten.
4. Wählen Sie unter KNOTEN DES VIRTUELLEN GERÄTS den Adapter und die SCSI-ID für virtuelle Geräte aus (z.B. SCSI (0:1)). Beachten Sie, dass der Eintrag (1:0) der VM einen weiteren SCSI-Adapter hinzufügt.
5. Überprüfen Sie die Information auf der Seite BEREIT ZUM ABSCHLIEßEN und klicken Sie auf BEENDEN.

Festplattenanschlusstyp ändern

Möchten Sie nach der Installation des Betriebssystems einen anderen Controller für eine Festplatte verwenden, bekommen Sie üblicherweise Probleme, wenn auf dieser das Betriebssystem installiert ist. Um dennoch z.B. aus Performancegründen (siehe Kasten »Adaptertypen« auf Seite 49) so einen Adapter austauschen zu können, gehen Sie wie folgt vor:

1. Wählen Sie Ihre ausgeschaltete VM aus und klicken Sie auf EINSTELLUNGEN BEARBEITEN.
2. Klicken Sie unter der Registerkarte HARDWARE auf den Button HINZUFÜGEN und wählen Sie FESTPLATTE aus. Klicken Sie auf WEITER.
3. Bestätigen Sie, dass Sie eine neue virtuelle Festplatte anschließen wollen, und klicken sie auf WEITER.
4. Legen Sie die Größe fest (1 MByte reicht) und wählen Sie im nächsten Fenster aus dem Pull-down-Menü z.B. SCSI(2:0) aus. Falls Sie schon einen SCSI-Adapter haben, dürfen Sie die neue Platte nicht an denselben Adapter hängen.
5. Klicken Sie auf BEENDEN, um das Fenster zu schließen. Wieder zurück bei den Eigenschaften der virtuellen Maschine sehen Sie fett hervorgehoben den neuen Adapter.
6. Klicken Sie auf den neuen Adapter und ändern Sie den Typ nach Ihren Vorstellungen. Klicken Sie auf OK, um das Fenster zu schließen.
7. Starten Sie die VM und installieren Sie die notwendigen Treiber für den neuen Controller, falls das Betriebssystem ihn nicht automatisch erkennt. Fahren Sie den Rechner anschließend wieder herunter.
8. Gehen Sie wieder in die Einstellungen der VM und entfernen Sie die neue Festplatte (von Festplatte löschen), die alte Festplatte entfernen Sie ebenfalls, aber dieses Mal nicht von Festplatte löschen. Klicken Sie auf OK.
9. Verbinden Sie sich mit der Konsole des ESXi Servers, z.B. mit *putty*, und navigieren Sie zum Verzeichnis der VM (z.B. `/vmfs/volumes/datastore1/vm-XP-1`).
10. Öffnen Sie die Beschreibungsdatei zur Bootfestplatte und tragen Sie an der Stelle mit dem alten Adaptertyp (`ddb.adapterType = "xxx"`) den neuen Typ ein. Das kann `ide`, `buslogic` oder `lsilogic` sein.

11. Gehen Sie wieder in die Einstellungen der VM und fügen dieser eine vorhandene Festplatte hinzu. Wählen Sie aus dem Verzeichnis der VM die *.vmdk*-Datei und bestätigen Sie die Eingabe.
12. Überprüfen Sie den hinzugefügten SCSI-Controller und ändern Sie diesen ggf. in den vorher installierten ab.

Aus Performancegründen empfehle ich, zumindest eine IDE-Festplatte in einen LSI Logic-Datenträger zu überführen. Für Datenpartitionen, die auf einem SAN liegen, sollten Sie den paravirtuellen Adapter von VMware wählen – aber nicht als Bootfestplatte.

Hinzufügen eines PCI-Geräts

Die *VMDirectPath-E/A* ermöglicht dem Gastbetriebssystem einer virtuellen Maschine den direkten Zugriff auf physische PCI- und PCIe-Geräte, die mit einem Host verbunden sind. Jede virtuelle Maschine kann mit bis zu sechs PCI-Geräten verbunden werden.

Mit einem Host verbundene PCI-Geräte können über die erweiterten Hardwareeinstellungen in der Registerkarte KONFIGURATION für den Host als für Passthrough verfügbar gekennzeichnet werden.

Folgende Voraussetzungen sind dabei gegeben:

Für die Verwendung von VMDirectPath muss die *Virtualization Technology for Directed I/O* (VT-d) von Intel oder die *I/O Virtualization Technology* (IOMMU) von AMD im BIOS des Hosts aktiviert sein. PCI-Geräte müssen mit dem Host verbunden und als für Passthrough verfügbar gekennzeichnet sein, damit Sie die Geräte einer virtuellen Maschine hinzufügen können. Außerdem können PCI-Geräte nur zu virtuellen Maschinen mit Hardwareversion 7 oder höher hinzugefügt werden.

So gehen Sie vor, wenn Sie physische Geräte einer virtuellen Maschine zuordnen wollen:

1. Wählen Sie die virtuelle Maschine im Bestandslistenfenster aus und klicken Sie auf VIRTUELLE MASCHINE → EINSTELLUNGEN BEARBEITEN.
2. Klicken Sie auf der Registerkarte HARDWARE auf HINZUFÜGEN.
3. Wählen Sie im Assistenten zum Hinzufügen von Hardware die Option PCI-GERÄT aus und klicken Sie auf WEITER.
4. Wählen Sie das Passthrough-Gerät, mit dem Sie die virtuelle Maschine verbinden möchten, aus der Drop-down-Liste aus und klicken Sie auf WEITER.
5. Klicken Sie auf BEENDEN.



Sollten Sie keinen Eintrag für das Hinzufügen bei der virtuellen Maschine finden, schauen Sie bei der Konfiguration des ESXi Servers unter ERWEITERTE EINSTELLUNGEN nach. Gegebenenfalls steht dort, dass der Host Passthrough gar nicht unterstützt.

Optionen der virtuellen Maschine

Auf der Registerkarte OPTIONEN können Sie die Einstellungen zu ALLGEMEINES, BETRIEB, ENERGIE-MANAGEMENT sowie ERWEITERTE EINSTELLUNGEN festlegen (siehe Abbildung 4-34). Die Einstellungen der virtuellen Maschine ermöglichen die Definition von Aktionen, die in verschiedenen Zuständen der virtuellen Maschine auftreten.

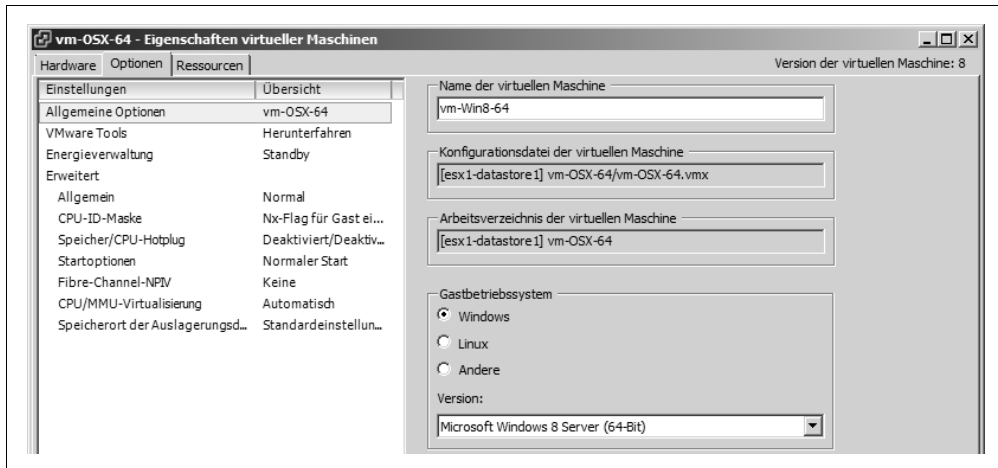


Abbildung 4-34: Optionen der VM konfigurieren

Allgemeine Optionen

Hierbei handelt es sich um Einstellungsmöglichkeiten zum Namen und dem ausgewählten Betriebssystem der VM. Weiterhin wird der Speicherort der VM angezeigt.

1. Gehen Sie in die Eigenschaften der virtuellen Maschine.
2. Klicken Sie auf die Registerkarte OPTIONEN.
3. Unter ALLGEMEINE OPTIONEN kann der Name der virtuellen Maschine geändert werden (das geht auch in der Bestandsliste über das Kontextmenü). Wenn Sie den Namen ändern, werden die Namen von Dateien auf der virtuellen Maschine bzw. des zugeordneten Verzeichnisses nicht geändert, solange Sie diese nicht auf einen anderen Storage schieben!
4. Das Arbeitsverzeichnis der virtuellen Maschine und ihre Konfigurationsdatei können nicht geändert werden.
5. In der Liste GASTBETRIEBSSYSTEM können Sie das Betriebssystem ändern, indem Sie über das Pull-down-Menü die neue Version auswählen.

Klicken Sie auf OK, um Ihre Änderungen zu speichern. Das Dialogfeld EIGENSCHAFTEN DER VIRTUELLEN MASCHINE wird geschlossen.

Betriebszustandsoptionen

Unter diesem Menüpunkt können die Schaltflächen zum Betriebszustand der VM und die dazugehörigen Skripten sowie die Uhrzeitsynchronisation geändert werden.

1. Sie haben auf der Registerkarte OPTIONEN unter VMWARE TOOLS die Möglichkeit, das Laufzeitverhalten der VM etwas zu ändern (siehe Abbildung 4-35). Die STOPP-Schaltfläche auf der Symbolleiste kann zum Ausschalten der virtuellen Maschine oder zum Herunterfahren des Gastbetriebssystems konfiguriert werden. Das kann sinnvoll sein, wenn man ein OS hat, das nicht heruntergefahren werden kann (z.B. DOS).

Die Schaltfläche zum ZURÜCKSETZEN auf der Symbolleiste kann zum Zurücksetzen der virtuellen Maschine oder zum Neustarten des Gastbetriebssystems konfiguriert werden.

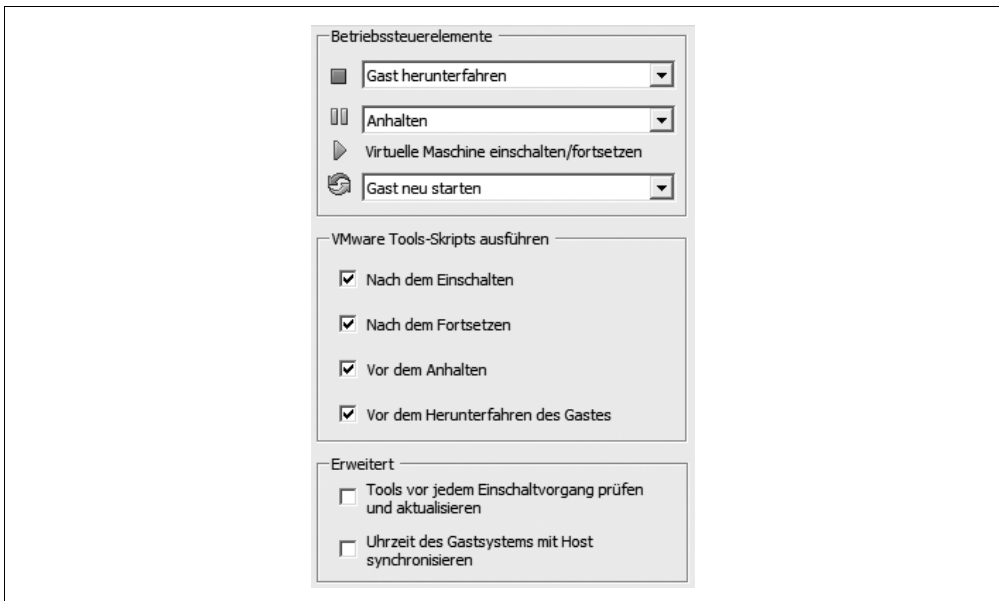


Abbildung 4-35: Betriebszustandsoptionen der VM

2. Wählen Sie die gewünschten Aktionen in den Listen unter BETRIEBSSTEUERUNGSELEMENTE aus.
3. (Optional:) Konfigurieren Sie die VMware Tools-Skripten so, dass sie nicht automatisch ausgeführt werden, wenn Sie den Betriebsstatus der virtuellen Maschine ändern, indem Sie die entsprechenden Optionen deaktivieren. Wenn Sie die VMware Tools installiert haben, können Sie die Skripten im laufenden Betrieb im OS abschalten. Auf dieser Registerkarte geht es nur, wenn die VM aus ist.
4. Unter ERWEITERT können Sie die Version der VMware Tools beim Starten überprüfen lassen und gegebenenfalls die Uhrzeit des Gasts mit der des Hosts synchronisieren.

Energieverwaltung

Klicken Sie auf die Registerkarte OPTIONEN und sehen Sie sich die Energieoptionen an. Die beiden Schaltflächen sollten selbsterklärend sein, wobei ein Server üblicherweise nicht in den Standby-Modus geht.

Wenn Sie sich dafür entschieden haben, die virtuelle Maschine eingeschaltet zu lassen, wählen Sie im Netzwerk der virtuellen Maschine WAKE-ON-LAN FÜR DATENVERKEHR DER VIRTUELLEN MASCHINE aus, indem Sie das Kontrollkästchen aktivieren.

Erweiterte Einstellungen

Die erweiterten Einstellungen sind laut VMware nur in bestimmten Situationen nützlich und sollten in der Regel nicht geändert werden. Ich gehe trotzdem auf sie ein, weil ich in der Praxis schon häufig Berührung mit ihnen hatte – und die folgenden Einstellungen auch brauchte.

Allgemein

- Um die Beschleunigung zu deaktivieren, aktivieren Sie das zuständige Kontrollkästchen. Sie können die Beschleunigung aktivieren und deaktivieren, während die virtuelle Maschine aktiv ist. Manche alten Applikationen haben ein Problem mit einem zu schnellen Prozessor – in so einem Fall könnte man ausprobieren, ob diese Funktion den gewünschten Effekt bringt (z.B. bei Foxpro-Datenbanken).



Es kommt schon mal vor, dass Sie meinen, die virtuelle Maschine sei blockiert, wenn in ihr Software installiert oder ausgeführt wird. Meist tritt dieses Problem zu Beginn einer Programmausführung auf. Manchmal kann man diesen Zustand kurzfristig umgehen, indem man die Beschleunigung in der virtuellen Maschine deaktiviert. Das bremst die virtuelle Maschine merklich. Verwenden Sie diese Option deshalb nur, um die obige Situation zu umgehen. Wenn dann keine Probleme mehr auftreten, nehmen Sie das Häkchen bei BESCHLEUNIGUNG DEAKTIVIEREN wieder weg.

- Mit dem Häkchen bei PROTOKOLLIERUNG AKTIVIEREN wird die eigentliche Datenerfassung ausgelöst. Damit werden üblicherweise sieben Logdateien im Verzeichnis der VM angelegt. Die Datei mit dem Namen *vmware.log* ist dabei die neueste, die älteren werden jeweils durchnummeriert. Die mit der höchsten Nummer ist die zweitälteste Logdatei.

Der Ausschnitt DEBUGGEN UND STATISTIKEN wird mit den folgenden Optionen angezeigt:

- NORMAL AUSFÜHREN.
- Um in den Fehlersuchmodus zu wechseln, aktivieren Sie das Kontrollkästchen INFORMATIONEN ZUM DEBUGGEN ERFASSEN. Für eine virtuelle Maschine werden dann

zusätzliche Informationen zur Fehlersuche zusammenstellt, die dem technischen Support von VMware bei der Behebung von Problemen von Nutzen sein können.

- Der Eintrag STATISTIKEN ERFASSEN war schon in älteren Versionen vorhanden, aber nicht auswählbar. Jetzt können hier zusätzliche Informationen über die VM aufgezeichnet werden. Bei Starten der VM werden der Unterordner *stats* angelegt und dort die Dateien abgelegt. In der enthaltenen Logdatei können Sie viele Parameter wie die ID der VM, den Zugriff auf den Prozessor und die MMU (Memory Management Unit) sehen.

Auf der Schaltfläche KONFIGURATIONSPARAMETER sehen Sie einige der Einstellungen zur virtuellen Maschine. Das ist ein Teil von dem, was in der Konfigurationsdatei der VM in ihrem Ordner steht. Über die Kommandozeile sieht man deutlich mehr Optionen – dazu folgen am Ende des Kapitels noch weitere Hinweise.

CPU-Identifikationsmaske

Das NX-Flag, das softwareseitig seit dem Servicepack 2 für Windows XP an Bord ist, wird auch von den heutigen CPUs hardwaremäßig unterstützt. NX steht für *NoExecute*, das wir in Windows-Betriebssystemen als Datenausführungsverhinderung unter SYSTEM-STEUERUNG → SYSTEM sehen können. Auch in der Datei *Boot.ini* wird dieser Wert angegeben mit *noexecute=optin* (Workstation) bzw. *noexecute=optout* (Server).

Der Sinn, diese Funktion vor der VM zu verstecken, liegt nur in der Kompatibilität beim Verschieben auf einen anderen Host, der das Flag noch nicht in der CPU hat.

Sollte bei den am Verschieben (vMotion) beteiligten Hosts nicht nur diese Funktion anders sein, kann man über ERWEITERT weitere Einstellungen zur CPU der virtuellen Maschine eingeben. Dabei handelt es sich um eine Maske, die z.B. neuere SSE4-Funktionen der Intel-Prozessoren ausblendet.

Sie können Erläuterungen der Symbole in diesem Dialogfeld anzeigen lassen, indem Sie auf LEGENDE klicken. Die virtuelle Maschine muss ausgeschaltet werden, bevor Sie diese Einstellung ändern können.

Speicher und CPU-Hotplug

Die VMware Tools müssen installiert sein, damit die Hotplug-Funktionen ordnungsgemäß funktionieren. Weiterhin muss das Gastbetriebssystem diese ebenfalls unterstützen, sonst sind die Felder ausgegraut.

Wenn Sie als Betriebssystem z.B. SUSE 11 64-BIT ausgewählt haben, steht Ihnen die Möglichkeit offen, weitere CPUs und Arbeitsspeicher im laufenden Betrieb hinzuzufügen.

Die Schaltflächen im Fenster aus Abbildung 4-36 sind selbsterklärend, weshalb ich hier nicht weiter auf sie eingehen werde.

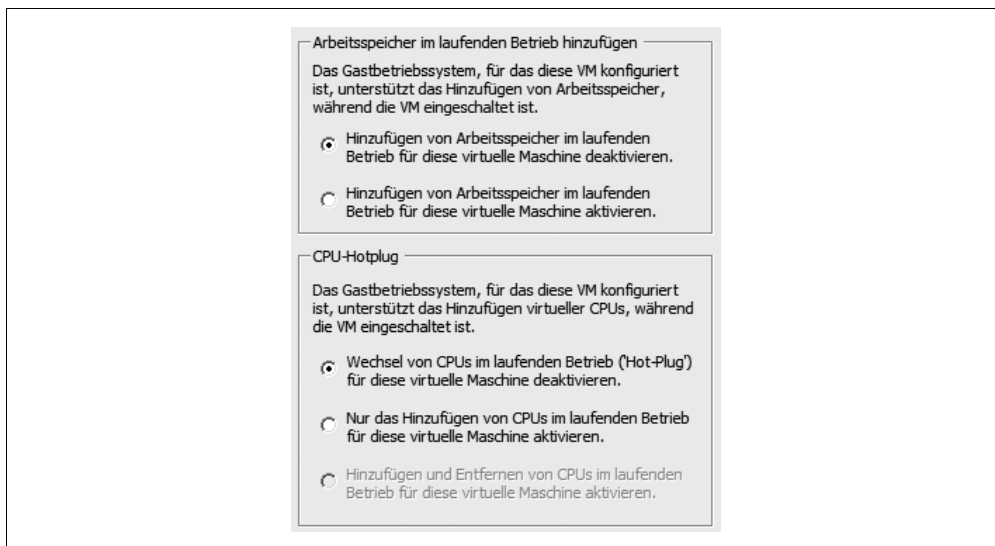


Abbildung 4-36: Hotplug für RAM und CPU

Startoptionen

Diese Einstellungen braucht man schon häufiger: Meist ist es nicht möglich, beim Starten der virtuellen Maschine ins BIOS/EFI zu gelangen. Sie müssten dazu die VM starten, dann mit der Maus den Fokus ins Fenster legen und die Taste F2 drücken.

Wählen Sie einfach das Kästchen unter BIOS-SETUP ERZWINGEN/EFI-SETUP ERZWINGEN aus, um beim nächsten Start der virtuellen Maschine das BIOS-Setup aufzurufen. Das Häkchen ist nach dem Starten der VM wieder weg.

Die STARTVERZÖGERUNG beim Einschalten bleibt hingegen dauerhaft erhalten. Hier können Sie die Dauer in Millisekunden angeben, für die der Beginn der Startsequenz verzögert werden soll, wenn die virtuelle Maschine eingeschaltet oder neu gestartet wird, also beispielsweise 10.000, um die BIOS-/EFI-Meldung 10 Sekunden lang anzeigen zu lassen. Im unteren rechten Bild der Anzeige sehen Sie dann einen Zähler, der bei null die VM startet. Mehr als 10 Sekunden, also 10.000 Millisekunden, können hier übrigens nicht eingestellt werden.

Unter STARTWIEDERHERSTELLUNG FEHLGESCHLAGEN verbirgt sich eine Einstellung, die ggf. beim Booten übers Netzwerk sinnvoll sein kann, wenn dieses kurzfristig überlastet ist. Ist die Last gesunken, könnte der nächste Bootvorgang erfolgreich sein. Leider lässt sich hier keine Grenze festlegen, so dass die VM ggf. bis zum nächsten Tag oder länger versucht, alle 10 Sekunden zu starten. Übrigens kann diese Einstellung nicht bei einem EFI-Boot funktionieren, weil hier beim erfolglosen Start über die festgelegten Medien eine Shell gestartet wird und der ESXi Server meint, alles wäre OK.

Fibre Channel-NPIV-Einstellungen

Wenn Sie ein Fibre Channel-SAN haben, können Sie ein Volume einer virtuellen Maschine direkt zuordnen. Die Einstellungen dazu können Sie hier eingeben. Standardmäßig ist NPIV (N-Port-ID-Virtualisierung) deaktiviert (siehe Abbildung 4-37).



Abbildung 4-37: Fibre Channel-LUN-Zuordnung

Mithilfe der NPIV können Sie einen einzelnen physischen Port auf Ihrem Fibre Channel-Host-Bus-Adapter (HBA) für mehrere virtuelle Ports mit jeweils eindeutigen Kennungen gemeinsam verwenden. Dadurch können Sie den Zugriff für jede virtuelle Maschine auf LUNs steuern.

Jeder virtuelle Port muss durch zwei WWNs (*World Wide Names*) gekennzeichnet werden: einen *World Wide Port Name* (WWPN) und einen *World Wide Node Name* (WWNN).

Für die NPIV-Unterstützung gelten laut VMware die folgenden Einschränkungen:

- NPIV muss auf dem SAN-Switch aktiviert sein. Wenn Sie Informationen zum Aktivieren von NPIV auf den Geräten benötigen, setzen Sie sich mit dem Switch-Hersteller in Verbindung.
- NPIV wird nur für virtuelle Maschinen mit RDM-Festplatten (*Raw Device Mapping*) unterstützt. Virtuelle Maschinen mit herkömmlichen virtuellen Festplatten verwenden weiterhin die WWNs der physischen HBAs des Hosts.
- Die physischen HBAs auf dem ESXi Host müssen mithilfe seiner WWNs auf eine LUN zugreifen können, so dass alle virtuellen Maschinen auf diesem Host mithilfe ihrer NPIV-WWNs auf diese LUN zugreifen können. Stellen Sie sicher, dass sowohl auf den Host als auch auf die virtuellen Maschinen zugegriffen werden kann.



Wenn Sie mehrere virtuelle Maschinen haben, die aus Versehen die gleichen WWNs verwenden, kann es passieren, dass Sie diese nicht mehr ausschalten können. Löschen Sie die WWNs oder vergeben Sie neue für eine der VMs.

Virtualisierte MMU

Bei der MMU handelt es sich allgemein um die Memory Management Unit, die als Funktion im Prozessor enthalten ist und virtuelle Speicheradressen in physische überträgt. Wenn ein Prozess Arbeitsspeicher anfordert, ist die MMU für die Umsetzung auf die tatsächliche Adresse verantwortlich. Da eine logische Adresse nicht unbedingt immer einer physischen Adresse zugeordnet werden muss, kann das Betriebssystem auch anderen Speicher ansprechen, z. B. eine Auslagerungsdatei. Das nennt sich dann *Speichervirtualisierung*, was beim ESXi Server der VMM (*Virtual Machine Monitor*) in Zusammenarbeit mit dem Kernel regelt (siehe Abbildung 4-38).

Die neueren Prozessoren von Intel und AMD unterstützen durch Befehlssatzerweiterungen die Virtualisierung des Prozessors durch die Technologie Intel VT-x (ehemals Vanderpool Technology, jetzt Virtualization Technology) bzw. AMD-V (ehemals Pacifica, manchmal auch SVM, Secure Virtual Machine). Seit Kurzem wird auch die Virtualisierung des Speichers von der CPU unterstützt (Intel EPT, Extended Page Tables, und AMD RVI, Rapid Virtualisation Indexing, oder Nested Page Tables, NPT). Beides muss ggf. durch das BIOS oder UEFI (Unified Extensible Firmware Interface) freigeschaltet werden.

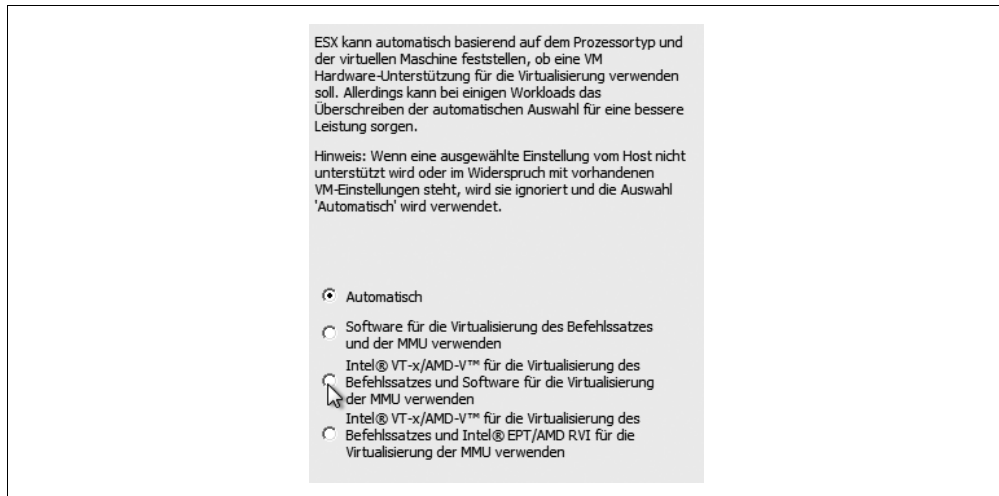


Abbildung 4-38: VMM und MMU durchreichen

Bei der Einstellung AUTOMATISCH sucht sich der VMM die Einstellungen selbstständig heraus, die von der Host-CPU und dem Gastbetriebssystem unterstützt werden, was für die meisten Systeme sehr gut funktioniert. Nur in ganz seltenen Fällen kann eine manuell

gewählte Einstellung für eine heterogene produktive Umgebung eine geringe Verbesserung der Leistung bringen – hier braucht also üblicherweise nichts verändert zu werden.

Weitere Informationen finden Sie im englischsprachigen White Paper *perf-vsphere-monitor_modes.pdf* von VMware auf der Website zu diesem Buch.

Speicherort der Auslagerungsdatei

Wie bereits oben erwähnt, wird beim Einschalten der VM der Arbeitsspeicher in gleicher Größe als Swap-Datei im Ordner der virtuellen Maschine abgelegt. In der Konfiguration des ESXi Servers kann ein anderer Speicherort für die Auslagerungsdatei eingerichtet und dieser der VM zugeteilt werden. vMotion wird dann aber gegebenenfalls nicht mehr unterstützt oder zumindest langsamer.

Wählen Sie eine der folgenden Optionen aus:

- **STANDARD** – Speichern Sie die Auslagerungsdatei der virtuellen Maschine im Standardspeicherort, der über die Auslagerungsdateieinstellungen für den Host oder Cluster definiert wird.
- **IMMER ZUSAMMEN MIT VIRTUELLER MASCHINE SPEICHERN** – Speichern Sie die Auslagerungsdatei der virtuellen Maschine im selben Ordner wie die Konfigurationsdatei der virtuellen Maschine.
- **IM DATENSPEICHER DER AUSLAGERUNGSDATEI FÜR DEN HOST SPEICHERN** – Speichern Sie die Auslagerungsdatei der virtuellen Maschine in dem Datenspeicher, der über die Auslagerungsdateieinstellungen für den Host oder Cluster definiert wird.

Ressourcenkontrolle der VM

Die Ressourcenkontrolle einer virtuellen Maschine unter ESXi ist eine der Funktionen, die einen VMware ESXi Server von anderen Virtualisierungslösungen klar unterscheidet, weil Sie nur hier eine derartige Vielzahl von Einstellungsmöglichkeiten haben. Mithilfe der Ressourcenkontrolle können Sie die vier Kernkomponenten (*Four Core*) des VMkernel, also Prozessor, Hauptspeicher, Storage und Netzwerk des Hosts, detailliert pro virtueller Maschine einstellen. Der ESXi Server bekommt ebenfalls Ressourcen zugeteilt, die in seiner Konfiguration angesehen und geändert werden können. Der Host hat standardmäßig den höchsten Anteil (Priorität) an Arbeitsspeicher, der viel höher ist als der der virtuellen Maschinen. Auch bei der CPU sind die Anteile sehr hoch, und eine Reservierung über die gesamte Kapazität ist eingetragen. Da Sie über den Host alle Arbeiten verrichten und dieser immer funktionieren muss, sollten Sie diese Einstellungen nur in Absprache mit dem VMware-Support ändern.

Bei der virtuellen Maschine sieht das manchmal ganz anders aus, wie Sie in Abbildung 4-39 sehen können. So nimmt sich ein DOS-Betriebssystem üblicherweise immer die ganze CPU, auch wenn auf der Oberfläche nur der Prompt steht. Hier ist es sinnvoll, eine

Einschränkung bezüglich der MHz-Zahl einzugeben. Auch sollten Sie bei virtuellen Novell Netware-Maschinen immer ein Auge auf den Verbrauch richten.

Übersicht Virtuelle Maschinen Ressourcenzuteilung Leistung Konfiguration Benutzer & Gruppen Ereignisse Berechtigungen			
CPU		Arbeitsspeicher	
Gesamtkapazität:	10131 MHz	Gesamtkapazität:	6841 MB
Reservierte Kapazität:	0 MHz	Reservierte Kapazität:	8 MB
Verfügbare Kapazität:	10131 MHz	Overhead-Reservierung:	0 MB
		Verfügbare Kapazität:	6833 MB

Abbildung 4-39: CPU- und Arbeitsspeicherressourcen

Die vier Kerneinträge erreichen Sie nicht alle über die Einstellung der virtuellen Maschine. Detailliert kann man hier lediglich Prozessor und Arbeitsspeicher einstellen und für die Zugriffe auf den Storage nur die ANTEILE und einen GRENZWERT für IOPS. Netzwerkeinschränkungen gehen nur über die Netzwerk-Switches.

CPU-Ressourcen

Bei den CPU-Einstellungen können Sie Prozessorressourcen für eine virtuelle Maschine zuweisen und dabei Reservierungen, Grenzen und Anteile angeben. Die Informationen zu CPU, Arbeitsspeicher und Datenträger können auch auf der Registerkarte RESSOURCENZUTEILUNG bei Host, Cluster oder Ressourcenpool eingestellt werden. Das ist sinnvoll, wenn Sie die Kapazitäten für mehrere virtuelle Maschinen bearbeiten möchten, und Sie haben gleich eine bessere Übersicht.

Einstellungsmöglichkeiten

Im Kasten »Begriffserklärung« wurden die drei Einstellungsmöglichkeiten Anteilswert, Reservierung und Grenzwert detailliert erklärt. Hier nun die speziellen Optionen zur CPU:

- Der ANTEILSWERT stellt eine relative Metrik für die Zuweisung der CPU-Kapazität dar. Sie können die Werte NIEDRIG (LOW), NORMAL, HOCH (HIGH) und BENUTZERDEFINIERT (CUSTOM) einstellen; dabei wird die Anzahl der Prozessoren mit 500, 1.000 bzw. 2.000 multipliziert. Unter BENUTZERDEFINIERT können Sie Werte zwischen 1 und 1.000.000 eingeben.
- RESERVIERUNG – Garantierte CPU-Zuweisung für diese virtuelle Maschine
- GRENZWERT – Höchstgrenze für die CPU-Zuweisung dieser virtuellen Maschine



Wählen Sie UNBEGRENZT (UNLIMITED), um keine Höchstgrenze festzulegen. Das scheint nicht das Gleiche zu sein wie den höchstmöglichen Wert zu nehmen und das Häkchen aus dem Kästchen zu entfernen. In der Praxis habe ich schon des Öfteren ein Stagnieren der Leistung bei VMs feststellen müssen. Zudem wird der Wert fest in die Konfigurationsdatei eingetragen, und wenn die Maschine in einen anderen Ressourcenpool kommt, ist es gegebenenfalls nicht mehr der Höchstwert.

Begriffserklärung

Bei den Ressourcenzuteilungen für CPU und RAM (siehe Abbildung 4-40) finden Sie die Begriffe »Anteile« (Shares), »Reservierung« (Reservation) und »Grenzwert« (Limit). Fangen wir mit dem Einfachsten an:

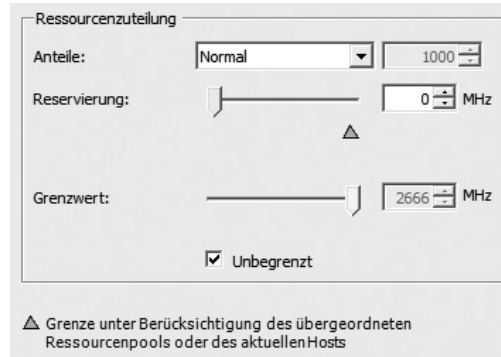


Abbildung 4-40: Ressourceneinstellungen

RESERVIERUNG: Sobald die virtuelle Maschine eingeschaltet wird, bekommt sie den MHz-Wert oder die Arbeitsspeichermenge zugeteilt, der bzw. die hier eingetragen ist, unabhängig von ihren tatsächlich benötigten Ressourcen. Schlimmstenfalls nimmt sie anderen Maschinen CPU-Zeit und RAM weg, obwohl es gar nicht nötig ist. Sind nicht mehr genug Ressourcen auf dem Host verfügbar, wird sie nicht eingeschaltet, und eine Fehlermeldung erscheint.

GRENZWERT: Hier wird die Obergrenze für die Maschine eingestellt, also wird sie in ihrer Laufzeitumgebung eingeschränkt, auch wenn vielleicht noch einiges an Arbeitsspeicher oder CPU-Zeit zur Verfügung stünde. Das angezeigte maximale Limit ist die Höchstgrenze, die auf dem ESXi Server zur Verfügung steht. In einem Cluster ändert sich das auf die Gesamtmenge der Clusterressourcen.

ANTEILE: Hiermit wird der Anteil der Gesamtkapazitäten, die zur Verfügung stehen, prozentual zwischen den VMs aufgeteilt. Das heißt, dass jede Maschine z.B. die gesamte CPU-Zeit bekommen kann. Erst wenn diese auf dem Host komplett aufgebraucht ist, wird nach den jeweiligen Anteilen geschaut. Der Maschine mit weniger Anteilen wird etwas weggenommen und der mit mehr Anteilen etwas dazugegeben. Aus diesem Grund sage ich dazu lieber »Prioritäten«.

Arbeitsspeicherressourcen

Im Fenster **ARBEITSSPEICHER** können Sie die RAM-Ressourcen für eine virtuelle Maschine angeben. Die Informationen zu CPU, Arbeitsspeicher und Datenträger können auch auf der Registerkarte **RESSOURCENZUTEILUNG** bei Host, Cluster oder Ressourcenpool einge-

stellt werden. Das ist sinnvoll, wenn Sie die Kapazitäten für mehrere virtuelle Maschinen bearbeiten möchten, und Sie haben gleich eine bessere Übersicht.

Einstellungsmöglichkeiten

Im Kasten »Begriffserklärung« wurden die drei Einstellungsmöglichkeiten Anteilswert, Reservierung und Grenzwert detailliert erklärt. Hier nun die speziellen Optionen zum Arbeitsspeicher:

- Der ANTEILSWERT stellt eine relative Metrik für die Zuweisung der RAM-Kapazität dar. Sie können die Werte NIEDRIG (LOW), NORMAL, HOCH (HIGH) und BENUTZERDEFINIERT (CUSTOM) einstellen; dabei wird die Menge des Arbeitsspeichers mit 5, 10 bzw. 20 multipliziert. Unter BENUTZERDEFINIERT können Sie Werte zwischen 1 und 1.000.000 eingeben.
- RESERVIERUNG – Garantierte RAM-Zuweisung für diese virtuelle Maschine
- GRENZWERT – Höchstgrenze für die RAM-Zuweisung dieser virtuellen Maschine

Festplattenressourcen

Im Bedienfeld FESTPLATTEN-RESSOURCEN kann keine Reservierung eingetragen werden, aber ein Grenzwert für E/A-Vorgänge (siehe Abbildung 4-41). Über die Anteile (Prioritäten) können Sie den virtuellen Festplatten I/O-Bandbreite genehmigen, da diese Ressource serverabhängig ist und nicht clusterübergreifend abgerufen werden kann. In der Praxis hat sich jedoch herausgestellt, dass die virtuellen Maschinen viel wahrscheinlicher durch die obigen beiden Einstellungen zu RAM und CPU eingeschränkt werden als durch Festplattenressourcen.

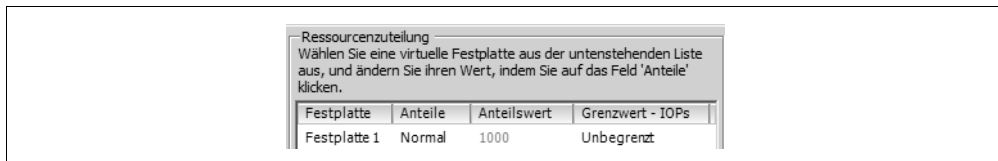


Abbildung 4-41: Ressourcenzuteilung

Einstellungsmöglichkeiten

Der ANTEILSWERT stellt eine relative Metrik für die Zuweisung der Festplattenübertragungskapazität dar. Sie können die Werte NIEDRIG (LOW), NORMAL, HOCH (HIGH) und BENUTZERDEFINIERT (CUSTOM) einstellen; dabei werden 500, 1.000 bzw. 2.000 genommen. Unter BENUTZERDEFINIERT können Sie Werte zwischen 1 und 1.000.000 eingeben.

- DER GRENZWERT – IOPs bestimmt die Höchstgrenze für die E/A-Übertragungen pro Sekunde dieser virtuellen Maschine.



Hat Ihre VM mehrere Festplatten, können Sie zu jeder einzelnen die Werte hier festlegen.

Erweiterte CPU-Einstellungen

Im Fenster ERWEITERTE CPU-RESSOURCEN (siehe Abbildung 4-42) können Sie Optionen für physische Prozessorkerne und Hyperthreading festlegen. Diese Anzeige haben Sie nicht, wenn Ihr Host nur einen Prozessor und kein Hyperthreading hat oder sich in einem DRS-Cluster (*Distributed Ressource Scheduling*, also Load-Balancing) befindet.



Abbildung 4-42: Erweiterte CPU-Einstellungen



Die Hyperthreading-Technologie ermöglicht es einem einzelnen physischen Prozessorkern, sich wie zwei logische Prozessoren zu verhalten und damit zwei unabhängige Anwendungen gleichzeitig auszuführen. Die Leistung eines Systems wird durch das Hyperthreading zwar nicht verdoppelt, aber es wirkt sich positiv aus, indem Leerlaufressourcen besser ausgenutzt werden.

Die Option GEMEINSAMER KERNZUGRIFF MIT HYPER-THREADING bietet Kontrolle darüber, ob eine virtuelle Maschine nur für einen Teil an einem physischen Prozessorkern geplant werden soll (Hyperthreading muss auf dem Server aktiviert sein).

Die Option PLANEN VON AFFINITÄT ermöglicht eine genaue Kontrolle darüber, wie die Verteilung der virtuellen CPUs auf die physischen Kerne des Servers abläuft.

Im Auswahlmenü können Sie folgende Einstellungen vornehmen:

- ALLE (Standard) – Die virtuellen CPUs dieser virtuellen Maschine können sich die Cores mit anderen virtuellen CPUs dieser oder anderer virtueller Maschinen frei teilen.
- INAKTIV – Die virtuellen CPUs dieser virtuellen Maschine verwenden einen Prozessorkern bei entsprechender Planung exklusiv. Der andere Hyperthread des Kerns wird angehalten, während diese virtuelle Maschine den Kern benutzt.

- **INTERN** – Auf einer virtuellen Maschine mit genau zwei virtuellen Prozessoren können diese beiden virtuellen Prozessoren einen physischen Kern (nach Ermessen des ESXi Server-Planers) gemeinsam nutzen, doch verwendet diese virtuelle Maschine einen Kern niemals gemeinsam mit einer anderen. Wenn die Anzahl der auf dieser virtuellen Maschine vorhandenen Prozessoren nicht 2 ist, ist diese Einstellung identisch mit der Einstellung **INAKTIV**.



In einem DRS-Cluster ist die Option **AFFINITÄT** nicht zulässig, und ihre Einstellungen werden gegebenenfalls gelöscht, wenn die VM auf einen anderen Server migriert wird. Falls die VM nicht verschoben werden kann, müssen Sie sich direkt am ESXi Server anmelden und die Affinität löschen. Der Sinn dieser Option liegt allein in der Optimierung der Performance einer bestimmten Gruppe von virtuellen Maschinen auf demselben Server.

Erweiterter Arbeitsspeicher

Auf mancher physischer Hardware gibt es zusätzlich zur Affinität der Prozessoren auch noch die Affinität von Arbeitsspeicher. Der Fachbegriff dafür ist *NUMA-Arbeitsspeicheraffinität*. Abbildung 4-43 zeigt beispielhaft die Einstellungsmöglichkeiten. Die Abkürzung NUMA steht für *Non-Uniform Memory Architecture* und wird bei Mehrprozessorcomputern eingesetzt, die einen speziellen Speicherkontroller dafür besitzen. Dabei hat jede CPU einen eigenen Arbeitsspeicher mit einem bestimmten Adressbereich, über den andere CPUs ebenfalls auf die Daten im RAM zugreifen können (*Distributed Shared Memory*).

Beachten Sie dabei, dass die beteiligten CPUs häufig auf den Arbeitsspeicher warten müssen und dann der Einsatz einer NUMA-Affinität negative Folgen für die Performance mit sich bringt.

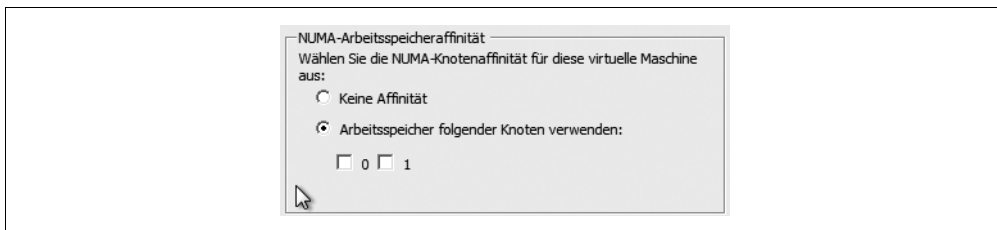


Abbildung 4-43: Einstellungen zur NUMA-Arbeitsspeicheraffinität

BIOS-Einstellungen der virtuellen Maschine

Um die BIOS-Einstellungen der virtuellen Maschine zu sehen oder zu verändern, muss man relativ schnell mit Maus und Tastatur sein. Die Anzeige des POST (*Power On Self Test*) ist recht kurz und geht meist ohne Details vor sich (siehe Abbildung 4-44).

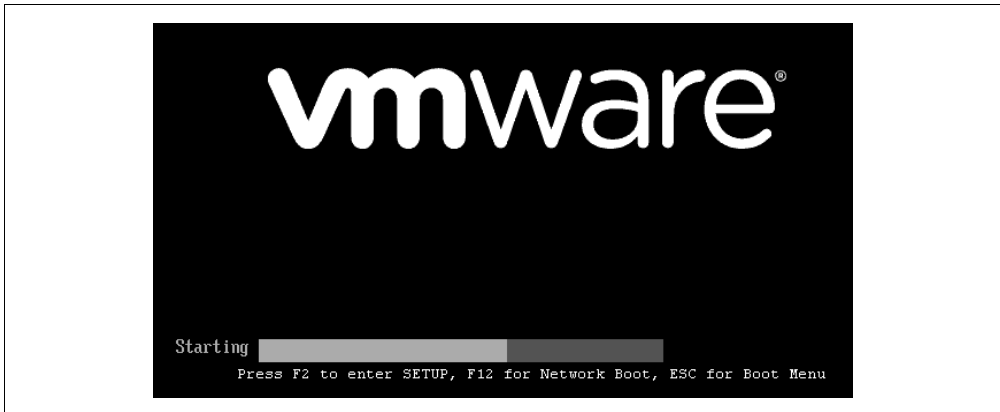


Abbildung 4-44: BIOS-Meldung beim Start der VM

Mit der Taste F2 kommt man zu den Einstellungen – allerdings liegt der Fokus von Tastatur und Maus noch beim Hostsystem. Also muss man zunächst mit der Maus in das Fenster der gerade startenden Maschine klicken und anschließend die F2-Taste drücken – das gelingt nicht immer beim ersten Mal.

Will man nur die Bootreihenfolge umstellen, z.B. für die Installation auf das optische Laufwerk, kann man nach dem Fokuswechsel mit der Maus die Taste Esc drücken, um ins Bootmenü zu kommen. Hier hat man dann die folgende Auswahl:

- REMOVEABLE DEVICES: üblicherweise Floppy, ZIP, LS120
- HARD DRIVE: angeschlossene Festplatte (können auch mehrere sein)
- CD-ROM DRIVE: CD- oder DVD-Laufwerke, also optische Geräte
- NETWORK BOOT: Anzeige der Netzwerkkarte (MBA, *Managed Boot Agent*)

Weiterhin hat man die Möglichkeit, von hier aus in die BIOS-Einstellungen zu gelangen.

Mithilfe der Taste F12 bekommen Sie die Möglichkeit, aus dem Netzwerk zu starten. Die Funktionalität ist die gleiche wie bei einer PXE-kompatiblen Netzwerkkarte (*Preboot eXecution Environment*), wie Abbildung 4-45 zeigt. Es wird also nach Dateien im Netzwerk mit der eingestellten MAC-Adresse gesucht – meistens zunächst ein DHCP-Server (*Dynamic Host Configuration Protocol*).

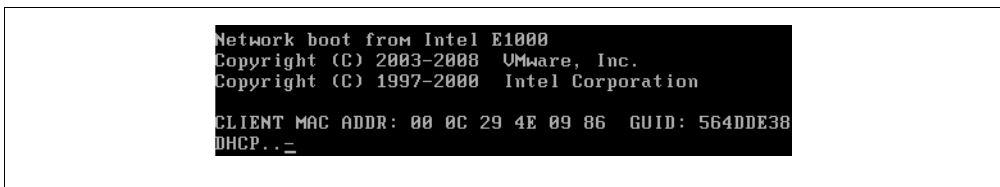


Abbildung 4-45: Starten über das Netzwerk mit PXE

Die vorgegebenen Grundeinstellungen für die VM bezüglich des BIOS brauchen normalerweise nicht verändert zu werden. Nur in Ausnahmesituationen ist das angebracht. Das moderne Phoenix-BIOS sieht zunächst nicht anders aus als das einer echten physischen Maschine.

Tastaturbelegung und -handhabung

Mit den Pfeiltasten Pfeil hoch und Pfeil runter neben dem Nummernblock kommen Sie zu den jeweiligen Features. Die Pfeiltasten nach links und rechts führen zum nächsten bzw. vorherigen Menü. Änderungen können über die Tasten + und – auf dem Nummernblock erfolgen. Meist haben Sie auch die Möglichkeit, die Enter-Taste zu drücken und in einem kleinen Fenster wiederum mit den Pfeiltasten die Einstellungen vorzunehmen. Anschließend bestätigen Sie sie erneut mit Enter (siehe Abbildung 4-46).

F1	Help	↑↓	Select Item	-/+	Change Values	F9	Setup Defaults
Esc	Exit	↔	Select Menu	Enter	Select ► Sub-Menu	F10	Save and Exit

Abbildung 4-46: Funktionstasten im BIOS

Bei den Zeilen, an denen ein Dreieck angezeigt wird, kommt man mit Enter in ein Untermenü. Häufig wird hier dann in der rechten Hälfte des Fensters eine spezielle Hilfe angezeigt (*Item Specific Help*). Mit Esc verlässt man das Untermenü wieder.

Einstellungen

Unter dem Menüpunkt MAIN findet man – wie üblich – die Einstellungen zu Datum und Uhrzeit, die angeschlossenen IDE-Platten (SCSI-Platten werden hier üblicherweise nicht angezeigt!), Einstellungen zur Tastatur (Verzögerung und Wiederholrate) und eine Auflistung des Arbeitsspeichers nach alter DOS-Konvention.

Weiterhin hat man die Möglichkeit, statt des Bildes *vmware* mit Laufbalken den DIAGNOSTIC SCREEN zu wählen, um mehr Informationen zum POST zu bekommen.

Bei ADVANCED findet man nur wenige Einstellungen, und diese sind für die emulierte Hardware meist uninteressant. Einzig die MULTIPROCESSOR SPECIFICATION sollte man bei alten Betriebssystemen (nur wenn es damit Probleme gibt und auch nur wenn man ein MPS hat) vom voreingestellten Wert 1.4 auf 1.1 herabsetzen. Das brauchen Sie z.B. bei Windows NT.

Wie bei einem normalen BIOS können Einstellungen unter SECURITY vorgenommen werden. Über das User-Passwort kann die Maschine gestartet werden, das Supervisor-Passwort ist für den Start der VM und die BIOS-Einstellungen notwendig. Nach der Eingabe eines Passworts kann dann festgelegt werden, ob beim Booten immer ein Passwort abgefragt wird oder nur beim Aufruf des BIOS.

Die Power-Management-Einstellungen unter POWER sind sehr dürftig. Da neuere Betriebssysteme diese Einstellungen aber meistens selbst übernehmen, ist das nicht weiter schlimm.

Im Menüpunkt BOOT (siehe Abbildung 4-47) können Sie die Bootreihenfolge dauerhaft einstellen; andernfalls hat man ja – wie schon erwähnt – auch die Möglichkeit, während des Bootens die Taste Esc zu drücken.

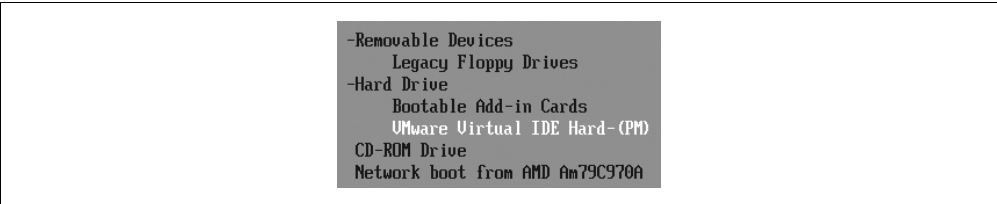


Abbildung 4-47: Boot-Menü

Um die Geräte unter einem der Menüpunkte sehen zu können, braucht man dort nur die Enter-Taste zu drücken. Alle der virtuellen Maschine zur Verfügung stehenden bootfähigen Geräte werden dann angezeigt. Mit den Tasten + und – kann man die Geräte und die oberen Menüpunkte nach oben bzw. unten verschieben, um die Bootreihenfolge einzustellen.

Über den Menüpunkt EXIT kann man das BIOS mit oder ohne Speichern verlassen. Auch hat man hier die Möglichkeit, die Änderungen zu verwerfen, zu speichern oder die Standardeinstellungen von VMware zu laden, wie Abbildung 4-48 zeigt.

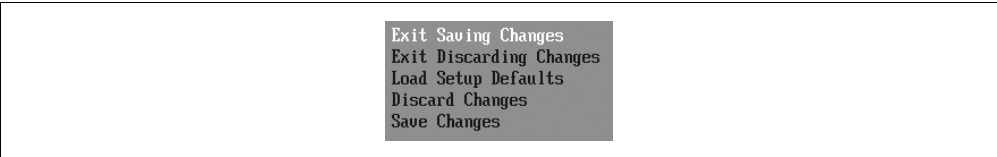


Abbildung 4-48: BIOS verlassen

Tabelle 4-4: Optionen des Menüpunkts Exit im BIOS

Englisch	Deutsch
Exit Saving Changes	Änderungen speichern und BIOS verlassen
Exit Discarding Changes	Änderungen nicht speichern und BIOS verlassen
Load Setup Defaults	Standardeinstellungen von VMware laden
Discard Changes	Änderungen verwerfen – BIOS nicht beenden
Save Changes	Änderungen speichern – BIOS nicht beenden



Denken Sie bitte daran, dass für die Tastatur noch kein Treiber geladen wurde und daher die Y-Taste noch mit Z belegt ist.
Beachten Sie, dass die BIOS-Einstellungen immer im gleichen Schema vorliegen – unabhängig vom ausgewählten Betriebssystem!

EFI-Einstellungen der virtuellen Maschine

Um die EFI-Einstellungen der virtuellen Maschine zu sehen oder zu verändern, muss man relativ schnell mit Maus und Tastatur sein. Die Anzeige des POST (*Power On Self Test*) ist recht kurz und geht meist ohne Details vor sich.

Mit der Taste F2 kommt man zu den Einstellungen – allerdings liegt der Fokus von Tastatur und Maus noch beim Hostsystem. Also muss man zunächst mit der Maus in das Fenster der gerade startenden Maschine klicken und anschließend die F2-Taste drücken – das gelingt nicht immer beim ersten Mal.

Besser geht man in den Einstellungen der VM auf die Registerkarte OPTIONEN und dann auf die Einstellung STARTOPTION und setzt dort das Häkchen bei SETUP ERZWINGEN.

Startet man anschließend die VM, gelangt man in ein Menü mit drei Auswahlmöglichkeiten:

- CONTINUE, also Weitermachen, heißt, dass die VM ohne Änderungen gestartet wird.
- BOOT MANAGER zeigt alle Optionen für die Startgeräte der VM an. Mit den Pfeiltasten kann man einen Eintrag auswählen und mit Return die VM über dieses Gerät einmalig starten.
- BOOT MAINTENANCE MANAGER bietet wiederum sechs Untermenüs:
- BOOT OPTIONS – eine Bootoption als Anwendung oder Wechselmedium festlegen
- DRIVER OPTIONS – einen Treiber als Startoption hinzufügen
- CONSOLE OUTPUT MODE SELECT – Auflösung des Bildschirms ändern
- BOOT FROM A FILE – eine Datei als Bootoption festlegen
- SET BOOT NEXT VALUE – ein Gerät als nächstes Startgerät festlegen
- RESET THE SYSTEM – ein Reset für das System durchführen

Dateien der virtuellen Maschine

Auf dem VMFS-Volume des ESXi Servers befindet sich unsere Maschine üblicherweise in einem eigenen Verzeichnis. Unabhängig davon, ob dieses ein lokaler oder ein SAN-Storage ist, wird das Volume in das Dateisystem des ESXi Hosts eingebunden und ist von dort aus auf der Kommandozeile erreichbar. Auch über den Datastore-Browser (siehe Abbildung 4-49) lassen sich die Dateien anzeigen. Klicken Sie dazu auf Ihre virtuelle Maschine und wählen Sie dann im rechten Fenster den dort angezeigten Storage mit der rechten Maustaste aus. Wählen Sie dann DATENSPEICHER DURCHSUCHEN.



Sollten dort zwei oder mehr Plattenbereiche angezeigt werden, haben Sie gegebenenfalls noch ein ISO-Image an die VM gebunden, das auf einem anderen Speicherplatz liegt, die Festplatte auf einen anderen Storage gelegt oder die Einstellungen zur Auslagerungsdatei geändert.

[esx5-datastore2] W2K3-32				
Name	Größe	Bereitgestellte Größe	Typ	Geändert
W2K3-32-aux.xml	0,01 KB		Datei	18.10.11 16:20:54
W2K3-32-931881d0....	0,02 KB		Datei	09.09.11 10:08:58
W2K3-32.vmx	2,80 KB		Datei	30.12.11 12:16:35
W2K3-32.vmx	3,00 KB		Virtuelle Maschi...	30.12.11 12:16:35
W2K3-32.vmsd	0,04 KB		Datei	18.10.11 19:04:32
W2K3-32.vmdk	4.820.992,00 KB	15.728.640,00 KB	Virtuelle Festplat...	30.12.11 07:22:29
W2K3-32.nvram	8,48 KB		Nicht flüchtige A...	30.12.11 07:44:51
vmware-8.log	73,51 KB		Protokolldatei der.	29.12.11 11:42:50
vmware-7.log	149,04 KB		Protokolldatei der.	18.10.11 19:04:33
vmware-6.log	65,83 KB		Protokolldatei der.	18.10.11 16:27:46
vmware-5.log	73,57 KB		Protokolldatei der.	17.10.11 18:03:44
vmware-4.log	97,63 KB		Protokolldatei der.	12.09.11 21:25:09
vmware-3.log	96,58 KB		Protokolldatei der.	09.09.11 10:12:40
vmware.log	89,42 KB		Protokolldatei der.	30.12.11 07:44:52

Abbildung 4-49: Fenster des Datastore-Browsers

Im Datenspeicherbrowser klicken Sie im linken Fenster auf das Verzeichnis Ihrer VM, so dass in der rechten Hälfte die Dateien erscheinen. Über das Kontextmenü in der oberen Zeile des Browsers können Sie Spalten hinzufügen oder wegnehmen und mit der linken Maustaste die Sortierung ändern sowie die Spaltengröße anpassen. Beim erneuten Öffnen ist das Fenster aber wieder im alten Zustand.



Die tatsächliche Festplattendatei wird hier zusammen mit ihrer Konfigurationsdatei als eine einzige Datei angezeigt. Auf der Kommandozeile oder mit einem *ssh*-Tool (wie *putty*, *WinCMD*, *Veeam* o. Ä.) sehen Sie dort aber beide Dateien.

Die Dateien im Verzeichnis der VM lassen sich grob in drei Bereiche aufteilen:

- Konfigurationsdateien der virtuellen Maschine
- zugewiesene Festplatten
- Logdateien

In Tabelle 4-5 sehen Sie die möglichen Dateiendungen mit ihrer Bedeutung als Beispiel für die virtuelle Maschine mit Namen *VM1*.

Tabelle 4-5: Dateiendungen bei der VM

Datei	Bedeutung
<i>VM1.vmx</i>	Das ist die eigentliche Konfigurationsdatei, in der u. a. der Anzeigenname, die gewählte Hardware und der Speicherort der virtuellen Maschine vermerkt sind.
<i>VM1.vmx</i> <i>f</i>	Die erweiterte Konfigurationsdatei zur <i>.vmx</i> -Datei. Einzige Datei im XML-Format.
<i>VM1.nvram</i>	Die BIOS- oder EFI-Einstellungen der virtuellen Maschine

Tabelle 4-5: Dateiendungen bei der VM (Fortsetzung)

Datei	Bedeutung
<i>vmware.log</i>	Die Protokolldateien der VM, in der Sie Statusmeldungen, Konfiguration der VM und Weiteres finden (max. Anzahl: 7).
<i>VM1-nnn.hlog</i>	Eine Protokolldatei, die während vMotion Fehler aufzeichnet. Startet die VM nach vMotion, kann die Datei gelöscht werden.
<i>VM1-flat.vmdk</i>	Die eigentliche Festplatte der VM. Darin liegen die Daten des Gastbetriebssystems.
<i>VM1.vmdk</i>	Diese Datei enthält die geometrischen Daten zur Festplatte (Köpfe, Zylinder, Sektoren), den Erstellungstyp und den Namen der Festplattendatei.
<i>VM1-nnn.vmdk</i>	Virtuelle Festplatte, die Änderungen z. B. beim Snapshot festhält
<i>VM1.dsk</i>	Altes, monolithisches Festplattensystem des alten ESXi Servers
<i>VM1.vmdk.redo</i>	Änderungen an der Festplatte werden hier aufgezeichnet. Liegt immer dort, wo auch die Festplatte der VM liegt, außer bei RDM.
<i>VM1-Snapshot1.vmsn</i>	Hauptspeichereinhalt der VM zum Zeitpunkt des Snapshots. Zu jedem Snapshot gibt es eine eigene Datei.
<i>VM1.vmsd</i>	Informationen zu Snapshots. Ohne Snapshot Größe 0.
<i>VM1-nnn.vmss</i>	Virtual Machine Suspend State. Diese Datei enthält den Hauptspeichereinhalt der VM zum Zeitpunkt des Auslösens des Snapshots.
<i>VM1.vmdk.lck</i>	Schreibschutzanzeige zur virtuellen Festplatte
<i>VM1-nnn.vswp</i>	RAM-Auslagerungsdatei der VM. Frühere ESXi-Versionen hatten eine zentrale Swap-Datei, jetzt besitzt jede VM eine eigene.
<i>VM1.vmdk-delta.redo_nnn</i>	Das ist eine Differenzdatei (auch »REDO-Log« genannt). Dabei ist zu beachten, dass Änderungen nach einem erfolgten Snapshot in die Deltadatei(en) geschrieben werden.
<i>VM1.vmtx</i>	Virtual Machine-Template-Datei
nnn = Bezeichner, bestehend aus Buchstaben und/oder Zahlen.	



Es müssen bei Ihren virtuellen Maschinen nicht alle Dateien vorhanden sein. Die *.vswp*-Datei existiert z.B. nur, wenn die Maschine eingeschaltet ist. Die *.vmsn*- und *.vmss*-Dateien sind nur vorhanden, wenn die Maschine »suspended« ist. REDO-Dateien sind nur vorhanden, wenn nicht in die Festplattendatei geschrieben wird, usw.

Die wichtigsten Dateien der virtuellen Maschine sind also folgende:

1. *.vmdk* und *-flat.vmdk* (Festplatte und Konfigurationsdatei zur Festplatte)
2. *.vmx* und *.vmxf* als eigentliche Konfigurationsdateien

Die Dateien *.nvram* und *.vmsd* werden beim Starten der Maschine neu erstellt, falls sie nicht vorhanden sind. Bei jedem Start der VM oder wenn die Datei die maximale Größe erreicht hat, wird eine neue Logdatei geschrieben, wobei die Datei *vmware.log* immer die

aktuelle ist. Die anderen Logdateien werden fortlaufend nummeriert und bei Erreichen der siebten wird jeweils die älteste gelöscht.

Inhalt der .vmx-Datei

Wirft man einen Blick in die Konfigurationsdatei der virtuellen Maschine, wird man einiges von dem wiederfinden, was man bei der Erstellung angegeben hat. Da es sich hier um eine Textdatei handelt, kann sie mit einem Editor, der die Linux-konformen Zeilenwechsel richtig interpretiert, geändert werden. Im Folgenden gehe ich auf einige wichtige Parameter ein.



In der `.vmx`-Datei Ihrer Maschine müssen nicht alle Einstellungen vorhanden sein, und es können auch andere Einträge in dieser Datei stehen. Die Reihenfolge der Einträge habe ich zum Teil geändert. VMware fügt neue Einträge meistens am Ende der Datei ein und ändert auch Einträge und belässt sie an ihrer ursprünglichen Stelle.

Tabelle 4-6: Inhalt der `vmx`-Datei

Eintrag in der Datei	Bemerkung
<code>#!/usr/bin/vmware</code>	Damit wird das Programm angegeben, mit dem diese Datei assoziiert ist. In neuen Versionen nicht mehr benutzt.
<code>.encoding = "UTF-8"</code>	Format der <code>.vmx</code> -Datei
<code>config.version = "8"</code>	Version der Konfigurationsdatei
<code>virtualHW.version = "8"</code>	Angabe, welche virtuelle Hardwareversion in der virtuellen Maschine vorhanden ist
<code>bios.bootDelay = "10000"</code>	Verzögerung der BIOS-/EFI-Meldung
<code>bios.forceSetupOnce = "FALSE"</code>	Beim nächsten Starten ins BIOS-/EFI-Setup gehen
<code>bios.bootRetry.enabled = "TRUE"</code>	Wenn Startgerät nicht gefunden wurde, nach 10 Sekunden erneut versuchen
<code>checkpoint.vmState = ""</code>	Beim Suspend-Modus steht hier der Name der <code>.vmss</code> -Datei.
<code>checkpoint.vmState.readOnly = "FALSE"</code>	Nur-lesen-Modus für die Suspend-Datei
<code>cleanShutdown = "FALSE"</code>	Flag, ob die VM sauber heruntergefahren oder in den Schlafmodus versetzt wurde. Beim Einschalten wird der Wert wieder auf FALSE gesetzt.
<code>deploymentPlatform = "windows"</code>	Zugrunde liegende Hardwareplattform
<code>disable_acceleration = "TRUE"</code>	Hardwarebeschleunigung ausschalten
<code>displayName = "VM1"</code>	Der Anzeigename der virtuellen Maschine
<code>ethernet0.addressType = "generated"</code>	MAC-Adresstyp der ersten NIC

Tabelle 4-6: Inhalt der vmx-Datei (Fortsetzung)

Eintrag in der Datei	Bemerkung
ethernet0.generatedAddress = "00:0c:29:91:a1:5a"	Die MAC-Adresse des ersten Netzwerkadapters. Die ID wird bei mehreren Adaptern hochgezählt.
ethernet0.generatedAddressOffset = "0"	Offset zur generierten MAC-Adresse. Meistens erst bei der zweiten NIC gesetzt.
ethernet0.networkName = "VM Network"	Portgruppenname des Switchs der VM
ethernet0.pciSlotNumber = "32"	Steckplatz der Netzwerkkarte
ethernet0.present = "TRUE"	Angabe, ob ein Netzwerkadapter vorhanden ist. Bei mehreren Adaptern wird die ID hochgezählt.
ethernet0.virtualDev = "e1000"	Art der Netzwerkkarte
evcCompatibilityMode = "FALSE"	Kompatibilitätsmodus für vMotion
extendedConfigFile = "VM1.vmx"	Name der erweiterten Konfigurationsdatei
firmware = "efi"	Typ des Startgeräts (BIOS oder EFI)
floppy0.clientDevice = "TRUE"	Ist Floppy an den vSphere Client-PC angeschlossen?
floppy0.fileName = "/dev/fdo"	Name des Disketten-Image oder des physischen Pfads zum Laufwerk
floppy0.present = "TRUE"	Angabe, ob ein Diskettenlaufwerk vorhanden ist. Bei mehreren Laufwerken wird die ID hochgezählt.
floppy0.startConnected = "FALSE"	Angabe, ob das Diskettenlaufwerk beim Starten angeschlossen sein soll
guestCPUID.0 = "0000000a756e65476c65746e49656e69"	CPU-ID-Maske der VM
guestCPUID.1 = "000006fb00010800800022010febbbff"	
guestCPUID.80000001 = "000000000000000000000000120100800"	
guestOS = "winntenterprise"	
guestOSAltName = "Microsoft Windows Server 2003, Enterprise Edition (32-Bit)"	
hostCPUID.0 = "0000000a756e65476c65746e49656e69"	CPU-ID-Maske des Hosts
hostCPUID.1 = "000006fb000408000000e3bdbfebfbbff"	
hostCPUID.80000001 = "000000000000000000000000120100800"	
hpet0.present = "TRUE"	High Precision Event Timer der Intel-CPU
ide1:0.clientDevice = "TRUE"	IDE Secondary Master am Client
ide1:0.deviceType = "atapi-cdrom"	Art des IDE-Geräts
ide1:0.fileName = ""	Name der CD-ROM-Imagedatei oder des physischen Pfads zum Laufwerk
ide1:0.present = "TRUE"	Angabe, ob ein IDE-Controller vorhanden ist

Tabelle 4-6: Inhalt der vmx-Datei (Fortsetzung)

Eintrag in der Datei	Bemerkung
<code>ide1:0.startConnected = "FALSE"</code>	Angabe, ob das optische Laufwerk beim Einschalten verbunden ist
<code>mem.hotadd = "TRUE"</code>	Hinzufügen von RAM zur Laufzeit
<code>memsize = "2048"</code>	Zugewiesener Hauptspeicher in MByte
<code>monitor.virtual_exec = "hardware"</code> <code>monitor.virtual_mmu = "hardware"</code>	Einträge zur CPU/MMU-Virtualisierung
<code>numvcpus = "2"</code>	Anzahl der zugewiesenen CPUs der VM
<code>nvrAm = "VM1.nvrAm"</code>	BIOS-Datei der VM
<code>parallel0.fileName = "<Pfad/Name>"</code> <code>parallel0.fileType = "file"</code> <code>parallel0.present = "TRUE"</code>	Einstellungen zum Parallelport
<code>pCiBridge0.pCiSlotNumber = "17"</code> <code>pCiBridge0.present = "TRUE"</code> <code>pCiBridge4.functions = "8"</code> <code>pCiBridge4.pCiSlotNumber = "21"</code> <code>pCiBridge4.present = "TRUE"</code> <code>pCiBridge4.virtualDev = "pCiErootPort"</code> <code>pCiBridge5.functions = "8"</code> <code>pCiBridge5.pCiSlotNumber = "22"</code> <code>pCiBridge5.present = "TRUE"</code> <code>pCiBridge5.virtualDev = "pCiErootPort"</code> <code>pCiBridge6.functions = "8"</code> <code>pCiBridge6.pCiSlotNumber = "23"</code> <code>pCiBridge6.present = "TRUE"</code> <code>pCiBridge6.virtualDev = "pCiErootPort"</code> <code>pCiBridge7.functions = "8"</code> <code>pCiBridge7.pCiSlotNumber = "24"</code> <code>pCiBridge7.present = "TRUE"</code> <code>pCiBridge7.virtualDev = "pCiErootPort"</code>	Virtualisierte Steckplätze der vorhandenen PCI-Geräte
<code>powerType.powerOff = "soft"</code> <code>powerType.powerOn = "default"</code> <code>powerType.reset = "soft"</code> <code>powerType.suspend = "hard"</code>	Einstellungen bei den VMware Tools zu den Schaltflächen der virtuellen Maschine
<code>replay.supported = "TRUE"</code> <code>replay.filename = ""</code>	Funktion wird nur unter VMware Workstation unterstützt.
<code>sched.mem.shares</code>	Zugeteilte Shares für den Arbeitsspeicher
<code>sched.cpu.shares</code>	Zugeteilte Shares für den Prozessor
<code>sched.swap.derivedName = "/vmfs/volumes/4b417378-f7511562-e413-001517bf29f8/VM1/VM1-33817e33.vswp"</code>	Name und Ort der Auslagerungsdatei der VM
<code>scsi0.pCiSlotNumber = "16"</code>	Steckplatz des SCSI-Controllers

Tabelle 4-6: Inhalt der vmx-Datei (Fortsetzung)

Eintrag in der Datei	Bemerkung
<code>scsi0.present = "TRUE"</code>	Angabe, ob ein SCSI-Controller in der virtuelle Maschine steckt. Bei mehreren Controllern wird die SCSI-ID hochgezählt.
<code>scsi0.sharedBus = "none"</code>	Angabe, ob der SCSI-Adapter für die gemeinsame Verwendung eingestellt wurde
<code>scsi0.virtualDev = "lsilogic"</code>	Art des SCSI-Bus-Adapters
<code>scsi0:0.deviceType = "scsi-hardDisk"</code>	Typ des ersten Geräts am SCSI-Adapter
<code>scsi0:0.fileName = "VM1.vmdk"</code>	Name des ersten Geräts am SCSI-Adapter
<code>scsi0:0.present = "TRUE"</code>	Angabe, ob erstes Gerät vorhanden ist
<code>scsi0:0.redo = ""</code>	Angabe, ob unabhängiger Modus eingeschaltet ist
<code>svga.autodetect = "TRUE"</code>	Automatisch die Einstellungen der VGA-Karte erkennen
<code>svga.vramSize = "6291456"</code>	Arbeitsspeicher der VGA-Karte, hier 6 MByte
<code>tools.remindInstall = "FALSE"</code>	Tools-Version beim Einschalten überprüfen
<code>tools.syncTime = "FALSE"</code>	Angabe, ob die VMware Tools die Zeit mit dem Wirt abgleichen
<code>tools.upgrade.policy = "useGlobal"</code>	Individuelle oder allgemeine Einstellung zum Upgrade der Tools
<code>usb.pciSlotNumber = "34"</code>	Steckplatz des USB-Hostadapters
<code>usb.present = "TRUE"</code>	Angabe, ob USB vorhanden
<code>usb:0.deviceType = "hid"</code>	Typ des ersten USB-Geräts
<code>usb:0.present = "TRUE"</code>	Erstes USB-Gerät vorhanden
<code>usb:1.deviceType = "hub"</code>	Typ des zweiten USB-Geräts
<code>usb:1.present = "TRUE"</code>	Zweites USB-Gerät vorhanden
<code>usb:1.speed = "2"</code>	Geschwindigkeit, hier USB 2.0
<code>uuid.bios = "56 4d c4 29 f2 b4 42 33-f7 cc b0 bb 57 91 a1 5a"</code>	Eindeutige ID der VM
<code>uuid.location = "56 4d c4 29 f2 b4 42 33-f7 cc b0 bb 57 91 a1 5a"</code>	Erstellungsort der VM
<code>vc.uuid = "52 0f 00 b1 36 2f c0 d7-d4 5c 18 8d 74 fc 16 da"</code>	Eindeutige ID der VM im vCenter Server
<code>vcpu.hotadd = "TRUE"</code>	Hinzufügen von CPUs im laufenden Betrieb
<code>virtualHW.productCompatibility = "hosted"</code>	Kompatibilität der virtuellen Hardware stimmt mit dem Host überein.
<code>monitor.virtual_mmu = "hardware"</code>	Einstellung zur CPU/MMU-Virtualisierung
<code>monitor.virtual_mmu = "hardware"</code>	
<code>vmi.present = "FALSE"</code>	VMI-Paravirtualisierung aktiviert
<code>vmotion.checkpointFBSize = "6291456"</code>	Eintrag für vMotion bezüglich des RAM der Grafikkarte
<code>vmx.buildType = "stats"</code>	Statistiken protokollieren

Tabelle 4-6: Inhalt der *vmx*-Datei (Fortsetzung)

Eintrag in der Datei	Bemerkung
<code>wwn.node = "21de000c2900019b"</code>	Einträge für Fibre-Channel-NPIV
<code>wwn.port = "21de000c2900029b"</code>	
<code>wwn.type = "host"</code>	

Hat man bei der VM unter OPTIONEN das Häkchen bei STATISTIKEN ERFASSEN gesetzt, gibt es im Verzeichnis der Maschine noch ein Unterverzeichnis namens *stats*, in dem sich die zugehörigen Dateien befinden.

Die MAC-Adresse der VM

Die Hardwareadresse der virtuellen Maschine wird beim ersten Starten automatisch generiert und in die *vmx*-Datei eingetragen. Über die grafische Oberfläche können Sie sie einsehen und mittlerweile auch beliebig verändern.

1. Klicken Sie dazu auf die virtuelle Maschine und wählen Sie EINSTELLUNGEN BEARBEITEN aus.
2. Klicken Sie dann auf NETZWERKADAPTER 1 oder einen beliebigen anderen. Im rechten Teil des Fensters sehen Sie dann die automatisch zugewiesene Adresse, meist im Bereich von *00:0c:29:xx:yy:zz*.
3. Ist die Maschine ausgeschaltet, können Sie hier eine manuelle Adresse eintragen. Der Anfangsbereich liegt bei *00:50:56:00:00:00*, also den ebenfalls von VMware erworbenen sechs Stellen.
4. Bei Bedarf können Sie aber eine beliebige 12-stellige MAC-Adresse nach dem obigen Muster (mit Doppelpunkten) eintragen.

Gerade wenn man eine physische Maschine in eine virtuelle konvertiert und die bisherige MAC-Adresse beibehalten muss, kann man hier endlich ohne Probleme die vorige Einstellung eintragen.

Davon unabhängig können Sie natürlich auch diese Einstellungen beim Treiber zur Netzwerkkarte im gestarteten Betriebssystem einstellen (siehe Abbildung 4-50).

Bedenken Sie bei dieser Änderung, dass manche Software die Hardwareadresse der Netzwerkkarte aus deren Konfigurationsport direkt abfragt und sich durch diese Einstellung nicht überlisten lässt. Über den erstgenannten Weg sollte es aber funktionieren.

Bedenken Sie weiterhin, dass doppelt vergebene MAC-Adressen in einem Netzwerk zu erheblichen Problemen führen können und es sehr schwer ist, diesen Fehler zu identifizieren. Ein doppelter Name oder eine bereits vorhandene IP-Adresse wird üblicherweise vom Betriebssystem der Maschine gemeldet – eine doppelte Hardwareadresse leider nicht.

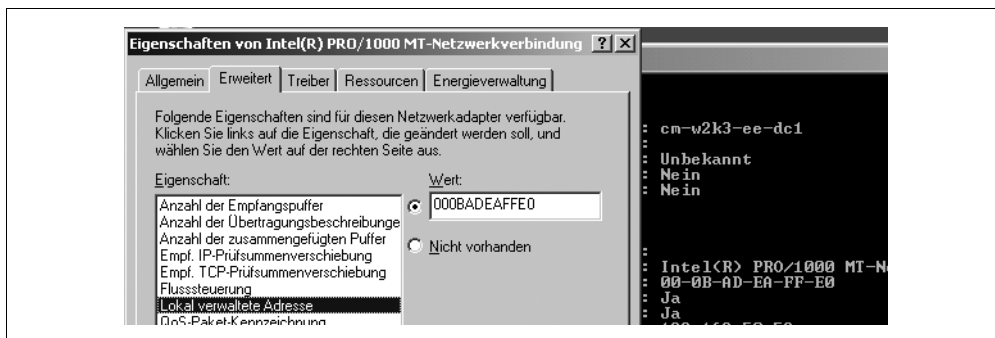


Abbildung 4-50: MAC-Adresse im Betriebssystem ändern

In diesem Kapitel habe ich beschrieben, wie eine virtuelle Maschine richtig erstellt wird, welche Einstellungs- und Wahlmöglichkeiten man dabei hat, worauf es bei den VMware Tools ankommt und wie man nachträglich Änderungen durchführt.

Im nächsten Kapitel werden wir uns nochmals den ESXi Server vorknöpfen und dort genauso detailliert die Einstellungs- und Wahlmöglichkeiten beleuchten.

Konfiguration und Einstellungen des ESXi Servers

Nachdem wir nun mindestens einen laufenden ESXi Server und mindestens eine virtuelle Maschine erstellt und konfiguriert haben, ist es an der Zeit, uns die Konfiguration des Hosts näher anzuschauen.

Beim aktuellen ESXi Server 5.0 können noch diverse weitere Einstellungen gesetzt und verändert werden. Vieles davon war auch schon bei der Vorgängerversion 4.x vorhanden – einige Einstellschrauben sind aber jetzt anders oder neu.

Die meisten dieser Anzeigen und Einstellungsmöglichkeiten – ausgenommen Netzwerk und Speicher (Storage) – werden Sie wohl eher selten benötigen. So wird z. B. der Systemstatus auch als Alarm gemeldet, sollte mal ein Fehler auftreten.

Auch wenn Sie nicht jeden Punkt dieses Kapitels der Reihe nach durchlesen wollen, sollten Sie wenigstens beim ersten ESXi Server Folgendes einer genaueren Betrachtung unterziehen:

- **HARDWARE – PROZESSOREN:** Hier sollten Sie je nach vorliegenden physischen CPUs das Hyperthreading überprüfen und es gegebenenfalls im BIOS/EFI und an diesem Punkt einschalten.
- **SOFTWARE – DNS UND ROUTING:** Sind alle gemachten Angaben während der Installation korrekt eingetragen worden, oder hat sich im Laufe der Zeit vielleicht die IP-Adresse eines DNS-Servers verändert?
- **SOFTWARE – UHRZEITKONFIGURATION:** Stimmen die Angaben zum NTP-Server? Beachten Sie auch unbedingt die Einstellungen bei den VMware Tools innerhalb der VMs. Beachten Sie dazu auch die Angaben in Kapitel 4.
- **HOCH-/HERUNTERFAHREN VIRTUELLER MASCHINEN:** Ist nur sinnvoll auf einem allein stehenden ESXi Server, da es so eine Einstellung leider nicht über den vCenter Server gibt. Schauen Sie sich dazu im Kapitel 9 das Skript für USV/UPS an, ob dieses in Ihrer Umgebung das Tool der Wahl ist.

Ich werde in der Reihenfolge der Einträge in den beiden Abschnitten **HARDWARE** und **SOFTWARE** die Punkte mit kurzen Hinweisen erläutern, die man bei der Grundkonfiguration beachten sollte.



Den beiden großen und wichtigen Themen »Netzwerk« und »Storage« (Speicher) sind mit den Kapiteln 6 und 7 zwei eigene Kapitel gewidmet, in denen sehr detailliert mit Beispielen auf sie eingegangen wird.

Hardwareeinstellungen des ESXi Servers

Sieht man von den beiden wichtigsten Bereichen Netzwerk- und Speichertechnik ab, die ich in den nächsten Kapiteln detailliert besprechen werde, gibt es hier nur sehr wenig, das man einstellen oder ändern muss (siehe auch die Aufzählung oben).

Der Vollständigkeit halber gehe ich aber kurz auf die einzelnen Punkte ein, die in Abbildung 5-1 gezeigt werden.

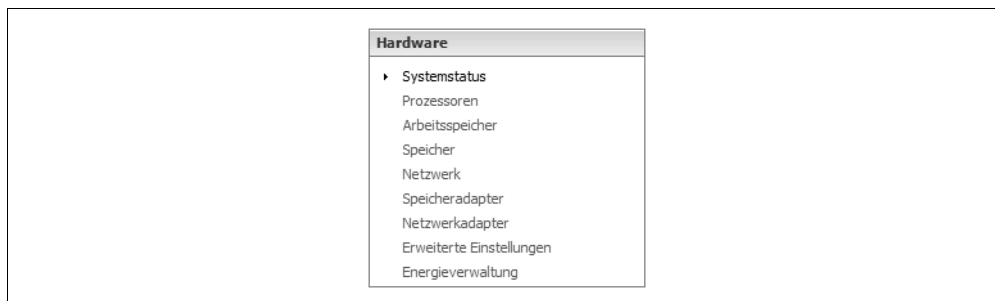


Abbildung 5-1: Konfiguration – ESXi Hardware

Hardwaresystemstatus

Bei den von VMware zertifizierten Servern erscheinen hier mehr oder weniger viele Angaben zu den Geräten und Treibern. Am einfachsten vergleicht man die Anzeige mit dem Hardwarestatus im BIOS eines Rechners, bei dem man ebenfalls keine Einstellungen vornehmen kann. Üblich sind hier Angaben zu Prozessoren, Arbeitsspeicher, Lüftern, Netzwerkkarten, BIOS und weiteren Geräten, an die Sensoren angeschlossen oder darin integriert sind. Dazu zählen auch diverse Temperaturen und Umdrehungszahlen, die vom ESXi Server ausgelesen und grafisch dargestellt werden. Die Zuverlässigkeit der Anzeige beruht auf den jeweiligen Sensoren, nicht auf der Abfragesoftware, die das SMASH-Profil (*Systems Management Architecture for Server Hardware*) dafür nutzt.

Per Link oben rechts in der Ecke sind die AKTUALISIERUNG der Anzeige und das ZURÜCKSETZEN der Sensoren möglich. Wird ein Status ungleich NORMAL festgestellt, wird dieses in Gelb oder – schlimmer! – in Rot dargestellt. Die Schwellenwerte für Gelb und Rot las-

sen sich nicht einstellen. Ist in dieser Spalte nichts aufgeführt, kann der Wert nicht ermittelt werden.



Wenn der ESXi Server Mitglied beim vCenter Server ist, gibt es das zusätzliche Plugin vCenter-Hardwarestatus, das dann auch Alarime versenden kann, z. B. per Mail oder SNMP-Trap (dazu später mehr in Kapitel 10).

Hardware – Prozessoren

Unter diesem Punkt werden die installierten Prozessoren mit Typ, Anzahl der Kerne, Geschwindigkeit und Anzahl der Sockel angezeigt. Die Summe der logischen Prozessoren ergibt sich aus der Anzahl der Sockel mal Anzahl der Kerne. Haben Sie, wie in Abbildung 5-2 gezeigt, nur einen Sockel, reicht eine Lizenz aus. Bei zwei Sockeln benötigen Sie zwei Lizenzen, usw. Die Anzahl der Kerne pro Sockel oder der logischen CPUs spielt dabei zunächst keine Rolle.

Prozessoren		
Allgemein		
Modell	Intel(R) Xeon(R) CPU	X3440 @ 2.53GHz
Prozessorgeschwindigkeit	2,5 GHz	
Prozessor-Sockets	1	
Prozessor-Cores pro Socket	4	
Logische Prozessoren	8	
Hyper-Threading	Aktiviert	

Abbildung 5-2: Prozessoren des ESXi Servers

Hyperthreading

Das von Intel erfundene Hyperthreading, das als Erstes bei einigen XEON-CPU's ab Anfang 2002 und später in Pentium-4-Prozessoren eingesetzt wurde, wird aktuell wieder in den neuen Core i7- und XEON-CPU's genutzt.

Es handelt sich dabei aber nicht um zwei echte Rechenkerne, sondern es wird nur ein zusätzlicher Registersatz und ein APIC (*Advanced Programmable Interrupt Controller*) verwendet. Mengenmäßig erweitert Intel den Prozessor dadurch um 1 % mehr Transistoren, ohne den Cache zu erhöhen, auf den beide Teile zugreifen.

Für die Virtualisierung bringt das Hyperthreading eine bessere Verteilung der Lasten. Da nicht jede Anwendung innerhalb einer VM damit klarkommt, kann es individuell in den jeweiligen Einstellungen abgeschaltet werden.

Die Höchstanzahl der logischen CPUs ist auf 160 pro Host beschränkt. Davon können einer virtuellen Maschine je nach Lizenz maximal 32 zugeteilt werden. Sie können bis zu 2.048 virtuelle Prozessoren pro Host an Gäste verteilen. Im Dialogfeld EIGENSCHAFTEN

können Sie gegebenenfalls Hyperthreading aktivieren oder deaktivieren – lesen Sie im Kasten Seite 115 mehr zum Thema »Hyperthreading«. Durch Hyperthreading verdoppelt sich die Anzahl der logischen Prozessoren, nicht aber die Leistung – die wird im besten Falle um ca. 6–10% erhöht.

Im unteren Teil des rechten Fensters kann das Startgerät des ESXi Servers über STARTOPTIONEN für den nächsten anstehenden Boot ausgewählt werden. Das funktioniert aber nur, wenn man das in Abbildung 5-3 gezeigte Kästchen angeklickt hat und bei Auswahl von OK sofort neu startet.

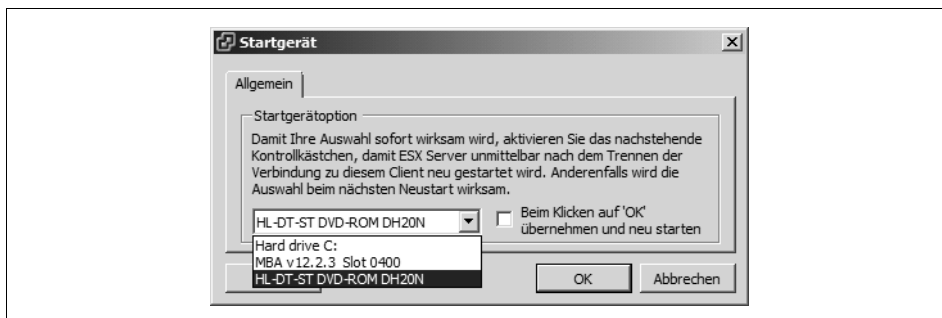


Abbildung 5-3: Startoptionen des ESXi Servers

Hardware – Arbeitsspeicher

Hier werden der gesamte Arbeitsspeicher, das vom System benutzte RAM und das für die virtuellen Maschinen zur Verfügung stehende RAM aufgelistet. Beachten Sie dabei, dass unter der Registerkarte RESSOURCENZUTEILUNG deutlich weniger Arbeitsspeicher als Gesamtkapazität für die VMs zur Verfügung steht. Warum das so ist, sehen Sie unter dem Punkt SOFTWARE – ZUTEILUNG VON SYSTEMRESSOURCEN.

Hardware – Erweiterte Einstellungen

Ab vSphere4 unterstützt ESXi eine direkte PCI-Geräteverbindung (DirectPath-I/O-Konfiguration) für virtuelle Maschinen, die auf Intel Nehalem- oder AMD-V-Plattformen ausgeführt werden. Dazu muss im BIOS des Hosts die Funktion von Intel (VT-d) oder AMD (IOMMU) eingeschaltet sein. Jede virtuelle Maschine mit Hardwareversion 7 oder 8 kann mit bis zu sechs Passthrough-Geräten verbunden werden. Die Einstellungen finden Sie unter ESXi-HOST → KONFIGURATION → ERWEITERTE EINSTELLUNGEN.

Die folgenden Funktionen sind nicht für virtuelle Maschinen verfügbar, die mit VM-DirectPath konfiguriert sind:

- vMotion und DRS (Ausnahme: Ein Distributed Virtual Switch von Cisco oder ihre Lizenz beinhaltet Direct Path vMotion.)
- Hinzufügen und Entfernen von virtuellen Geräten im laufenden Betrieb

- Anhalten und Fortsetzen (Suspend und Resume)
- Snapshots können nicht erstellt, wiederhergestellt oder übernommen werden.
- Fehlertoleranz (Fault Tolerance)
- Hohe Verfügbarkeit (High Availability)
- DRS, also Performance-Balancing (Eingeschränkte Verfügbarkeit; die virtuelle Maschine kann Teil eines Clusters sein, aber nicht über Hosts hinweg migriert werden.)

Auf der Seite PASSTHROUGH-KONFIGURATION (siehe Abbildung 5-4) werden alle verfügbaren Passthrough-Geräte aufgelistet. Das können PCI- und PCIe-Geräte sein. Ein grünes Symbol bedeutet, dass ein Gerät aktiviert und aktiv ist. Ein orangefarbenes Symbol zeigt, dass sich der Status des Geräts geändert hat und der Host neu gestartet werden muss, bevor das Gerät verwendet werden kann.

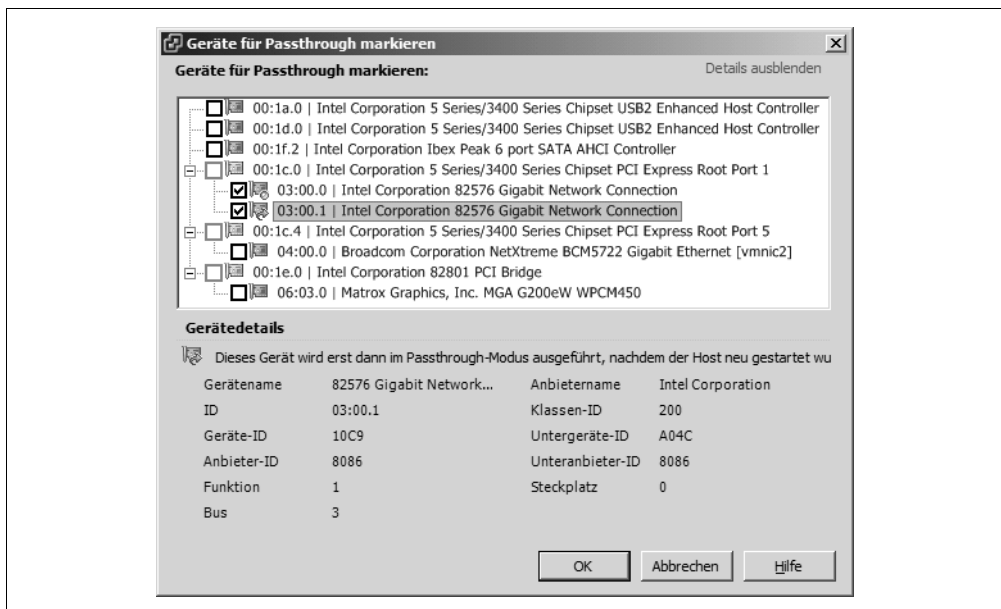


Abbildung 5-4: Passthrough-Geräte

Wenn Sie hier ein Gerät aktivieren, steht es nach dem Neustart des Hosts den Gästen zur Verfügung. Dort können Sie dann beim Gast unter EINSTELLUNGEN BEARBEITEN → HARDWARE → HINZUFÜGEN → PCI-GERÄT diese Komponente der virtuellen Maschine hinzufügen.



Nicht jede Serverhardware bietet diese Funktion. Bei einigen in der Kompatibilitätsliste stehenden Rechnern wird diese Funktion nicht angeboten. Achten Sie auf die BIOS-Einstellungen Intel VT-d und AMD IOMMU.

Für die VM wird der Arbeitsspeicher automatisch vollständig als reserviert eingetragen.

Hardware – Energieverwaltung

Je nachdem, welche Prozessoren im ESXi Server werkeln, kann hier die Energieverwaltung des Hosts in vier verschiedenen Modi eingestellt werden. Über den Link **EIGENSCHAFTEN** oben rechts öffnet sich ein neues Fenster mit den Auswahlmöglichkeiten. Sollten Sie in dem Fenster eine Änderung machen, wird diese nicht sofort angezeigt, sondern erst wenn Sie auf **AKTUALISIEREN** geklickt haben. Sollte die Funktion im BIOS nicht aktiviert sein, sehen Sie nur den Hinweis, dass sie nicht unterstützt wird. Bei HP-Servern nennt sich das Energiemanagement übrigens »Cooperative Power Management«.

Softwareeinstellungen des ESXi Servers

Im Abschnitt **SOFTWARE** werden die Konfigurationsoptionen wie in Abbildung 5-5 angezeigt. Auch auf diese Punkte werde ich kurz eingehen.

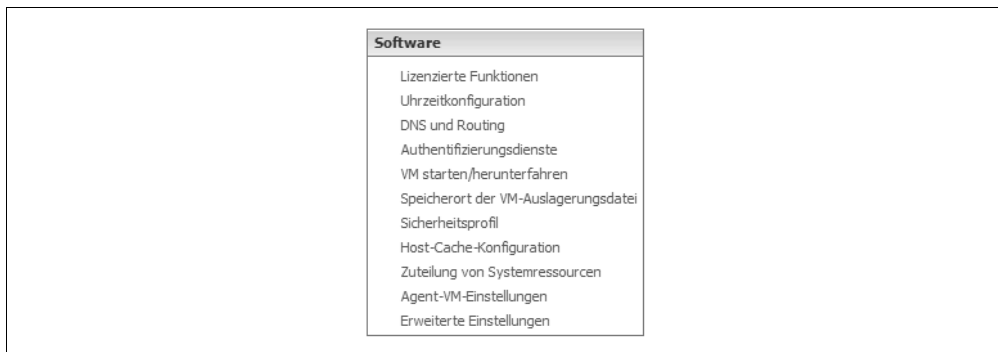


Abbildung 5-5: Konfiguration – ESXi Software

Software – Lizenzierte Funktion

Zeigt den aktuellen Lizenzierungsstatus in der virtuellen Infrastrukturumgebung an. Dazu zählen Lizenzquellen, Lizenzserver oder -datei, Lizenztyp und Add-on-Lizenzierung, z.B. vMotion, HA (High Availability), Fault Tolerance oder DRS (Performance Balancing). Oben rechts finden Sie den Link **BEARBEITEN**, den Sie auswählen können, um dem Host einen neuen oder anderen Lizenzschlüssel zuzuweisen. Auch können Sie hier Lizenzquelle, Lizenztypen und Lizenzierung für zusätzliche Funktionen angeben. Manchmal funktioniert die Eingabe von Lizenzen hier nicht; gehen Sie in diesem Fall über **HOME** → **LIZENZIERUNG**, damit es klappt (nur über den vCenter Server).



Bedenken Sie bitte, dass Sie nach der Testzeit Ihre Lizenzen einspielen müssen, sonst können Sie Ihre VMs nicht mehr starten. Haben Sie Funktionen während der Testzeit konfiguriert, die Ihre tatsächliche Lizenz nicht abdeckt, müssen Sie dies erst rückgängig machen, also z.B. die Portgruppe für vMotion erst löschen, wenn Ihr Vertrag keine vorsieht.

Lizenzierte Funktionen
ESX Server-Lizenztyp
Produkt: Testmodus Läuft ab: 17.02.12
Produktfunktionen:
Bis zu 32-Wege-Virtual SMP
vCenter-Agent für VMware-Host
vStorage-APIs
VMsafe
vSphere HA
Virtuelle Hardware, die im laufenden Betrieb ausgewechselt werden kann
vMotion
vSphere FT
vSphere Data Recovery
vShield-Zonen
vSphere DRS
Storage vMotion
MPIO / Multi-Pathing von Drittanbietern
vSphere Distributed Switch
Hostprofile
Virtueller Konzentrador des seriellen Remoteports
Storage I/O Control
Direct Path vMotion
vAAI
Gemeinsam genutztes Smartcard-Lesegerät
Speicher-DRS
Profilgesteuerter Speicher
vMotion Metro
vSphere Auto Deploy
vSphere View Accelerator

Abbildung 5-6: Übersicht über lizenzierte Funktionen

Einiges von dem, was in Abbildung 5-6 zu sehen ist, ist selbsterklärend (z.B. dass »32-Wege-Virtual-SMP« bedeutet, dass es für die VM mit symmetrischem Multiprozessoring bis zu 32 CPUs gibt), andere Funktionen wie vMotion, HA, Fault Tolerance, Data Recovery und DRS werden wir noch detailliert besprechen. Deshalb erkläre ich hier nur die nicht ganz eindeutigen Produktfunktionen.

vCenter-Agent für VMware Host

Hier ist nur der Agent zum ESXi Server gemeint, der gebraucht wird, wenn der Host zum vCenter Server hinzugefügt wird. Dieser wird durch den vCenter Server aktiviert und konfiguriert.

vStorage-APIs

Softwareschnittstelle für SAN-Anbieter, um z.B. das Multipathing, die Sicherheit oder ein Backup besser unterstützen zu können.

VMsafe

Erlaubt das Hinzufügen von zusätzlichen Sicherheitsprodukten von Drittanbietern, die dann in Zusammenarbeit mit der Virtualisierungsschicht eine höhere Sicherheit für den Server und die Gäste gewährleisten. McAfee und TrendMicro waren die ersten Hersteller, die eine Antivirenlösung für diese Schnittstelle anboten. Eine zusätzliche Software in der VM ist dann obsolet.

vSphere Data Recovery

Die Backup-Appliance von VMware wird in Kapitel 16 ausführlich beschrieben.

vShield-Zonen

vShield-Zonen ist eine Art Firewall für die virtuellen Maschinen. Sie erleichtern die Sicherheit über Policies bei Anwendungen in verteilten Umgebungen über Netzwerksegmentierung von Benutzern und sensiblen Daten.

MPIO/Multi-Pathing

Arbeitet im Zusammenhang mit vStorage-APIs. Auch hier geht es um eine Software-schnittstelle für verteilte Zugriffe auf einen gemeinsamen Storage.

DVfilter

Der interne Name für DVfilter ist vNetwork Appliance API, was die Funktion besser beschreibt. Hier geht es um die Netzwerksicherheit, die mit VMsafe zusammenarbeitet, bezüglich der verteilten virtuellen Switches (vSphere Distributed Switch).

vAAI

vAAI, *vSphere Storage API for Array Integration*, ist ebenfalls eine Softwareschnittstelle für SAN-Hersteller.

vMotion Metro

Ein vMotion über große Strecken, die eine hohe Latenzzeit hat, wird über vMotion Metro abgewickelt. Diese Funktion ist automatisch aktiviert, wenn sie in der eingegebenen Lizenz enthalten ist, und lässt sich nicht weiter konfigurieren.

vSphere View Accelerator

Eine Funktion für VMware View, die Desktops für Anwender zur Verfügung stellt. Damit wird für das Produkt View eine Caching-Option zur Verfügung gestellt, die Master-Images im RAM hält und damit deutlich schneller darauf basierende Desktops starten und ausführen kann.

Software – Uhrzeitkonfiguration

Hier werden die auf dem ESXi Server gesetzte Uhrzeit – umgerechnet auf die eingestellte Zeitzone des Clients – und das Datum angezeigt. Geben Sie möglichst direkt nach der Installation einen NTP-Server an, mit dem sich der Host aktualisiert. Dafür kann z. B. die Rolle des PDC-Emulators des ersten Windows-Domänencontrollers genutzt werden (siehe auch »VMware Tools anpassen« im Kapitel 4).

Software-DNS und Routing

Zeigt DNS- und Routing-Informationen an (siehe Abbildung 5-7). Dazu zählen Servername und -domäne, DNS-Server, die an den Server angeschlossen sind, Suchdomänen und Standard-Gateways. Im Dialogfeld EIGENSCHAFTEN können Sie diese Identifikationselemente angeben und ändern. Wenn Sie den Namen oder die Domäne des ESXi Servers ändern, müssen Sie den Host nicht neu starten.

DNS und Routing	
Hostidentifikation	
Name	esx1
Domäne	gfu.dom
DNS-Server	
Methode	Statisch
Bevorzugter DNS-Server	192.168.50.10
Alternativer DNS-Server	
Domänen suchen	
gfu.dom	
Standard-Gateways	
VMkernel	192.168.50.10

Abbildung 5-7: DNS und Routing

Authentifizierungsdienste

Es besteht die Möglichkeit, den ESXi Server in die Active Directory Zone mitaufzunehmen. Das hat den Vorteil, dass Sie für User im AD Berechtigungen vergeben können. Gehört der Host zu einem vCenter Server, brauchen Sie das nicht zu tun, weil die Berechtigungen dann über dieses Mitglied der Domäne erledigt werden. Der Host trägt sich dabei als Computer ins AD ein – ein Eintrag im DNS wird dadurch aber nicht erstellt.

VM starten/herunterfahren

Zeigt eine Liste virtueller Maschinen auf dem Server an und ob diese beim Start des ESXi Servers hoch- oder heruntergefahren werden sollen. Im Dialogfeld EIGENSCHAFTEN müssen Sie zunächst die Automatik über das Kontrollkästchen aktivieren, um Einstellungen machen zu können. Das Fenster teilt sich in zwei Bereiche, von denen der obere die allgemeinen Einstellungen betrifft und der untere der Einstellung der expliziten Konfigurationen der einzelnen VMs dient.

Hier können Sie einstellen, wann die jeweilige virtuelle Maschine in welcher Abhängigkeit zu einer anderen VM auf dem Server ein- oder ausgeschaltet wird oder in den Suspend-Modus geht. Die Optionen umfassen unter anderem das Starten oder Anhalten zu bestimmten Zeitpunkten in Relation zum Ein- und Ausschalten des ESXi Servers.



Wenn Sie eine USV (unterbrechungsfreie Stromversorgung) oder UPS (*Uninterruptible Power Supply*) einsetzen, sollten Sie Überlegungen zu jeder einzelnen Maschine anstellen: Exchange- und Datenbankserver sind wahrscheinlich schneller im Suspend-Modus als heruntergefahren. Gegebenenfalls sollten Sie die VMware Tools nutzen und eigene Skripten für das Beenden von Diensten anlegen. Erfahrungsgemäß fährt z.B. ein Exchange-Server schneller herunter, wenn die betroffenen Dienste über die Kommandozeile mit `net stop <service>` beendet werden.

VMs ohne VMware Tools können nicht heruntergefahren werden – schicken Sie diese in den Suspend-Modus.



Wenn Sie den ESXi-Host in den vCenter Server aufnehmen, wird dieser Dialog wieder deaktiviert. Sie können ihn anschließend erneut aktivieren oder z.B. HA für den Neustart der VMs konfigurieren. Wirklich helfen wird Ihnen das aber nicht, weil die VMS ja vielleicht auf einem anderen Server landen. So eine Einstellung gibt es im vCenter Server leider nicht (siehe dazu »Skripten« in Kapitel 9).

Software – Speicherort der VM-Auslagerungsdatei

Wie in Kapitel 4 ausführlich erklärt wurde, wird beim Einschalten einer virtuellen Maschine üblicherweise in ihrem Verzeichnis auf dem Storage eine Auslagerungsdatei in der Größe des Arbeitsspeichers angelegt und beim Ausschalten wieder gelöscht. Hier kann man den Speicherort dieser Datei für alle VMs auf dem Host ändern – und bei einer einzelnen Maschine dieses wieder außer Kraft setzen.

Software – Sicherheitsprofil

Zeigt die Firewall-Informationen für eingehende und ausgehende Verbindungen an. Hier sind nur die notwendigen Funktionen für den Betrieb des ESXi Servers enthalten. Diese Firewall betrifft nicht die virtuellen Maschinen!

Alles, was Sie im EIGENSCHAFTEN-Fenster nicht finden, können Sie auch nicht ändern. Durch VMsafe können Drittanbieter auf dem ESXi Server Software bereitstellen, die dann die Firewall-Einstellungen erweitert.

Üblicherweise werden Ports automatisch geöffnet, wenn ein Agent aktiviert wird, z. B. bei NTP oder Software-iSCSI. Die Firewall lässt übrigens ICMP-Pakete für Ping durch, und die Netzwerkkarte antwortet auch.

Über die Eingabeaufforderung können Firewall-Einstellungen in der Datei `/etc/vmware/firewall/service.xml` konfiguriert werden. Dabei können vordefinierte Dienste wie `ntpClient` verändert oder auch beliebige andere definiert werden. Auch die Ports für FTP finden Sie hier.

Besser ist es jedoch, eine eigene XML-Datei in diesem Verzeichnis zu erstellen, um so den Überblick über die Veränderungen zu behalten. Erstellen Sie z.B. eine Datei namens *SMB.xml*, um den Zugriff auf Windows-Freigaben zu regeln. Halten Sie sich dabei an das Muster, wie es in der Datei *service.xml* definiert ist. Die Datei muss jeweils mit dem Eintrag `<ConfigRoot>` anfangen. Dann kommt eine Service-ID, falls Sie mehrere Regeln erstellen wollen, und dann der Name der ID (`<id>SMB</id>`) usw.

Am Ende der Datei muss `</ConfigRoot>` stehen. Sind Sie mit der Datei fertig, müssen Sie noch die Firewall aktualisieren. Das können Sie auf der Kommandozeile mit folgendem Befehl erreichen:

```
esxcli network firewall refresh
```

Über den vSphere Client sehen Sie die Änderungen anschließend erst, nachdem Sie auch hier auf den Link **AKTUALISIEREN** geklickt haben (siehe Abbildung 5-8).

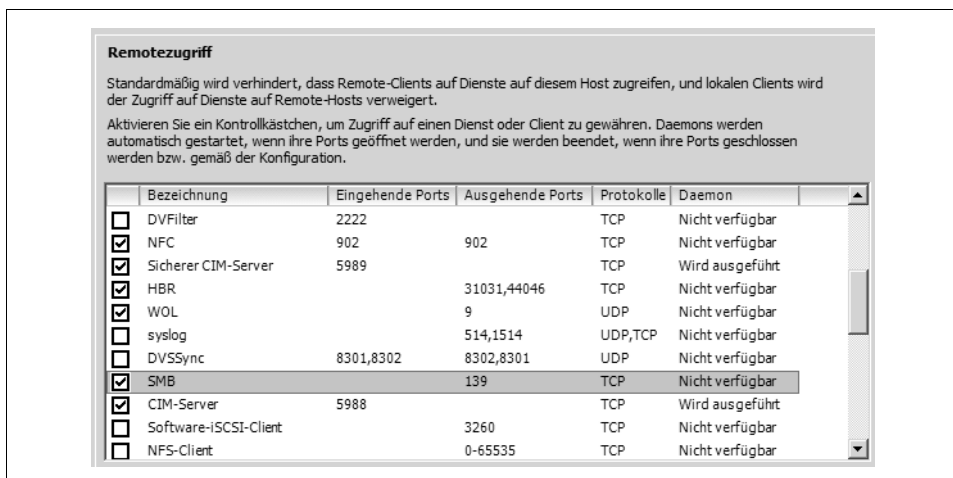


Abbildung 5-8: Ergänzte Firewall-Einträge

Möchten Sie einige Zugriffe nur über bestimmte IP-Adressen oder Subnetze zulassen, können Sie auf der grafischen Oberfläche über den Link **EIGENSCHAFTEN** die jeweilige Bezeichnung auswählen und anschließend auf den Button **FIREWALL...** klicken. Standardmäßig sind die Zugriffe aus allen Subnetzen erlaubt. Sind in der Firewall Dienste für den jeweiligen Port zuständig, können Sie in diesem Fenster über den Button **OPTIONEN...** die Startart einstellen oder auch den Dienst neu starten.

Sollten Sie auf dem ESXi Server zusätzliche Pakete (VIB-Dateien) installieren wollen, dann beachten Sie die Akzeptanzebene im unteren Teil bei der Firewall. Die VIB-Dateien beinhalten Signaturen, die die Installation beim gewählten Profil ermöglichen können oder auch nicht.



Die Änderungen an dieser Stelle können das Updaten des ESXi Servers ggf. nachteilig beeinflussen, denn die Firmware-Updates und Patches sind ebenfalls VIB-Dateien.

Software – Host-Cache-Konfiguration

Wenn Ihr Host eine SSD-Festplatte besitzt, können Sie diese als schnellen Zwischenspeicher für Ihre VMs nutzen. Eine Auslagerungsdatei der virtuellen Maschine wird trotzdem in ihrem Verzeichnis erstellt, aber die Geschwindigkeit des jeweiligen Storage ist dann nicht mehr so wichtig. Dieser sehr schnelle Cache wird vom ESXi für alle VMs genutzt, aber von jeder nur zu einem geringen Teil, weil ja die Kapazität einer SSD noch eher gering ist. Andere Storages als SSD können hier nicht verwendet werden.

Software – Zuteilung von Systemressourcen

Wie bereits bei der Ressourcenzuteilung der virtuellen Maschine erwähnt, hat der ESXi Server ebenfalls Einstellungen zu Arbeitsspeicher und CPU-Zeit. Dieser Punkt zeigt die Einstellungen für die Ressourcenzuteilung des Servers an. In den Dialogfeldern für die Bearbeitung können Sie den CPU- und Speicheranteil konfigurieren, der für den Host reserviert wird. Im Dialogfeld zum Umschalten zwischen EINFACH und ERWEITERT können Sie die Systemressourcenpools des Servers sowie den für ausgewählte Serverfunktionen reservierten Speicheranteil anzeigen lassen. Eine Änderung sollten Sie nur in Zusammenarbeit mit dem VMware-Support vornehmen.



Die Änderungen an dieser Stelle können das Laufzeitverhalten des ESXi Servers sehr nachteilig beeinflussen – lassen Sie deshalb die Standardeinstellungen besser so, wie sie sind!

Software – Agent-VM-Einstellungen

Zeigt eine Liste installierter Appliances auf dem ESXi Server an. Das sind üblicherweise fertig konfigurierte Maschinen, die im OVF-Format heruntergeladen und installiert werden können. Über den Link PROPERTIES... können dann der Datenspeicher und das Netzwerk für diese Appliance festgelegt werden.

Software – Erweiterte Einstellungen

Zeigt eine Liste von Einstellungen an, deren Verwendung von VMware nur dann empfohlen wird, wenn der technische Support von VMware Sie dabei anleitet.



Auch hier sollten Sie ohne konkrete Hinweise vom VMware-Support keine Änderungen vornehmen. Im Verlaufe des Buches werde ich noch die eine oder andere Option besprechen.

Die in der Hilfe zum vSphere Client angezeigte Konfigurationsdatei existiert nicht! Es war in der Vorgängerversion noch ein Verzeichnis mit sehr vielen Dateien, das jetzt nicht mehr vorhanden ist. Sie finden Ihre Änderungen in der Datei *esx.conf* im Verzeichnis */etc/vmware/*.

Wie Sie bis hierher in diesem Kapitel erfahren haben, ist die Konfiguration des ESXi Servers – abgesehen von Netzwerk und Speicher (Storage) – keine große Sache. Beachten Sie aber bitte die wichtigen Hinweise und Warnungen, die ich zu den einzelnen Punkten gegeben habe.

In den bisherigen Kapiteln und Seiten haben Sie schon einige Informationen über den ESXi Server erhalten. Er bietet aber noch weitere Einstellungen auf den Registerkarten und im Menü, auf die ich nun zu sprechen kommen werde.

Registerkarten des ESXi Servers

Auf den Registerkarten werden vielerlei Übersichten, Informationen, Listen und mögliche Konfigurationen angezeigt, auf die ich in diesem Abschnitt näher eingehe. Beachten Sie, dass ein Teil der Informationen hier schon sichtbar ist, obwohl sie nur in Verbindung mit dem vCenter Server Sinn ergeben und auch dann erst anwählbar sind. Andere Informationen wiederum sind später, wenn der ESXi Server über den vCenter Server gemanagt wird, nicht mehr vorhanden, z. B. lokale Benutzer und Gruppen.

Registerkarte »erste Schritte«

Dieses Register ist für den ersten Kontakt mit den Elementen gedacht, die in der Oberfläche angezeigt werden. Nach dem einmaligen Durchlesen möchte man diese Informationen aber meistens nicht mehr sehen. Sie können diese Karten alle auf einmal ausblenden, wenn Sie oben im Menü auf den Eintrag BEARBEITEN klicken, dann CLIENTEINSTELLUNGEN auswählen und das Häkchen im unteren Teil des Fensters bei REGISTERKARTEN »ERSTE SCHRITTE« ANZEIGEN herausnehmen. Diese Änderung betrifft nur den PC, an dem Sie sitzen, und wird lokal abgespeichert.

Registerkarte »Übersicht«

In dieser Darstellung werden die wichtigsten Informationen über den Host dargestellt. Hier erscheint im oberen Teil ggf. die Meldung KONFIGURATIONSPROBLEME, wenn Sie den Remote-Zugang und die ESXi-Shell zugelassen haben.

Das Fenster teilt sich ansonsten in fünf Bereiche, die jeweils zusammengehörige Anzeigen gruppieren. Der letzte Bereich HOSTVERWALTUNG ist jedoch nur ein Link auf die Internetseite von VMware, von der man sich die Software für den vCenter Server herunterladen kann.

Gruppe Allgemein

In dieser Gruppe (siehe Abbildung 5-9) wird zunächst die Hardware samt Hersteller und Modell aufgeführt, dazu der Lizenzmodus. Die angezeigten Prozessorsocket sind für die Lizenzierung wichtig, denn es wird eine Lizenz pro Prozessorsocket nötig, unabhängig von den Prozessorkernen. Mehr Informationen zu Ihrer lizenzierten Version finden Sie auf der Registerkarte KONFIGURATION im Abschnitt SOFTWARE → LIZENZIERTE FUNKTIONEN (wie bereits oben beschrieben).

Allgemein	
Hersteller:	HP
Modell:	ProLiant DL360 G7
CPU-Kerne:	8 CPUs x 2,666 GHz
Prozessortyp:	Intel(R) Xeon(R) CPU E5640 @ 2.67GHz
Lizenz:	Testmodus
Prozessor-Sockets:	2
Kerne pro Socket:	4
Logische Prozessoren:	16
Hyper-Threading:	Aktiv
Anzahl an Netzwerkkarten:	8
Zustand:	Verbunden
Virtuelle Maschinen und Vorlagen:	2
VMotion aktiviert:	Nicht verfügbar
VMware EVC-Modus:	Nicht verfügbar
Host für die Fehlertoleranz konfiguriert:	Nicht verfügbar
Aktive Aufgaben:	
Hostprofil:	Nicht verfügbar
Profil-Übereinstimmung:	 Nicht verfügbar

Abbildung 5-9: Allgemeine Informationen zur ESXi-Hardware

Die Anzahl der logischen Prozessoren ergibt sich aus der Anzahl der Sockel mal der Kerne plus gegebenenfalls Hyperthreading. Haben Sie also 4 Intel Xeon-Prozessoren mit jeweils 8 Kernen und aktiviertem Hyperthreading, sollte bei logischen Prozessoren die Anzahl 32 stehen. Davon können je nach Lizenz bis zu 32 der virtuellen Maschine gegeben werden.

Die notwendige oder empfohlene Anzahl der Netzwerkkarten hängt vom gewünschten Einsatz des ESXi Servers ab. Hier sind beim Einzelbetrieb mindestens zwei Karten erforderlich, beim Einsatz über den vCenter Server im Cluster sollten es mindestens drei sein. Für bestimmte Aufgaben, z.B. iSCSI-SAN- oder NFS-Storage-Anbindung, vMotion und

Fault Tolerance, wird jeweils mindestens eine dedizierte NIC empfohlen. Beachten Sie dazu auch die Hinweise in Kapitel 6 zu den vSwitches mit Teaming von Adaptern.

Die unteren Einträge auf der Seite betreffen einen allein stehenden ESXi Server gar nicht, sondern werden erst relevant, wenn dieser in den vCenter Server aufgenommen wurde. Deshalb gehe ich erst ab Kapitel 10 darauf ein.

Gruppe Befehle

Die Befehle (siehe Abbildung 5-10), die Sie über die jeweiligen Links erreichen, bekommen Sie auch über das Kontextmenü des Servers und das Pull-down-Menü. Wie Sie eine NEUE VIRTUELLE MASCHINE erstellen, wurde bereits ausführlich besprochen, und wie ein NEUER RESSOURCENPOOL anzulegen ist, erfahren Sie in Kapitel 10.

Für IN DEN WARTUNGSMODUS WECHSELN müssen alle virtuellen Maschinen ausgeschaltet oder im Suspend-Modus (angehalten) sein. Ist der Server in einem Cluster unter dem vCenter Server, werden die VMs gegebenenfalls mittels DRS automatisch auf andere ESXi Server verschoben (vMotion). Der Wartungsmodus bewirkt auf einem einzelnen ESXi Server, dass keine VMs mehr hochfahren oder aus dem Suspend-Modus geholt werden können. Der Wechsel in den Wartungsmodus findet erst statt, wenn alle Maschinen aus sind. Dann können auch weder Maschinen erstellt noch ähnliche Aktionen durchgeführt werden. Die jeweiligen Menüs und Anzeigen werden auf das dann noch Mögliche reduziert bzw. geändert.

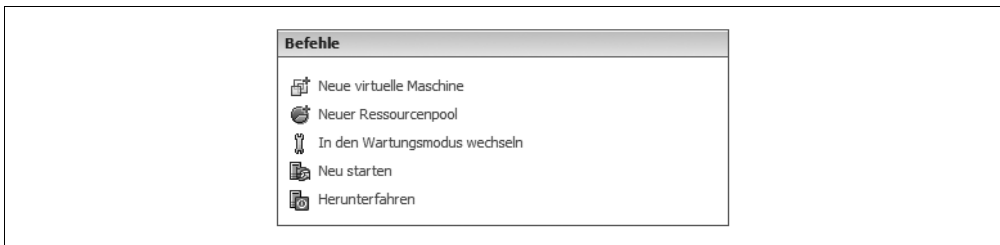


Abbildung 5-10: Mögliche Befehle am ESXi Server

Über die Befehle NEU STARTEN und HERUNTERFAHREN wird der ESXi Server versuchen, die noch laufenden virtuellen Maschinen ebenfalls herunterzufahren oder – je nachdem, was Sie unter KONFIGURATION → VMS STARTEN/HERUNTERFAHREN eingestellt haben – in den Anhaltmodus zu setzen. Haben Sie zu einer laufenden Maschine nichts eingestellt, wird diese hart beendet. Ist der Server in einem Cluster unter dem vCenter Server, werden die VMs gegebenenfalls trotzdem automatisch auf andere ESXi Server verschoben. Außerdem erhalten Sie einen Hinweis, wenn er sich nicht im Wartungsmodus befindet. Es könnte ja ein anderer Benutzer angemeldet sein, der gerade eine neue Maschine erstellt oder hochfahren möchte. Wenn Sie eine Begründung eingegeben haben, fährt der ESXi Server herunter und startet gegebenenfalls neu.

Gruppe Ressourcen

Ähnlich wie bei der virtuellen Maschine wird zunächst der momentane Verbrauch an CPU und Arbeitsspeicher in Zahlen und als Laufbalken angezeigt (siehe Abbildung 5-11). Die Kapazitäten beziehen sich aber auf die gesamte Nutzung der virtuellen Maschinen inklusive des Hosts und eines jeweiligen Overhead.

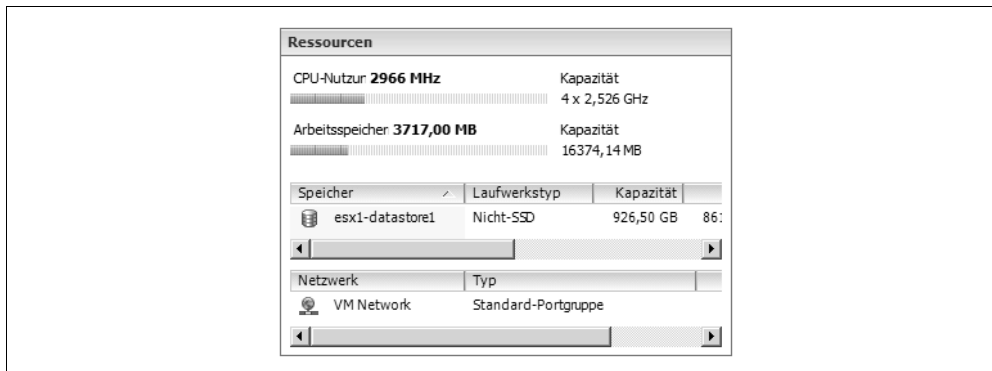


Abbildung 5-11: Ressourcenübersicht

Dargestellt werden alle dem Host zugänglichen Datenspeicher mit Gesamtkapazität und noch freiem Platz sowie die Zeit und das Datum, von wann diese Anzeige stammt. Beachten Sie, dass gegebenenfalls Abweichungen der Angaben z.B. durch die Erstellung einer neuen Maschine hier nicht sofort angezeigt werden. Sie können auf den jeweiligen Storage mit der rechten Maustaste klicken, um eine Aktualisierung zu bekommen.

Der letzte Eintrag listet die konfigurierten Portgruppen der virtuellen Maschinen auf. Die Portgruppen vom VMkernel (Management Network, FT, vMotion, Storage usw.) werden hier nicht angezeigt.

Gruppe Fault Tolerance

Diese Gruppe wird erst interessant, wenn der Host zu einem Cluster im vCenter Server gehört und dort virtuelle Maschinen im gespiegelten Modus laufen – dazu später mehr in Kapitel 10.

Registerkarte »Virtuelle Maschinen«

Wie in Abbildung 5-12 zu sehen ist, sind hier alle virtuellen Maschinen aufgeführt, die auf dem Host registriert sind. Dabei kann man

- den Zustand (eingeschaltet oder ausgeschaltet),
- den Speicherplatz, der für die Maschine bereitgestellt ist (inklusive Auslagerungsdatei),
- den zurzeit benötigten Speicherplatz (inklusive Auslagerungsdatei),

- die CPU-Last, den diese VM auf dem Host verursacht,
- den Arbeitsspeicher, den diese VM auf dem Host braucht, und
- den benutzten prozentualen Anteil am konfigurierten Arbeitsspeicher

sehen. Weiterhin wird gegebenenfalls eine Anmerkung zur virtuellen Maschine angezeigt, die man eingetragen hat, und auch Alarmaktionen, wenn der Host über den vCenter Server läuft.

Name	Zustand	Betriebszeit	Host-CPU - MHz	Hostarbeitsspeicher -	Gastarbeitsspe
VM-Doerrie...	Eingeschaltet	2 Minuten	2072	307	92
Ubuntu-Do...	Eingeschaltet	2 Minuten	29	256	75
TEST_XP_...	Eingeschaltet	2 Minuten	670	1055	92

Abbildung 5-12: Informationen über die Ressourcen der VMs

Wie bei fast jeder Liste, die man sich über den vSphere Client ansehen kann, lassen sich hier noch weitere Spalten hinzufügen (siehe Abbildung 5-13). Auch eine beliebige Sortierung kann man erreichen, indem man auf den gewünschten Spaltenkopf klickt. Die Reihenfolge ist übrigens bei jeder Liste beliebig durch Klicken mit der linken Maustaste veränderbar.



Abbildung 5-13: Spalten ein- und ausblenden

Die Breite der Spalten lässt sich ähnlich wie bei Microsoft Excel mit der linken Maustaste oder einem Doppelklick ändern. Leider wird die Spaltenbreite beim erneuten Aufruf des

Fensters wieder auf die vorigen Breite zurückgesetzt (manchmal nicht sofort, sondern erst später).

Hat man in dieser Liste viele virtuelle Maschinen, kann man oben rechts über das Feld NAME, ZUSTAND ODER ... auch einen Filter einsetzen. Wollen Sie z.B. nur die eingeschalteten Rechner sehen, klicken Sie in das Filterfeld, geben dort EINGESCHALTET an und drücken die Enter-Taste. Es reicht auch aus, nur einen Teil der Zeichenkette zu verwenden. Wenn Sie das Feld löschen und erneut Enter drücken, werden wieder alle Maschinen angezeigt.

Registerkarte »Ressourcenzuteilung«

In Kapitel 4 ging es schon detailliert um die Ressourcen der virtuellen Maschine. In dieser Übersicht lassen sich für alle VMs die vergebenen Einstellungen und mögliche Fehlkonfigurationen erkennen. Beachten Sie, dass Sie für Ihre VMs nur in Ausnahmefällen Grenzwerte oder Reservierungen eintragen sollten. Weitere Details finden Sie in Kapitel 18.

Registerkarte »Leistung«

Der ESXi Host speichert die Leistungsdaten der virtuellen Maschinen und seine eigenen nur für einen Zeitraum von maximal einem Tag. Erst durch den vCenter Server mit eigener Datenbank dafür stehen größere Zeiträume zur Verfügung. Beachten Sie in dieser Registerkarte oben links den Hinweis, dass der Graph nur alle 20 Sekunden aktualisiert wird. Was in dem angezeigten Diagramm dargestellt wird, steht auch oben links in der Ecke.

Über den Link DIAGRAMMOPTIONEN kommen Sie in ein neues Fenster, in dem Sie sich auch Wertekategorien aussuchen können:

- Arbeitsspeicher
- Betrieb
- CPU
- Datenspeicher und Festplatte
- Netzwerk
- Speicheradapter und -pfad
- System
- vSphere Replication

Für jede dieser Kategorien kann zwischen ECHTZEIT und LETZTER TAG (PAST DAY) gewählt werden; auf der rechten Seite finden Sie verschiedene Objekte und deren Leistungsindikationen. Mit Ausnahme der Einträge SPEICHERADAPTER UND -PFAD haben Sie LINIENDIAGRAMM, STAPELDIAGRAMM und STAPELDIAGRAMM (PRO VM), bei SYSTEM nur das Liniendiagramm. Ihre Einstellungen können Sie über die Schaltfläche DIAGRAMMEIN-

STELLUNGEN SPEICHERN festhalten und über DIAGRAMMEINSTELLUNGEN VERWALTEN wieder laden (siehe Abbildung 5-14). Über das letzte Icon können Sie sich ein eigenes Fenster für die Leistung anzeigen lassen – und das auch mehrfach unabhängig voneinander.

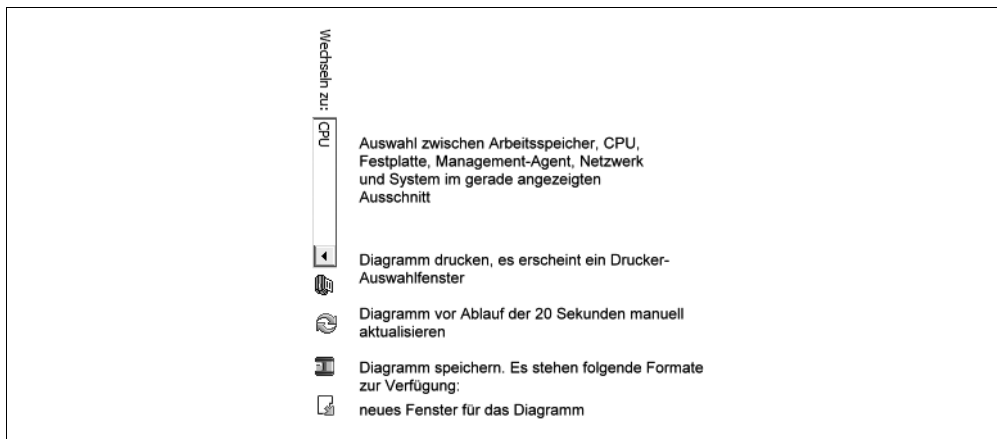


Abbildung 5-14: Die Schaltflächen oben rechts



Die Prozentangaben auf der linken Seite des Graphen beziehen sich auf die aktuelle Ansicht, nicht auf die zur Verfügung stehenden Ressourcen. Fahren Sie mit der Maus über die Anzeige, dann bekommen Sie die korrekten Prozentzahlen angezeigt.

Registerkarte »Lokale Benutzer und Gruppen«

Wie bei jedem Betriebssystem üblich, sind nach der Installation schon einige vordefinierte Benutzer und Gruppen im System angelegt, bei Linux-basierten Systemen sind es ein paar mehr, unter Windows nur wenige. Das liegt an der unterschiedlichen Handhabung der Dienste, die im Hintergrund werkeln, und deren notwendige Berechtigungen.

Weiterhin ist bei einem Linux-System der User *root* die höchste Instanz, hat also die höchste Berechtigung. Beim Windows-System ist es das System selbst. Der Administrator darf längst nicht alles. Bei unserem Host handelt es sich also eher um Linux als um Windows, obwohl hier kein echtes Betriebssystem mehr vorhanden ist (Busybox).

Die User-ID (UID) sagt unter anderem etwas über die Rechte im System aus. Grob gesagt: Je niedriger die ID, desto höher die Berechtigungen, und umgekehrt.

Der erste User wird mit der UID 501 angelegt und gehört automatisch zur Gruppe *users*. Schalten Sie auf die Anzeige *Gruppen* um, sehen Sie dort die Gruppe *users* und mit einem Doppelklick auf die Gruppe den gerade erstellten Benutzer.

Mit einem Klick der rechten Maustaste in das Fenster der Benutzer kommen Sie in ein Kontextmenü, über das Sie neue Benutzer anlegen können. Im Fenster NEUEN BENUTZER

ANLEGEN brauchen Sie nicht alle Felder auszufüllen. Wichtig sind BENUTZER (sollten Sie kleinschreiben) und KENNWORT (2*). Wenn Sie das Häkchen bei DIESEM BENUTZER SHELL-ZUGRIFF ERTEILEN setzen und ihn zur Gruppe *root* hinzufügen, kann er sich an der Konsole (Kommandozeile) des Hosts anmelden – auch über eine Remote-Verbindung. Weitere Voraussetzung für den Remote-Zugriff ist das Öffnen von Port 22 für SSH. Sie können sich also als »normaler User« anmelden und im Bedarfsfall anschließend mit dem Befehl *su* (*substitute user*) zum *root* ummelden. Ein User in der Gruppe *root* darf noch lange nicht alles, was der User *root* darf.



Beim ESXi Server werden die UUIDs wiederverwendet, wenn ein User gelöscht wurde. Achten Sie unbedingt auf die Dateien des gelöschten Users, weil der neue User automatisch Berechtigungen darauf erhalten kann.

Führen Sie einen Doppelklick auf einen Benutzernamen aus, können Sie dessen Einstellungen bearbeiten. Dazu gehören auch das Setzen eines neuen Passworts und das Hinzufügen zu einer Gruppe.

Bevor Sie einem Benutzer Berechtigungen zuweisen, lesen Sie unbedingt den Abschnitt ab Seite 133. Die Vererbung der Rechte läuft hier nicht wie z. B. bei Windows!

Unter ANSICHT im oberen Teil des Fensters können Sie zwischen BENUTZER und GRUPPEN umschalten. Sie können hier auch Gruppen erstellen und ihnen Benutzer hinzufügen oder sie aus ihnen entfernen.

Registerkarte »Ereignisse«

Jede Aktion von Benutzern oder System, die an einer virtuellen Maschine oder dem ESXi Host ausgeführt wird, wird mitprotokolliert und beim ESXi Server an dieser Stelle aufgeführt. Dazu gehören auch die An- und Abmeldungen von Benutzern. Die Meldungen, die hier erscheinen, sind vordefiniert und werden beim Auslösen hier aufgelistet. Je nach Schweregrad kann der Typ eine Information (ein weißes i im blauen Kreis), eine Warnung (ein Ausrufezeichen im gelben Dreieck) oder eine Fehlermeldung (ein Ausrufezeichen auf roter Raute) sein, die auch mit dem jeweiligen Icon farblich dargestellt wird. Zu jedem Ereignis erscheinen Datum und Uhrzeit des Auftretens und im unteren Teil des Abschnitts gegebenenfalls, welche vorherigen Ereignisse zu dieser Meldung geführt haben.

Wenn Sie nur die Ereignisse für eine VM sehen wollen, klicken Sie auf die virtuelle Maschine in der Bestandsliste und anschließend auf deren Registerkarte EREIGNISSE. Sie können aber auch die Hostereignisse nach dieser Maschine filtern, dann bekommen Sie das gleiche Ergebnis. Auch können Sie hier wieder nach Spalten sortieren.

Über das Menü DATEI → EXPORT → LISTE EXPORTIEREN können Sie die Ereignisse als *.html*-, *.htm*-, *.xls*-, *.csv*- oder *.xml*-Datei abspeichern.



Falls Fehler bei Ihrem Host oder einer virtuellen Maschine auftreten, stehen diese natürlich hier bei den Ereignissen dabei. Manchmal trifft man allerdings auf wenig aussagekräftige Sätze wie »A general system error occurred«. Häufig sind dann abhängige Ereignisse aufgeführt, die zu dem Fehler geführt haben, oder es werden Variablen oder deren Werte mit aufgeführt, z.B. »svga.vramSize«. Suchen Sie am besten im Internet über die VMware-Community oder Google nach diesem Eintrag, und Sie werden sicherlich fündig.



Weitaus detailliertere Informationen als in dieser Auflistung bekommen Sie zur virtuellen Maschine in deren Logdateien über die Kommandozeile. Sie können auch über den Datastore-Browser die Datei auf Ihren Rechner herunterladen und dann diese mit Wordpad o. Ä. öffnen (wegen der anderen Zeilenumbrüche in Linux sollten Sie nicht Notepad nehmen). Hier sehen Sie deutlich mehr Hinweise, die auf den Fehler schließen lassen. Die Informationen zum Host werden in verschiedenen Logdateien auf dem System selbst im Verzeichnis `/var/log` abgespeichert. Sehen Sie sich die Dateien `vmkeventd`, `vmkernel`, `vmkwarning` und die Datei `hostd.log` z.B. mit dem Programm `less` an, etwa so: `less /var/log/vmkernel`.

Registerkarte »Berechtigungen«

Die Informationen und Möglichkeiten auf dieser Registerkarte hängen von den erstellten Benutzern auf der vorherigen Karte und den Rollen unter der Verwaltung ab. Bei Rollen handelt es sich um Gruppen von definierten Berechtigungen, die den Zugriff einzelner Anwender bzw. Gruppen auf bestimmte Objekte des ESXi Servers steuern. Nur User und Gruppen, die Sie vorher angelegt haben, können hier mit Rechten versehen werden. Die Möglichkeiten, ihnen Rechte zu geben, hängen wiederum von den Rollen ab, die unter der Verwaltung vordefiniert sind oder von Ihnen neu erstellt wurden. Haben Sie noch keine individuellen Rollen erstellt, stehen Ihnen hier nur drei Berechtigungsstufen (Rollen) zur Verfügung: KEIN ZUGRIFF, NUR LESEN und ADMINISTRATOR.



Windows- und Domänenbenutzern können Sie nur Rechte über den vCenter Server vergeben, oder wenn Sie unter Konfiguration → Authentifizierungsdienste den Host ins AD integriert haben. Lesen Sie mehr darüber in Kapitel 10, *Der vCenter Server*.

Rechtevergabe

Sie können Berechtigungen auf eine einzelne virtuelle Maschine, einen Ressourcenpool oder auf den Host setzen. Rechte, die Sie auf Hostebene vergeben, werden üblicherweise nach unten hin vererbt. Das Vererben wird durch Genehmigungsregeln festgelegt und nicht allgemein angewendet. Wenn Sie sich im Fenster **BERECHTIGUNG SETZEN** befinden, achten Sie auf die Schaltfläche, mit der Sie die Vererbung außer Kraft setzen können.



Für ein Unterobjekt definierte Berechtigungen überschreiben immer die von übergeordneten Objekten übernommenen Berechtigungen. Das heißt: Wenn ein Benutzer Rechte auf einem übergeordneten Objekt besitzt, z.B. durch eine Gruppenzugehörigkeit auf dem ESXi Server, und Sie andere Rechte auf einem untergeordneten Objekt setzen, z.B. einer virtuellen Maschine, hat er hier nur die Berechtigungen, die explizit gesetzt wurden – nicht gegebenenfalls höhere durch die Vererbung.

Da die Rechtevererbung hier gänzlich anders ist, als man allgemein erwarten würde, folgen noch ein paar klärende Sätze dazu.

Wenn Sie Berechtigungen anwenden, werden sie in der Hierarchie von oben nach unten überschrieben. Werden Berechtigungen für dasselbe Objekt definiert, sind mehrere Fälle möglich:

Fall 1 – Ein Anwender ist Mitglied von mehreren Gruppen mit unterschiedlichen Berechtigungen. Für jedes Objekt, über dessen Berechtigungen die Gruppe verfügt, gelten die gleichen Berechtigungen, als wären sie dem Anwender direkt gewährt worden.

Fall 2 – Für dasselbe Objekt wurden mehrere Gruppenberechtigungen definiert, und der Anwender gehört mindestens zwei dieser Gruppen an.

- Wenn für dieses Objekt keine zusätzlichen Rechte explizit für diesen Anwender angegeben wurden, werden ihm alle Berechtigungen gewährt, die den Gruppen für dieses Objekt zugewiesen wurden.
- Wenn für dieses Objekt explizit eine Genehmigung für diesen Anwender angegeben wurde, hat diese Berechtigung Vorrang vor allen Gruppenberechtigungen.

Beispiel 1: Erweitern der Berechtigungen eines Anwenders X

- Rolle 1 kann virtuelle Maschinen einschalten.
- Rolle 2 kann Snapshots von virtuellen Maschinen erstellen (zu Snapshots kommen wir in Kapitel 8).
- Der Gruppe A wird die Rolle 1 in der virtuellen Maschine zugewiesen.
- Der Gruppe B wird die Rolle 2 in der virtuellen Maschine zugewiesen.

Anwender X wird keine explizite Genehmigung zugeteilt:

- Anwender X gehört zu den Gruppen A und B.
- Anwender X kann VM einschalten und Snapshots erstellen.

Beispiel 2: Einschränken der Berechtigungen eines Anwenders Y

- Rolle 1 kann virtuelle Maschinen einschalten.
- Rolle 2 kann Snapshots von virtuellen Maschinen erstellen.
- Der Gruppe A wird die Rolle 1 im übergeordneten Ordner der virtuellen Maschine zugewiesen.
- Der Gruppe B wird die Rolle 2 in der virtuellen Maschine zugewiesen.

Die Nur-lesen-Berechtigung von Anwender Y wird in der virtuellen Maschine entfernt:

- Anwender Y kann Snapshots erstellen, aber VMs nicht einschalten.



Wenn Sie Änderungen bei den Berechtigungen vornehmen, müssen sich die Anwender nicht ab- und wieder anmelden, damit diese wirksam werden. Alle Änderungen werden sofort wirksam.

Rollen

Eine Rolle ist ein vordefiniertes Set von Rechten, die Sie einem Benutzer oder einer Gruppe zuteilen können. Die drei vorkonfigurierten Standardrollen, die Sie unter VERWALTUNG → ROLLEN finden, können nicht geändert werden. Wenn in bestimmten Situationen andere Zugriffsberechtigungen benötigt werden, erstellen Sie eine zusätzliche Rolle oder klonen eine vordefinierte und passen sie Ihren Anforderungen an.

Standardrollen auf dem ESXi Server

Es folgen ein paar kurze Hinweise zu den Rechten, die für die drei Standardrollen vordefiniert sind.

- KEIN ZUGRIFF: Diese Rolle wird genommen, um die eigentliche Vererbung der Berechtigungen wieder außer Kraft zu setzen. Ein User, dem diese Rolle z. B. für eine VM zugewiesen wird, kann dies nicht sehen oder ändern. Die Registerkarten sind zwar vorhanden und können angeklickt werden, der Inhalt ist aber leer.
- NUR LESEN: User mit diesem Recht können zwar alle Details sehen, aber nichts ändern. Alle Vorgänge über die Schaltflächen oder Kontextmenüs sind sichtbar, aber nicht auswählbar. Auch die Remote-Console ist für diesen Benutzer nicht erreichbar.
- ADMINISTRATOR: Hiermit werden alle Berechtigungen auf alle Objekte auf dem ESXi Server vergeben. Sie können aber auch administrative Berechtigungen auf untergeordnete Objekte, also VMs oder Ressourcenpools, vergeben, die sich nicht auf den ESXi Host auswirken. Mit diesem Recht können Sie auch selbst Berechtigungen vergeben.



Wenn Sie einen Klon einer Rolle erstellen, wird die neue Rolle nicht automatisch auf denselben Anwender bzw. dieselbe Gruppe und dieselben Objekte angewendet wie in der Ausgangsrolle. Das müssen Sie manuell tun.



Nicht alle Möglichkeiten, die man durch Setzen von Häkchen in der Rolle hat, sind auf dem ESXi Server sinnvoll. Einige Rechte sind nur über den vCenter Server anwendbar. Dazu gehören ALARME, DATENCENTER, GEPLANTE AUFGABE, einiges unter GLOBAL, einiges unter HOST → BESTANDSLISTE, HOSTPROFIL, ORDNER, SITZUNGEN, VAPP, VERTEILTE VIRTUELLE PORTGRUPPE, VERTEILTER VIRTUELLER SWITCH, einiges unter VIRTUELLE MASCHINE → BEREITSTELLUNG (Vorlagen) und einiges unter VIRTUELLE MASCHINE → INTERAKTION.



Wenn Sie eine neue Rolle erstellen oder eine vordefinierte klonen, sollten Sie die gesetzten Berechtigungen vor dem Zuweisen an einen Benutzer auf jeden Fall testen. Manchmal übersieht man bei den vielen Kästchen (siehe Abbildung 5-15) Abhängigkeiten, die dann die gewünschte Arbeit des Users unmöglich machen.

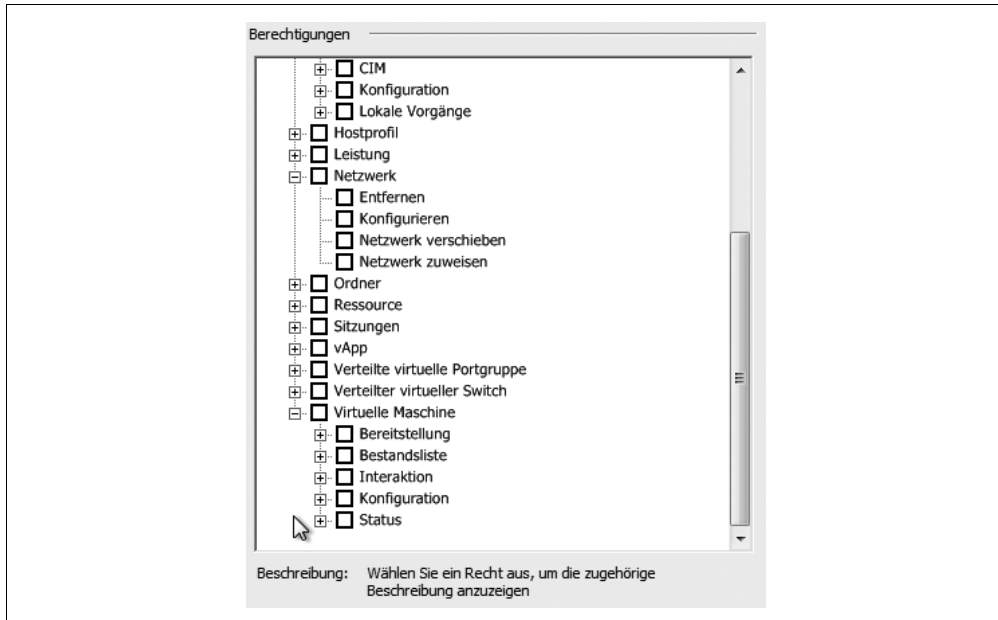


Abbildung 5-15: Definierbare Rechte

Geben Sie beispielsweise einem angelegten Benutzer alle Berechtigungen für eine virtuelle Maschine, indem Sie bei einer neuen Rolle das Häkchen bei VIRTUELLE MASCHINE setzen. Melden Sie sich als dieser User mit dem vSphere Client an und versuchen Sie, der VM eine Festplatte hinzuzufügen – das schlägt fehl, weil ihm der Zugriff auf den Datastore nicht erlaubt ist. Den kann er nur über zusätzliche Berechtigungen auf Hostebene bekommen. Die durch die dann erfolgende Vererbung gesetzten Rechte können Sie über die Rolle KEIN ZUGRIFF wieder einschränken.



Wenn Sie diesen ESXi Server mit den gesetzten Berechtigungen zu einem vCenter Server hinzufügen und der Benutzer sich über diesen anmeldet, hat er die vorher erteilten Rechte nicht, weil es sich um einen anderen User handelt. Beim vCenter Server, der auf einem Windows-System installiert wird, müssen Sie Berechtigungen neu definieren, weil Sie dort nur lokale User des Microsoft-Betriebssystems oder der Domäne hinzufügen können. Meldet der Benutzer sich aber am ESXi Host direkt an, hat er die Rechte. (Dazu später mehr in Kapitel 10.)



Ändern Sie die Berechtigungen der vordefinierten User auf dem ESXi Server nicht. Sonst kann es Probleme mit der Verwaltung des Hosts geben, auch wenn dieser zum vCenter Server hinzugefügt wird – denn der Windows-Rechner greift über den Linux-User *vpxuser* auf den ESXi Server zu.

Die Menüleiste unter ESXi

In den sieben Pull-down-Menüs in der Menüleiste ändern sich die anwählbaren Punkte abhängig davon, ob man auf einer virtuellen Maschine, einem Ressourcenpool oder dem Host steht. Vieles von dem, was man hier findet, haben wir schon besprochen, weil es auch über die Registerkarten oder Kontextmenüs erreichbar ist. Ich gehe deshalb hier nur auf die noch nicht besprochenen Einträge ein.

Menü »Datei«

Unter DATEI → NEU kann eine neue VM oder ein neuer Ressourcenpool erstellt werden, wenn Sie den ESXi Host ausgewählt haben. Berechtigungen können immer zugewiesen werden.

Die Auswahl DATEI → OVF-VORLAGE BEREITSTELLEN öffnet ein neues Fenster, über das Sie lokal oder aus dem Internet eine virtuelle Maschine oder eine vApp im OVF-Format (*Open Virtual Machine Format*) in den ESXi Server importieren können. Hierbei handelt es sich meistens um fertige VMs mit installiertem Betriebssystem und teilweise mit Software – sogenannte Appliances. Wo die Maschine liegt – lokal, auf einem optischen Datenträger, im LAN oder im Internet –, spielt dabei keine Rolle. Sie können sich auch selbst eine fertige Maschine in das OVF-Format konvertieren und irgendwo abspeichern, indem Sie auf Ihre VM klicken und anschließend auf DATEI → EXPORT → OVF-VORLAGE EXPORTIEREN. Vorteilhaft dabei ist, dass diese Vorlage deutlich weniger Platz beansprucht als die Dateien auf dem Host, und dass alle Informationen zu dieser VM mit abgespeichert werden. So eine Vorlage wird auch »virtuelle Appliance« genannt. Haben Sie eine OVF-Vorlage in einer anderen VMware-Software erstellt, müssen Sie den Converter nutzen, um sie bereitzustellen.

Immer wenn Sie eine Liste angezeigt bekommen, z.B. eine Liste aller virtuellen Maschinen, aller Berechtigungen, aller Benutzer usw., können Sie sich diese über DATEI → EXPORT → LISTE EXPORTIEREN als *.html*-, *.htm*-, *.xls*-, *.csv*- oder *.xml*-Datei abspeichern.

DATEI → EXPORT → ZUORDNUNGEN EXPORTIEREN ist auf dem ESXi Server nicht möglich. Erst über den vCenter Server können Sie sich die grafischen Zuordnungen von Host, VM, Storage und Netzwerken abspeichern.

Die Systemprotokolle lassen sich über DATEI → EXPORT → SYSTEMPROTOKOLLE EXPORTIEREN sichern. Dieser Vorgang kann ein wenig Zeit in Anspruch nehmen. Es werden alle untergeordneten Objekte und bei Bedarf auch Leistungsdaten in einem definierbaren

Zeitraum erfasst und abgespeichert. Beobachten Sie im zusätzlichen Fenster den Status (siehe Abbildung 5-16).

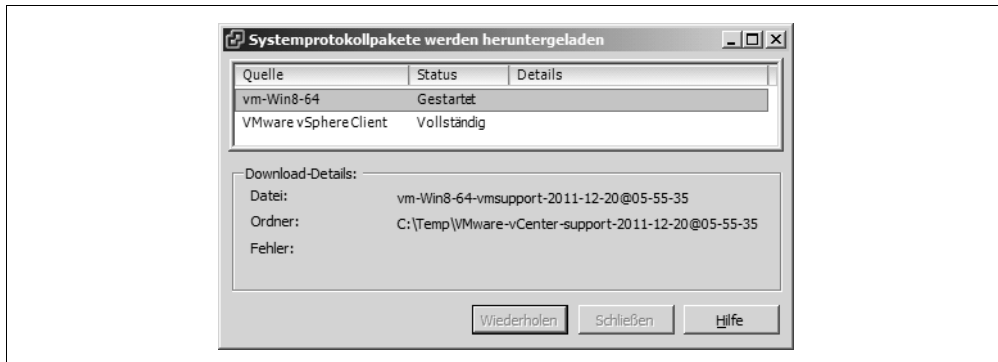


Abbildung 5-16: Systemprotokolle exportieren

Ist der Vorgang abgeschlossen, bekommen Sie ein Hinweis im Zusatzfenster, der Ihnen sagt, dass die Systemprotokolle vollständig heruntergeladen wurden. Am gewählten Speicherort befindet sich anschließend das Verzeichnis *VMware-vCenter-support-**<Datum>**@**<Uhrzeit>***, in dem eine gepackte Datei im *.tgz*-Format und ein weiterer gepackter Ordner im *.zip*-Format mit Logdateien des vSphere Clients liegen. In der komprimierten Datei finden Sie die wichtigsten Konfigurationsdateien in den Unterordnern des Hosts sowie der virtuellen Maschine.

esx1.gfu.dom VMware ESXi, 5.0.0, 469512 Test (Restzeit: 60 Tage)	
ALLGEMEIN	
Hersteller:	Dell Inc.
Modell:	PowerEdge T110
Prozessoren:	4 CPU x 2,526GHz
Prozessortyp:	Intel(R) Xeon(R) CPU X3440 @ 2.53GHz
Hyper-Threading:	Aktiv
GesamtArbeitsspeicher:	15,99 GB
Anzahl der Netzwerkkarten:	2
Zustand:	Verbunden
Virtuelle Maschinen:	3
vMotion-fähig:	Nein
Aktive Aufgaben	
RESSOURCEN	
CPU-Nutzung:	0% ██████████
Arbeitsspeichernutzung:	9% ██████████
DATENSPEICHER	
esx1-datastore1:	Kapazität: 926,50 GB (861,96 GB frei)
NETZWERKE	
VM Network	

Abbildung 5-17: Bericht – Hostübersicht

Haben Sie den Fokus auf den ESXi Host gesetzt, können Sie über DATEI → BERICHT → HOSTÜBERSICHT Laufzeitinformationen des Hosts als .htm-, .html- oder .xls-Datei abspeichern. Ein Beispiel sehen Sie in Abbildung 5-17.

Mit DATEI → VA MARKETPLACE DURCHSUCHEN bekommen Sie ein neues Fenster, über das Sie auf dem virtuellen Marktplatz von VMware nach fertigen virtuellen Maschinen – meist im OVF-Format – suchen können. Hier stellen Anbieter von diversen Anwendungen und Betriebssystemen zum Teil fertige Rechner zur Verfügung. Bei einem Teil davon handelt es sich um Testversionen, die anderen sind Vollversionen, die direkt einsatzbereit sind. Zu Testzwecken kann man sich z.B. *Nostalgia* herunterladen, eine virtuelle Maschine mit DRDOS als Betriebssystem und ein paar freien Spielen. Interessant daran ist der Performancehunger dieser VM: Auch wenn nur ein Prompt angezeigt wird, nimmt sich DOS immer 100 % der CPU-Leistung. Hier kann man diverse Ressourceneinstellungen austesten.



VMware hat auch für die Datensicherung mit Data Recovery eine fertige VM im OVF-Format erstellt. Diese wird auf die gleiche Weise bereitgestellt. Zu Data Recovery erhalten Sie in Kapitel 16 detaillierte Informationen.

Menü »Bearbeiten«

UMBENENNEN und ENTFERNEN sind hier möglich, wenn der Fokus auf einer ausgeschalteten virtuellen Maschine oder einem Ressourcenpool steht. Ist die VM eingeschaltet, geht nur UMBENENNEN.

Außerdem finden Sie hier die Einstellungen zum vSphere Client (CLIENTEINSTELLUNGEN), wie schon oben im Rahmen seiner Installation beschrieben.

Menü »Ansicht«

Dieses Menü dient der Navigation auf der Oberfläche mit den Einträgen ZURÜCK, VOR und HOME.

Weiterhin kann man sich das vSphere Client-Fenster einrichten, indem man die Symbolleisten NAVIGATIONSLEISTE, SYMBOLLEISTE und STATUSLEISTE aus- bzw. einblendet.

Für sehr große Umgebungen ist es unter Umständen sinnvoll, VIRTUELLE MASCHINEN IN DER BESTANDSLISTE ANZEIGEN abzuwählen. Dann werden nur noch die Hosts und Ressourcenpools angezeigt.

VORLAGEN IN DER BESTANDSLISTE ANZEIGEN hat hier noch keinen Sinn, da man diese nur im Zusammenhang mit dem vCenter Server erstellen kann.

Weiterhin können Sie hierüber von der VERWALTUNG zur BESTANDSLISTE und zurück navigieren.

ANSICHT → FILTER ist nur anwählbar, wenn Sie sich auf einer Liste befinden. Nehmen Sie das Häkchen dann heraus, ist die Auswahlmöglichkeit des Filterns ausgeblendet.

Menü »Bestandsliste«

Alles, was über dieses Menü erreichbar ist, bekommen Sie auch über das Kontextmenü der jeweiligen Objekte in der Bestandsliste – außer BESTANDSLISTE → VAPP, da vApp erst unter dem vCenter Server anwählbar ist (Details in Kapitel 12, *VMware vApp und Fernzugriff*).

Menü »Verwaltung«

Haben Sie sich mit dem ESXi Host direkt verbunden und nicht über den vCenter Server, ist dieses Menü nur erreichbar, wenn Sie bereits in VERWALTUNG → ROLLEN stehen. Die auswählbaren Punkte entsprechen auch hier denen des Kontextmenüs.

Menü »Plug-Ins«

Auch dieser Punkt wird erst nützlich, wenn der vCenter Server eingerichtet ist. Dann können Sie einige Plugins herunterladen und verwenden (Details ab Kapitel 10, *Der vCenter Server*).

Menü »Hilfe«

Über HILFE → HILFETHEMEN kommen Sie zur Onlinehilfe von VMware, die zusammen mit dem vSphere Client installiert wurde. Sie finden die Dateien im Verzeichnis `C:\Programme\VMware\...\Help\de\VIC50` (eventuell weicht der Pfad zu Ihrem Installationsverzeichnis etwas ab). Im Standardbrowser öffnet sich zunächst eine Übersicht mit verschiedenen Kapiteln, in denen grundlegende Hilfestellungen für Einsteiger geboten werden. Die herunterladbaren Dokumentationen als PDF-Datei – teilweise auf Deutsch – sind deutlich detaillierter und können von der Website zum Buch heruntergeladen werden. Sie können übrigens in vielen Zusatzfenstern auf die Schaltfläche HILFE klicken und kommen dann kontextbezogen auf die richtige Seite.

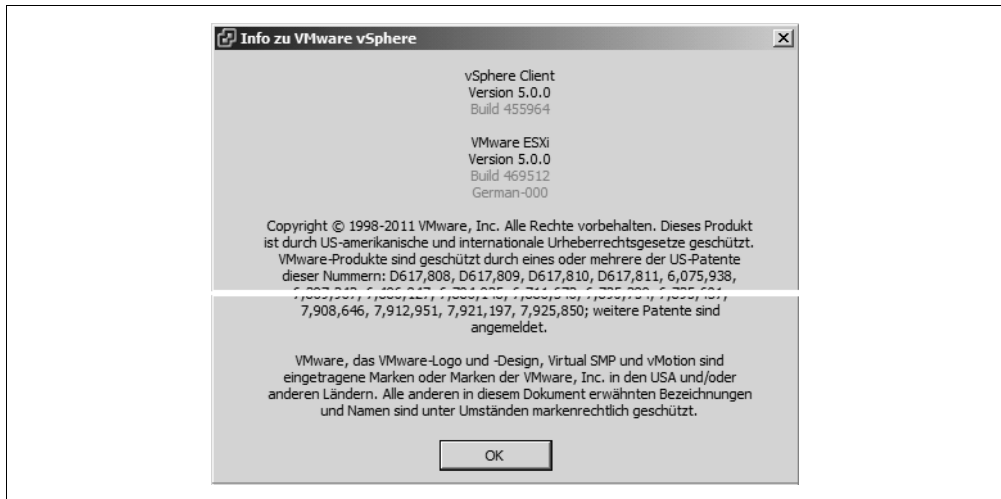
HILFE → HANDBÜCHER ist ein Link auf die VMware-Webseite http://www.vmware.com/support/pubs/vs_pubs.html, auf der weitergehende Literatur angeführt wird, die Sie teilweise auch herunterladen können. Leider kommen Sie hier nur auf die englischen Seiten – wenn Sie deutschsprachige suchen, werden Sie vielleicht unter http://www.vmware.com/de/support/support-resources/pubs/vs_pubs/vsphere-esxi-vcenter-server-pubs.html fündig.

HILFE → LERNPROGRAMM ist noch nicht anwählbar. Eventuell wird es später nach einem Update zur Verfügung stehen.

Über HILFE → VMWARE IM INTERNET werden Sie auf die Website weitergeleitet und können z.B. Onlinesupport in Anspruch nehmen (je nach Lizenz) oder Ihr Produkt registrieren lassen, je nachdem, wo und wie Sie es erworben haben.

HILFE → AUF UPDATES IM INTERNET PRÜFEN lädt eine Internetseite von VMware, über die Updates, Treiber und Tools sowie Open Source-Produkte heruntergeladen werden können.

HILFE → INFOS ZU VMWARE vSPHERE bringt ein neues Fenster auf die Oberfläche, das Versionsangaben und den Build des Clients und des Servers sowie die Patente anzeigt (siehe Abbildung 5-18).



Netzwerkconfiguration

Bevor Sie weitere virtuelle Maschinen auf den ESXi Servern erstellen, sollten Sie die Netzwerke und Storage-Zugriffe der Hosts konfigurieren. In diesem Kapitel werde ich detailliert auf die Netzwerkconfiguration eingehen, und Kapitel 7 befasst sich dann mit den Möglichkeiten, gemeinsame Storages einzurichten. Die Installation und Konfiguration des vCenter Servers mit verteilten vSwitches erfolgt später in diesem Buch.

Zur Basiskonfiguration des ESXi Servers gehören z.B.

- die Erstellung virtueller Switches und Ports,
- die Einrichtung des Netzwerks für virtuelle Maschinen,
- die Konfiguration des Netzwerks für vMotion, ein zweiter Management Port für den Verwaltungsdatenverkehr und gegebenenfalls Zugriff auf iSCSI- oder NFS-Speicher,
- das Konfigurieren des Dateisystems und verschiedener Speichertypen wie iSCSI, Fibre Channel und NFS sowie
- die zum Schutz Ihrer VMs enthaltenen Sicherheitsfunktionen bezüglich Netzwerk und Speicher.

Netzwerkkonzepte

Die meisten von Ihnen kennen einen *physischen Switch*. Er wird eingesetzt, um PCs miteinander zu verbinden, damit diese Daten austauschen können. Jeder Switch hat mehrere Anschlüsse (genannt Ports), die mit einem Kabel versehen zu einem anderen Switch gehen oder an einen Rechner, der am Netzwerkverkehr teilnehmen soll.

Ein Switch merkt sich für jeden Port die MAC-Adresse des angeschlossenen Geräts und leitet Datenpakete nur an diesen weiter (Ausnahme: Broadcasts, also Meldungen an alle).

Switches bilden den Kern eines physischen Netzwerks. Es können mehrere Switches zusammengeschlossen werden, um größere Netzwerke zu bilden (Kaskadierung, z.B. über einen Uplink-Port).

Virtuelle und physische Switches

Ein *virtueller Switch*, ein sogenannter *vSwitch* auf dem ESXi Server (siehe Abbildung 6-1), funktioniert ähnlich wie ein physischer Ethernet-Switch (Level 2 Hub): Er weiß, welche virtuellen Maschinen logisch an welche virtuellen Ports angeschlossen sind, und leitet die Daten nur an die entsprechende virtuelle Maschine weiter.

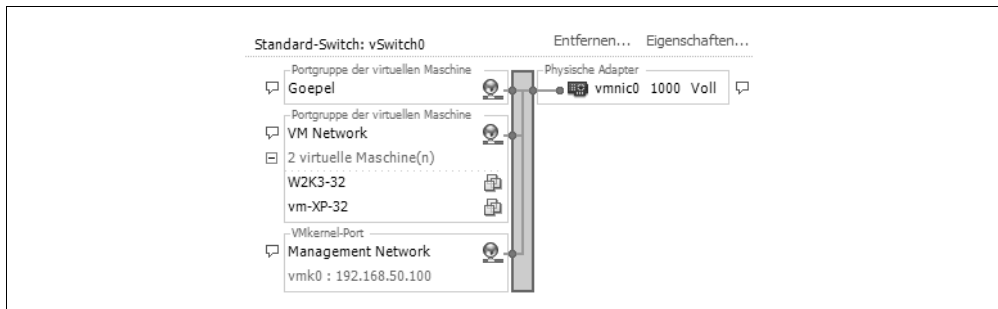


Abbildung 6-1: Virtueller Netzwerk-Switch

Ein vSwitch kann über physische Ethernet-Adapter (auch Uplink- oder Outbound-Adapter genannt) an physische Switches angeschlossen werden, um virtuelle und physische Netzwerke zu verbinden. Diese Verbindung ähnelt der Vernetzung physischer Switches zur Bildung größerer Netzwerke. Ein vSwitch funktioniert also ähnlich wie ein physischer Switch, verfügt aber nicht über alle erweiterten Funktionsmerkmale eines managbaren physischen Switch.

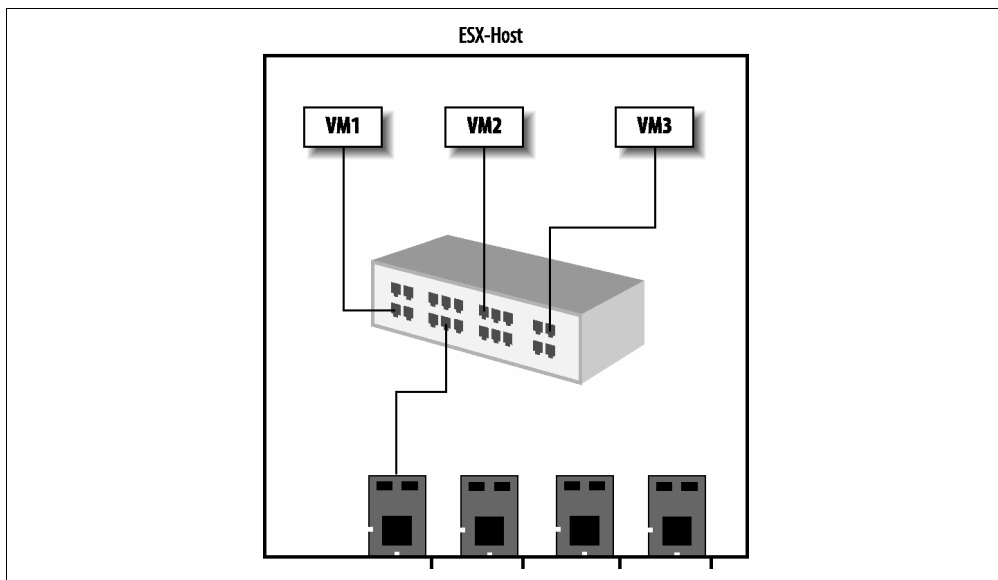


Abbildung 6-2: Kommunikation über Hypervisor

Ein *virtuelles Netzwerk* unterscheidet sich von einem physischen dadurch, dass die Daten, die von einer virtuellen Maschine zu einer anderen gesendet werden, nicht die Netzwerkkarte erreichen, sondern über den Hypervisor ausgetauscht werden (siehe Abbildung 6-2). Erst wenn die Ziel-VM auf einem anderen Host liegt oder wenn ein physischer Rechner das Ziel ist, werden die Daten über die Netzwerkkarte des Hosts an einen physischen Switch weitergeleitet (siehe Abbildung 6-3). Dann wird aber nicht mehr von einem »virtuellen Netzwerk« gesprochen.

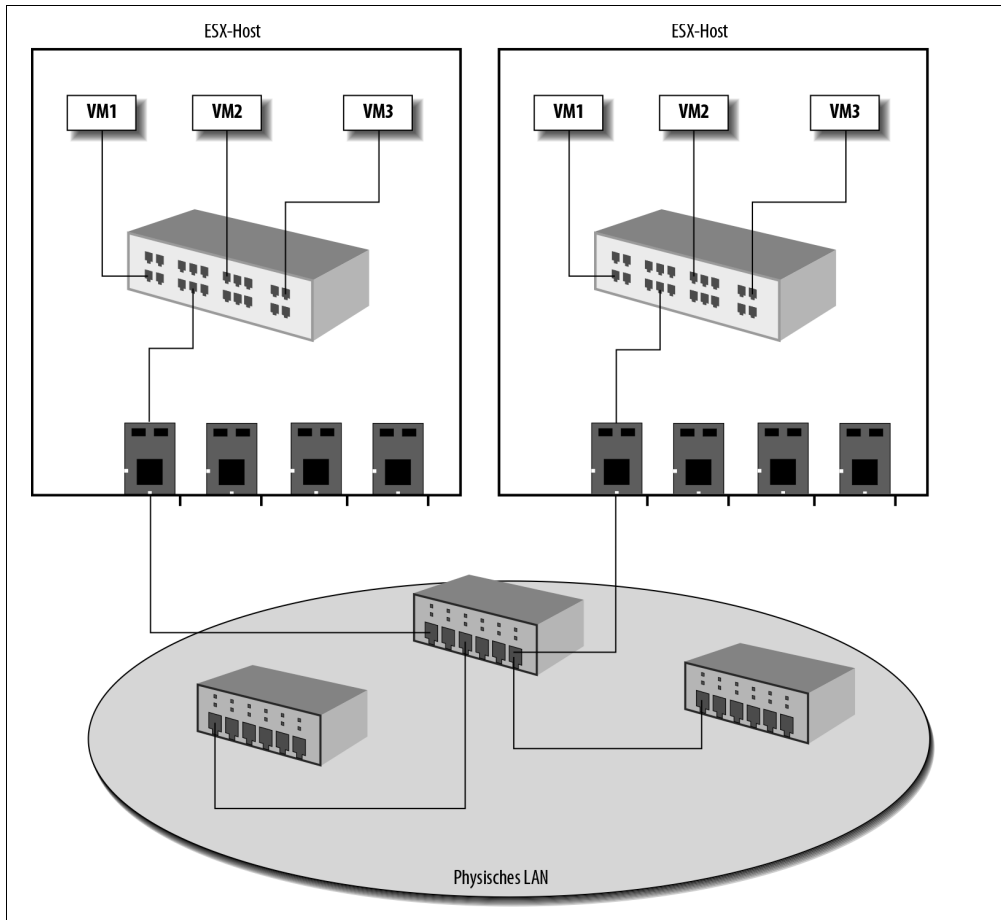


Abbildung 6-3: Kommunikation über das LAN

Die Netzwerkkonzepte von VMware

VMware hat ab vSphere4 ein neues Netzwerkkonzept eingebunden, das aber nur in Zusammenhang mit dem vCenter Server möglich ist. Dabei handelt es sich um sogenannte *verteilte Netzwerkschwitches*. Auf diese Neuerung gehe ich erst später ein, wenn wir

den vCenter Server installiert haben. Es folgt eine Beschreibung des Netzwerkkonzepts für einen einzelnen ESXi Host:

- Ein virtueller Switch kann in Gruppen mit bestimmten Ports aufgeteilt werden, wie in Abbildung 6-4 gezeigt. Für jede Portgruppe können dann unterschiedliche Einstellungen festgelegt werden, z. B. Bandbreitenbeschränkungen, Sicherheitseinstellungen oder VLAN-Tagging-Richtlinien.

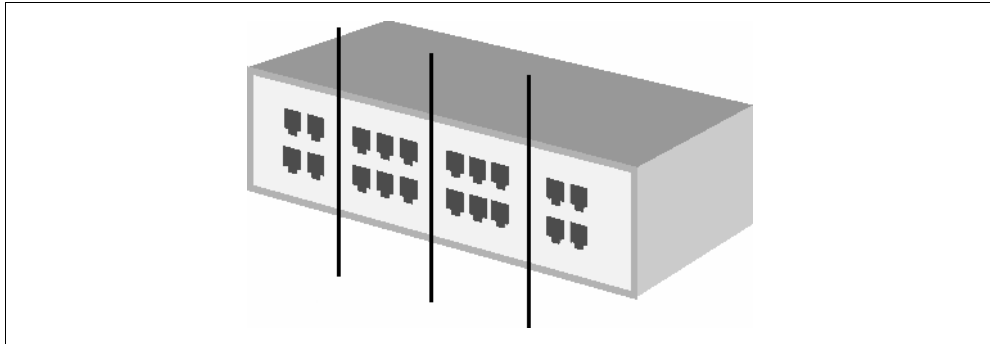


Abbildung 6-4: -4 In Gruppen aufgeteilter Switch

- Die Netzwerkdienste werden über diese Gruppen an vSwitches angeschlossen. Portgruppen definieren, wie eine Verbindung über den vSwitch an das physische Netzwerk erfolgt. Standardmäßig wird einem einzelnen vSwitch mindestens eine Portgruppe zugeordnet. Es ist nicht möglich, einen vSwitch ohne Portgruppe zu erstellen.
- NIC-Gruppierung (NIC-Teaming) tritt auf, wenn einem vSwitch mehrere physische Netzwerkkarten (Uplink-Adapter) zugewiesen werden, um eine Gruppe zu bilden. Eine Gruppe kann entweder den Datenverkehr zwischen dem physischen und dem virtuellen Netzwerk auf einige oder alle Netzwerkkarten der Gruppe aufteilen oder ein passives Failover im Fall einer Hardwarestörung oder eines Netzwerkausfalls bereitstellen.
- Mit VLANs kann ein einzelnes physisches LAN-Segment weiter aufgeteilt werden, so dass Portgruppen derart voneinander isoliert werden, als befänden sie sich in unterschiedlichen physischen Segmenten. Der Standard ist 802.1q.
- Der VMkernel-TCP/IP-Netzwerkstapel unterstützt iSCSI, NFS, vMotion, Fault Tolerance und das Management Network für den Verwaltungsdatenverkehr. Virtuelle Maschinen führen TCP/IP-Stapel ihrer eigenen Systeme aus und verbinden sich auf Ethernet-Ebene über virtuelle Switches mit dem VMkernel.
- IP-Speicher bezeichnet jede Art von Storage, der auf TCP/IP-Netzwerkkommunikation beruht. iSCSI und NFS können als Datenspeicher für virtuelle Maschinen oder für die direkte Einbindung von ISO-Dateien verwendet werden, die dann von der virtuellen Maschine als CD-/DVD-ROMs erkannt werden.
- TCP Segmentation Offload (TSO) ermöglicht einem TCP/IP-Stapel das Senden sehr großer Datenblöcke (bis zu 64 KByte), obgleich die maximale Übertragungseinheit

(*Maximum Transmission Unit*, MTU) der Schnittstelle kleiner ist. Der Netzwerkkad-
apter trennt anschließend den großen Datenblock in Datenblöcke mit MTU-Größe
und stellt eine angepasste Kopie der einleitenden TCP/IP-Header voran. Ein VMker-
nel-Port ist damit standardmäßig angelegt.

- Über die Migration mit vMotion kann eine laufende virtuelle Maschine von einem
Host auf einen anderen übertragen werden, ohne dass die virtuelle Maschine herun-
tergefahren werden muss. Für die optionale vMotion-Funktion ist ein eigener Lizenz-
schlüssel notwendig.



MTU und TSO einer oder mehrerer Netzwerkkarten an einem vSwitch
können auch über die grafische Oberfläche mit dem vSphere Client einge-
richtet werden. Das erfolgt nun nicht mehr nur über die Kommandozeile
(siehe »vSwitches optimieren« auf Seite 166).

Internet Protocol Version 6

vSphere unterstützt sowohl Internetprotokollversion 4 (IPv4) als auch Internetprotokoll-
version 6 (IPv6). Nach der Installation ist aber nur IPv4 auf dem ersten vSwitch eingerich-
tet. Zu einer IPv6-spezifischen Konfiguration in vSphere gehört das Angeben von IPv6-
Adressen für alle relevanten vSphere-Netzwerkschnittstellen – entweder durch die Eingabe
von statischen Adressen oder durch Verwendung von DHCP (Stateful Address Autocon-
figuration). Die IPv6-Adressen kann sich der Host auch über die sogenannte *Stateless
Address Autoconfiguration* über spezielle Routermeldungen holen. Dabei hat der Router
ein Präfix, aus dem sich angeschlossene Geräte ihre eigenen Information bilden können.

Aktivieren von IPv6

Die Unterstützung von IPv6 können Sie auf dem Host über den vSphere Client aktivieren
oder deaktivieren.

1. Klicken Sie in der BESTANDSLISTE auf Ihren Host.
2. Wählen Sie die Registerkarte KONFIGURATION.
3. Klicken Sie unter HARDWARE auf den Link NETZWERK.
4. Wählen Sie den gewünschten vSwitch und klicken Sie in der Ansicht oben rechts auf
den Link EIGENSCHAFTEN. Dann öffnet sich das Fenster aus Abbildung 6-5.

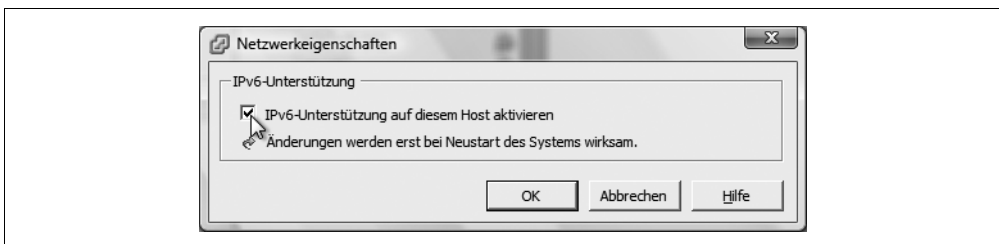


Abbildung 6-5: IPv6 einschalten

IPv6

Eine IP-Adresse ergibt sich aus einem Adressraum von 32 Bit, woraus sich eine Anzahl von 2^{32} möglichen verschiedenen Adressen ergibt. Das sind ca. 4,3 Milliarden Adressen, was auf den ersten Blick doch eine ganz beachtliche Menge zu sein scheint.

Gleichwohl ging man eine Weile recht verschwenderisch mit den Adressen um, und wenn man daran denkt, dass alle möglichen Geräte (ja, auch der heimische Kühlschrank) weltweit per Internet erreichbar sein sollen, wird klar, dass die verfügbaren Adressen doch langsam zur Neige gehen.

Die zurzeit gängige IP-Version wird als IPv4 bezeichnet. Der seit 1994 in Arbeit befindliche Nachfolger IPv6 verwendet dagegen einen Adressraum von 128 Bit, was zu einer geradezu unvorstellbaren Anzahl von möglichen IP-Adressen führt. IPv6 – oder IPnG (*IP next Generation*), wie dieser Standard auch bezeichnet wird – muss natürlich zu IPv4 kompatibel sein, was dadurch erreicht wird, dass die bisherigen IPv4-Adressen in den unteren Bereich von IPv6 aufgenommen werden. Neben den 128-Bit-Adressen bietet IPv6 zusätzliche Sicherheitsfunktionen (Authentication & Privacy), neue Routing-Mechanismen, eine flexiblere Klassenteilung und *Quality of Service*. Von der QoS, die man sich vereinfacht als eine garantierte Bandbreitenzuteilung für eine Übertragung vorstellen kann, sollen insbesondere Echtzeitanwendungen wie Ton und Video profitieren.

IPv4-Adressen werden dezimal in vier, IPv6 hexadezimal in acht Blöcken dargestellt. Neu ist die Abgrenzung durch Doppelpunkte (ähnlich wie bei der MAC-Adresse, *Media Access Control*), also z.B. 20F8:08DC:853A:083B:1121:B1C2:3007:1144.

IPv6-Adressen sind aus zwei logischen Teilen zusammengesetzt: einem 64 Bit langen Netzwerkpräfix und einer 64 Bit langen Hostadresse, die entweder aus der Hardwareadresse der Netzwerkkarte (MAC-Adresse) erstellt oder einfach sequenziell zugewiesen werden kann.

Ein Subnetz wird dann z. B. mit 20F8:08DC:853A:083B::/64 bezeichnet. Hat ein Netzwerkgerät die IPv6-Adresse 20F8:08DC:853A:083B:1121:B1C2:3007:1144, stammt es aus diesem Subnetz. Daraus folgt, dass dieses Subnetz auch zum übergeordneten Subnetz mit dem kürzeren Präfix 20F8:08DC:853A::/48 gehört.

Adressen aus diesem Subnetz fangen also bei

- 20F8:08DC:853A:0000:0000:0000:0001 an und hören bei
- 20F8:08DC:853A:FFFF:FFFF:FFFF:FFFE auf. Daher ist ein Subnetz mit nur einem PC als /128 gekennzeichnet.
- Eine Localhost-Adresse ist also mit ::0001/128 gekennzeichnet.
- FC00::/7 sind lokale Adressen, die von einem Internetrouter nicht weitergeleitet werden, wohl aber von LAN-Routern.
- FEC0::/10, also von FEC0 bis FEFF, sind für Multicast vorgesehen, ebenso wie der Adressbereich aus FF00::/8.

Erst seit Windows Vista wird IPv6 bei Microsoft-Betriebssystemen automatisch mitinstalliert und ist uneingeschränkt nutzbar. Bei Linux gilt die Unterstützung seit Kernel-Version 2.6, bei Solaris ab Version 8, bei AIX mit Version 4.3, bei MAC OS X seit Version 10.2.

5. Setzen Sie das Häkchen bei IPV6-UNTERSTÜTZUNG AUF DIESEM HOST AKTIVIEREN und klicken Sie auf OK.
6. Starten Sie den Host neu.

Netzwerkdienste

Ein virtueller Switch stellt für den Host und die virtuellen Maschinen mehrere verschiedene Dienste zur Verfügung, die auf Portgruppenebene konfiguriert werden können (siehe Abbildung 6-6). Eine Portgruppe (Verbindungstyp) kann nur auf einem *bestehenden* Switch erstellt werden.

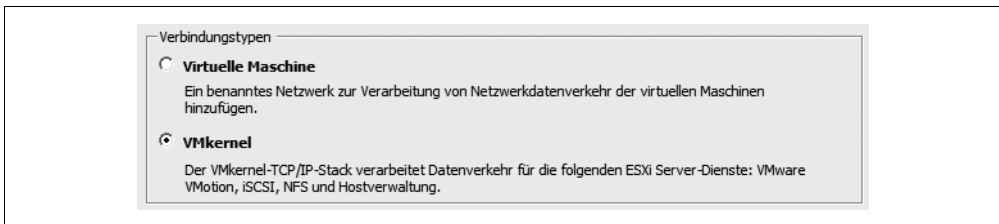


Abbildung 6-6: ESXi Netzwerkverbindungstypen

Man unterscheidet hier drei verschiedene Verbindungstypen:

- Die Verbindung von virtuellen Maschinen zum physischen Netzwerk sowie die Verbindung untereinander
- Das Verbinden von VMkernel-Diensten (zum Beispiel NFS, iSCSI, vMotion oder FT) mit dem physischen Netzwerk
- Ausführen von Management-Diensten für ESXi über die Hostverwaltung. Ein Management Network Port, der standardmäßig während der Installation festgelegt wird, ist für ESXi erforderlich, damit eine Verbindung mit Netzwerk- oder Remote-Diensten (einschließlich vSphere Client) eingerichtet werden kann.



Bei ESXi Hosts stehen nur zwei Verbindungstypen zur Verfügung (siehe Abbildung 6-6). Es gibt also keine Trennung zwischen VMkernel-Port und Remote-Zugriff: Beides wird über einen Managementport abgewickelt. Da beides beim ESXi nicht getrennt werden kann und keine unterschiedliche Gateways dafür eingetragen werden können, hat man hier wenig Flexibilität bezüglich unterschiedlicher Subnetze.

Die Konfiguration des Netzwerks kann über den vSphere Client erfolgen. Klicken Sie dazu auf einen ESXi Server und anschließend auf die Registerkarte KONFIGURATION. Im Abschnitt HARDWARE finden Sie unter anderem NETZWERK.

VLAN

Unter VLANs (*Virtual Local Area Networks*) versteht man virtuell voneinander getrennte Netzwerke auf einem Switch oder über mehrere physische Switches verteilt. Man benötigt also nicht zwingend zwei Switches, um zwei getrennte Netzwerke aufzubauen. Die Zugehörigkeit eines Rechners zu einem VLAN wird über eine VLAN-ID geregelt.

Um von einem VLAN in das andere zu gelangen, ist man auf einen Router oder einen Layer3-Switch angewiesen (die Routing-Funktionalität ist in den Switch integriert). Um einem Rechner alle VLANs zugänglich zu machen, muss man einen sogenannten »Trunkport« konfigurieren, der allerdings von der Netzwerkkarte des Systems auch unterstützt werden muss (802.1q-Unterstützung).

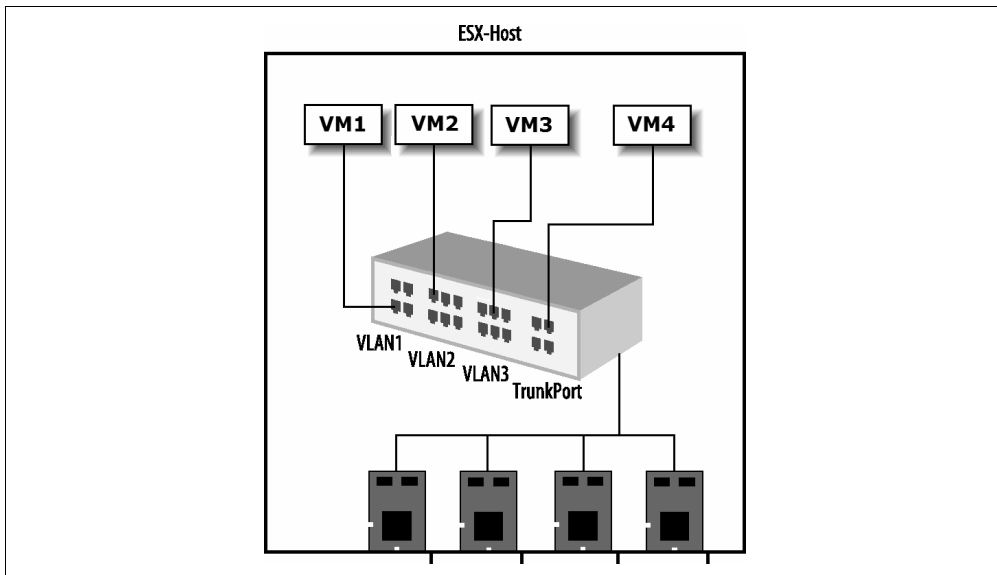


Abbildung 6-7: Host mit vier VMs und drei VLANs

In Abbildung 6-7 ist ein Hostsystem mit vier physischen Netzwerkkarten und vier laufenden virtuellen Maschinen zu sehen. Es sind hier vier virtuelle Netzwerke mit jeweils einer physischen Netzwerkkarte eingerichtet. Der Switch ist mit drei VLANs und einem Trunkport konfiguriert.

Es entsteht somit folgende Konstellation:

- VM1 ist im VLAN1 angesiedelt und sieht damit alle Systeme in VLAN1.
- VM2 ist im VLAN2 angesiedelt und sieht damit alle Systeme in VLAN2.
- VM3 ist im VLAN3 angesiedelt und sieht damit alle Systeme in VLAN3.
- VM4 ist auf einen Trunkport konfiguriert und sieht somit alle Systeme in VLAN1, VLAN2 und VLAN3.

Wie Sie sehen, können diese VLANs bei der Einrichtung der virtuellen Maschinen von Vorteil sein, weil man verschiedene virtuelle Netzwerke einrichten kann, die wiederum in verschiedenen VLANs liegen. Damit sind sehr sichere Netzwerke innerhalb der virtuellen Maschinen möglich. Bei vielen meiner Kunden werden VLANs anstelle von Subnetzen eingesetzt. Sie können dieses Prinzip auch für getrennte Netze nutzen, z.B. für die Buchhaltung und die Finanzabteilung.

VMware ESXi unterstützt über die realen VLANs hinaus auch »virtuelle VLANs«, die eine Trennung der VLANs durch virtuelle Switches erlauben. Daraus ergeben sich sehr flexible Möglichkeiten bezüglich der virtuellen Netzwerkstruktur, die von VMware Workstation und Microsoft Virtual Server nicht geboten werden.

Virtual Switch Tagging

Hier wird die Zuordnung der VLANs vom VMkernel übernommen und auf die virtuellen Switches übertragen (siehe Abbildung 6-8). Dazu müssen Sie den physischen Adapter des Wirtsystems mit einem Trunkport auf dem physischen Switch verbinden, damit alle Pakete und damit auch alle VLAN-IDs diesen Port passieren. Der Trunkport muss vom Switch her so konfiguriert werden, dass keine VLAN-IDs entfernt werden.

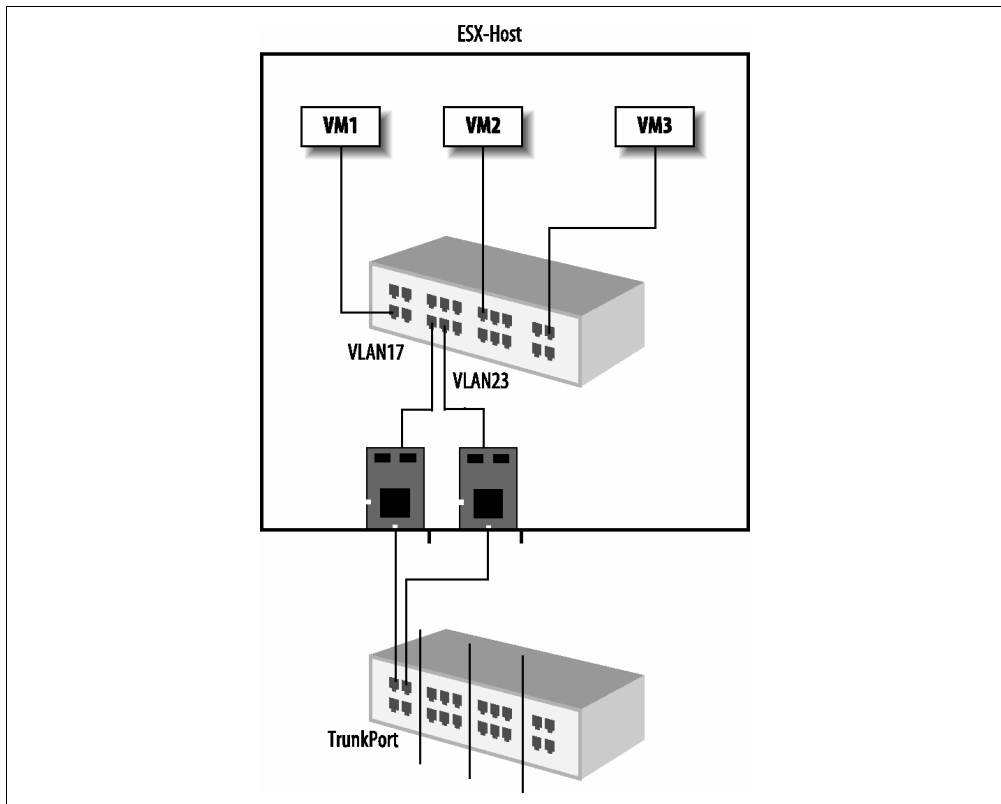


Abbildung 6-8: VLANs werden nur über den VMkernel realisiert.

Der VMkernel – in Form des virtuellen Switch – passt die getaggten Pakete dann so an, dass die virtuellen Maschinen nur die für sie bestimmten Pakete erhalten. Da die emulierten Netzwerkkarten kein VLAN-Tagging unterstützen, werden durch den VMkernel alle VLAN-relevanten Daten entfernt oder hinzugefügt, je nachdem, ob das Paket zur virtuellen Maschine unterwegs ist oder von ihr kommt.

Anhand des Beispiels in Abbildung 6-8 können Sie diese Konstellation genau nachvollziehen. Die beiden physischen Netzwerkadapter des Hostsystems sind auf einen Trunkport am physischen Switch gesteckt. Sobald nun Pakete mit der VLAN-ID 17 ankommen, wird das VLAN-Tagging durch den virtuellen Switch vom VMkernel entfernt und an die VM1-Netzwerkkarte weitergeleitet. Diese bekommt keine Informationen über die VLAN-Zugehörigkeit mehr mitgeteilt. Da die virtuellen Netzwerkkarten generell kein VLAN-Tagging verstehen, ist das auch die einzig sinnvolle Möglichkeit.

Wenn nun Pakete von der virtuellen Maschine VM1 verschickt werden, erweitert der virtuelle Switch das Paket automatisch um die VLAN-Tagging-Informationen. Genauso passiert es auch bei VM2, außer dass hier nur Pakete für VLAN-ID 23 vorbeigeschleust werden. Laut VMware wird die Netzwerkleistung dadurch nur minimal beeinträchtigt.

Um das Virtual Switch Tagging einzurichten, müssen Sie unter VMware ESXi mit sogenannten *Port Groups* oder Portgruppen arbeiten. In diesem Fall müssten Sie zwei Portgruppen einrichten: eine für VLAN-ID17 und eine für VLAN-ID 23. Dazu müssen Sie im vSC beim Erstellen des vSwitch eine VLAN-ID (siehe Abbildung 6-9) unterhalb des zu verwendenden virtuellen Netzwerks bei den Portgruppen einrichten.

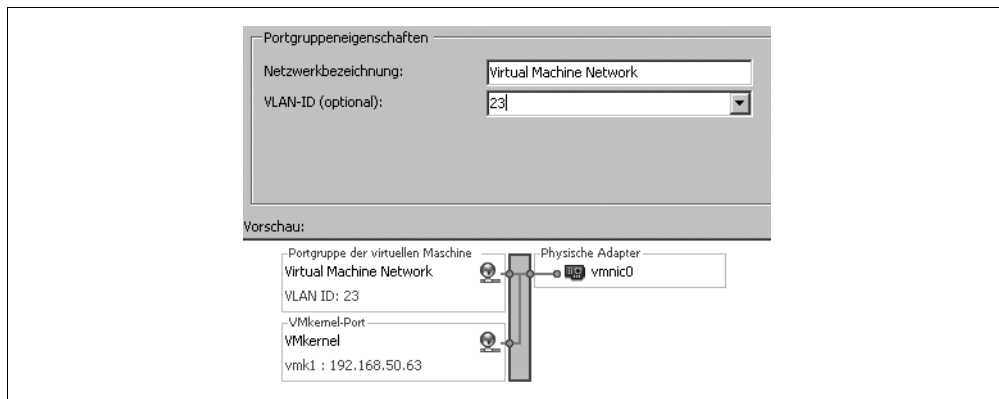


Abbildung 6-9: Einrichten eines VLANs für die VMs

Hier sollten Sie nun einen sprechenden Namen wählen, um später die Portgruppe direkt mit der VLAN-ID in Verbindung bringen zu können. Als VLAN-ID können Sie entweder eine zugeordnete VLAN-ID oder einen zugeordneten VLAN-ID-Bereich angeben, falls mehrere VLANs in der Portgruppe ankommen sollen.

Nachdem Sie die Portgruppen angelegt haben, sehen Sie sie unterhalb des entsprechenden virtuellen Netzwerks und können sie dort bearbeiten.

Sobald die Portgruppen eingerichtet sind, stehen Ihnen für die virtuellen Maschinen nur noch diese als Netzwerkverbindung zur Verfügung und nicht mehr der virtuelle Switch selbst.

Da die Netzwerknamen zum Funktionieren von vMotion immer gleich sein müssen, sollten Sie diese Portgruppen – wenn Sie vMotion verwenden möchten – bei allen beteiligten VMware ESXi Servern identisch benennen.

VLAN-Einsatz

Durch die Verwendung von VLANs, also virtuellen LAN-Umgebungen, kann man nur mit Switches Netzwerke logisch voneinander trennen und auf Router verzichten (Details siehe vorhergehenden Abschnitt).

Diese VLANs können entweder auf einem einzelnen speziellen Switch konfiguriert oder über mehrere verteilt werden. Dadurch können innerhalb einer durch Switches verbundenen Netzwerkinfrastruktur mehrere virtuelle Netzwerkumgebungen hergestellt werden, um beispielsweise Abteilungen sicher voneinander zu trennen.

Um von einem VLAN ins andere zu gelangen, ist zwingend ein Router oder ein Layer3-Switch erforderlich, der dann das Routing übernehmen kann. Außerdem gibt es die Trunkports, die VLAN-übergreifend alle Netzwerkpakete erhalten. Nun stehen Ihnen mehrere Wege offen, um die VLAN-Technologie in die virtuelle Umgebung zu bringen. VLANs werden anhand von VLAN-IDs voneinander unterschieden, die im Netzwerkpaket vermerkt sind. Dieses sogenannte VLAN-Tagging, das jedes Ethernet-Paket um vier Byte erweitert, in denen die VLAN-ID hinterlegt ist, wird im Netzwerkstandard IEEE 802.1q definiert.

Physisch am Switchport

Eine Möglichkeit besteht darin, schon im Netzwerkswitch nur bestimmte VLANs für den Port anzugeben, auf dem auch die physikalische Netzwerkkarte des Wirtsystems eingesteckt ist. Die Netzwerkkarten des Wirtsystems müssen den 802.1q-Standard unterstützen, damit die VLAN-Funktionalität gegeben ist.

vNetwork-Standardswitches

Sie können abstrakte Netzwerkgeräte erstellen, die als Standard-vNetwork-Switches (vSwitches) bezeichnet werden. Wie bereits eingangs beschrieben, kann ein vSwitch den Datenverkehr intern zwischen verschiedenen virtuellen Maschinen sowie zwischen virtuellen Maschinen und externen Netzwerken steuern.

Ein vSwitch arbeitet wie ein physischer Ethernet-Switch. Die Standardanzahl an logischen Ports für einen vSwitch, der mit dem vSphere Client erstellt wird, ist 120. In ESXi kann ein vSwitch jedoch bis zu 4.088 Ports haben. Der vSwitch, der während der Installation automatisch erstellt wird, hat beim ESXi Server ebenfalls 120 Ports.

An jeden Port können Sie den Netzwerkadapter einer virtuellen Maschine anschließen. Jeder Uplink-Adapter, der mit einem vSwitch verknüpft wurde, verwendet keinen sichtbaren Port. Ein 120-Port-vSwitch hat also in Wirklichkeit 128 Anschlüsse, wobei die acht für physische Adapter nicht angezeigt werden. Jeder logische Port auf dem vSwitch gehört zu einer Portgruppe. Jedem vSwitch kann darüber hinaus mindestens eine Portgruppe zugewiesen werden. Sie können auf einem einzelnen Host maximal 4.096 vSwitch-Ports auf mehreren vSwitches einrichten und diese mit maximal 32 physischen Netzwerkkarten (je nach Typ) verbinden.

Portgruppen

Die Ports auf dem vSwitch werden in Portgruppen zusammengefasst und können unabhängig voneinander konfiguriert werden. Jede Portgruppe hat einen eindeutigen Bezeichner (Namen), der bei allen ESXi Servern identisch sein muss und nicht doppelt vorhanden sein darf. Dabei ist auch die Groß- und Kleinschreibung zu beachten, weil sonst eine VM z. B. nicht per vMotion verschoben werden kann.

Ein Host kann bis zu 4.096 Ports auf Portgruppen verwalten, davon dürfen aber nur 1.016 aktiv sein. Die Beschränkung der Portgruppen beim vCenter Server liegt bei 5.000 insgesamt (beim Distributed vSwitch sind es 30.000).

Eine logische Unterteilung des Datenverkehrs eines Ethernet-Segments durch VLAN kann einer Portgruppe bei Bedarf zugewiesen werden. Damit die Portgruppen, die sich auf anderen VLANs befinden, für eine Portgruppe sichtbar sind, muss die VLAN-ID bei dieser auf 4095 gesetzt sein.

Beachten Sie, dass die VLAN-IDs und die Bezeichnungen der Portgruppen bei allen beteiligten Hosts gleich sein müssen, um die Konnektivität ordnungsgemäß widerzuspiegeln.

Portgruppen für virtuelle Maschinen

Sie können einer virtuellen Maschine über den vSphere Client eine Portgruppe zuweisen, indem Sie in die Einstellungen der VM gehen, dort auf die Netzwerkkarte klicken und unter NETZWERKBEZEICHNUNG eine andere Portgruppe auswählen. VMs weitere Netzwerkkarten hinzuzufügen, ist ebenfalls möglich, für jede NIC kann ein anderer Anschluss gewählt werden.



Bedenken Sie beim Einrichten von Portgruppen für virtuelle Maschinen, ob Sie diese zwischen Hosts migrieren möchten. Falls ja, stellen Sie sicher, dass sich beide Hosts in derselben Broadcast-Domäne befinden, also im selben Schicht-2-Subnetz.

ESXi unterstützt die Migration virtueller Maschinen zwischen Hosts unterschiedlicher Broadcast-Domänen nicht, weil die migrierte virtuelle Maschine dann möglicherweise auf dem neuen Netzwerk keinen Zugriff mehr hätte.

Einen neuen vSwitch erstellen

Es ist nicht möglich, einen leeren virtuellen Switch ohne Portgruppen zu erstellen. VM-Portgruppen stellen das Netzwerk für virtuelle Maschinen bereit.

1. Klicken Sie in der Bestandsliste auf Ihren Host und dann auf das Register KONFIGURATION.
2. Unter HARDWARE wählen Sie NETZWERK aus. Oben rechts im Fenster befindet sich der Link zu NETZWERK HINZUFÜGEN, der einen Assistenten startet.
3. Wählen Sie einen der verfügbaren Verbindungstypen aus, um einen vSwitch zu erstellen. Nehmen Sie den Typ VIRTUELLE MASCHINE und klicken Sie auf WEITER.
4. Sie können EINEN VIRTUELLEN SWITCH ERSTELLEN auswählen oder einen der aufgelisteten vorhandenen vSwitches und die diesem zugewiesenen physischen Adapter, die für diese neue Portgruppe verwendet werden sollen (siehe Abbildung 6-10).

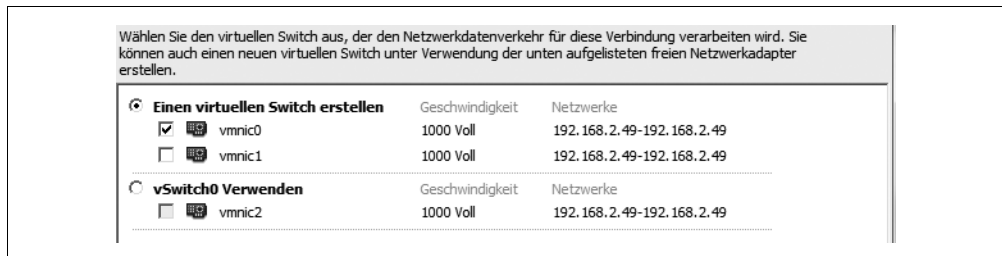


Abbildung 6-10: Auswahl der NICs (Network Interface Cards)

5. Klicken Sie auf WEITER.
6. Geben Sie unter PORTGRUPPENEIGENSCHAFTEN eine eindeutige, noch nicht vorhandene NETZWERKBEZEICHNUNG für die zu erstellende Portgruppe ein oder übernehmen Sie den Vorschlag.



Vergeben Sie beim Einrichten von Portgruppen sprechende Namen. Der Name VMkernel sagt z. B. nicht aus, welchem Zweck dieser dient. Wählen Sie stattdessen lieber »VMkernel iSCSI«, »VMkernel vMotion« oder etwas Entsprechendes.

7. Optional können Sie in das Feld VLAN-ID eine Zahl zwischen 1 und 4094 eingeben, wenn Sie ein VLAN verwenden. Wenn Sie 0 auswählen oder diese Option leer lassen, kann die Portgruppe nur normalen, also Nicht-VLAN-Datenverkehr sehen.

Geben Sie 4095 ein, kann die Portgruppe den gesamten Datenverkehr in einem VLAN sehen. Klicken Sie auf WEITER.

8. Sehen Sie sich die Zusammenfassung noch einmal an und klicken Sie dann auf BEENDEN. Kurze Zeit später erscheint der neue Switch grafisch dargestellt auf der Oberfläche.

Netzwerkconfiguration des VMkernels

Wie bereits erwähnt, wird eine Portgruppe des VMkernels für einige TCP/IP-Dienste benötigt. Dazu gehören

- der Hostverwaltungsdatenverkehr, über den der Netzwerkzugriff auf den Host funktioniert (Management Network),
- das Verschieben von VMs zwischen Hosts (vMotion),
- das Verschieben von Dateien von VMs auf andere Storages (Storage vMotion),
- das Synchronisieren von gespiegelten VMs (Fault Tolerance) und
- der Zugriff auf externen (IP-)Speicher wie iSCSI oder NFS.

Das Verschieben einer virtuellen Maschine per vMotion von einem Host auf einen anderen wird bei VMware übrigens »Migration« genannt. Mit vMotion können Sie laufende virtuelle Maschinen verschieben, ohne sie herunterfahren zu müssen. Damit das vMotion funktioniert, müssen die Einstellungen der Portgruppe des VMkernels auf jedem Host korrekt eingerichtet sein.

IP-Speicher wie iSCSI oder NFS können dieselbe VMkernel-Schnittstelle und -Portgruppe verwenden. Aus Performancegründen rate ich aber in produktiven Umgebungen davon ab. Nehmen Sie dafür – wenn möglich – lieber einen oder mehrere zusätzliche Netzwerkadapter an einem zusätzlichen vSwitch.

Der Netzwerkverkehr des VMkernels ist vollständig vom TCP/IP-Stapel der Hostverwaltung getrennt, auch wenn beide über den gleichen Outbound-Adapter angeschlossen sein sollten.

TCP/IP-Stapel auf VMkernel-Ebene

Der VMkernel-TCP/IP-Netzwerkstapel verarbeitet iSCSI, NFS und vMotion folgendermaßen:

- iSCSI wird als Datenspeicher für die Dateien von virtuellen Maschinen genutzt.
- iSCSI-Speicher ermöglicht die direkte Einbindung von ISO- und FLP-Dateien, die von virtuellen Maschinen als CD-/DVD-ROMs bzw. Floppys genutzt werden.
- NFS taugt auch als Datenspeicher für die Dateien von virtuellen Maschinen.
- NFS kann zum Anschluss von ISO- und FLP-Dateien verwendet werden, die für virtuelle Maschinen als CD-ROMs bzw. Floppys zur Verfügung stehen.

- Die Migration mit vMotion und Storage vMotion läuft ebenfalls direkt über den VMkernel, wobei Storage vMotion keine vMotion-aktivierte Portgruppe benötigt.
- Die Synchronisation von VMs im gespiegelten Modus (also Fault Tolerance) wird hierüber abgewickelt.



Wenn Ihr Host mehrere physische Netzwerkkarten hat, sollten Sie mehrere Pfade für das Software-iSCSI auf dem vSwitch konfigurieren (Multipathing) und möglichst Jumbo-Frames einsetzen.



ESXi unterstützt über TCP/IP nur die NFS-Version 3.



10-Gbit-Ethernet wird ebenfalls für iSCSI unterstützt. Sie können aber auch bis zu acht 1-Gbit-NICs zu einem Team zusammenschalten und auf iSCSI-Storages zugreifen.

Einrichten von VMkernel-Netzwerken

Die Einrichtung einer Portgruppe für den VMkernel läuft genauso ab, wie es oben für die VMs beschrieben wurde. Sie können einen neuen vSwitch erstellen oder auch einen vorhandenen auswählen und dort eine Portgruppe hinzufügen.

- Wenn Sie das Häkchen bei **DIESE PORTGRUPPE FÜR VMOTION VERWENDEN** setzen, meldet der Host diese Portgruppe als Broadcast den anderen Hosts im Cluster, so dass sie als die Netzwerkverbindung dienen kann, über die der Netzwerkverkehr für vMotion läuft.



Auf jedem Host kann die Eigenschaft für eine vMotion- und IP-Speicher-Portgruppe auch mehrfach aktiviert werden. Damit haben Sie die Möglichkeit, auch unterschiedliche Subnetze zu nutzen. Wenn diese Eigenschaft für keine der Portgruppen aktiviert wurde, ist eine vMotion-Migration auf diesen Host und von ihm weg nicht möglich.

- Wenn Sie das Häkchen bei **DIESE PORTGRUPPE FÜR DIE FEHLERTOLERANZPROTOKOLLIERUNG VERWENDEN** setzen, wird der Synchronisierungsdatenverkehr für Arbeitsspeicher, CPU und Cache zwischen gespiegelten virtuellen Maschinen darüber laufen (siehe Abbildung 6-11).
- Wenn Sie das Häkchen bei **DIESE PORTGRUPPE FÜR VERWALTUNGSDATENVERKEHR VERWENDEN** setzen, haben Sie eine redundante Zugriffsmöglichkeit über eine Remote-Verbindung auf den Host (siehe Abbildung 6-11). Diese Vorgehensweise empfehle ich zwecks Ausfallsicherheit; sie ist bei einem HA-Cluster Bedingung.

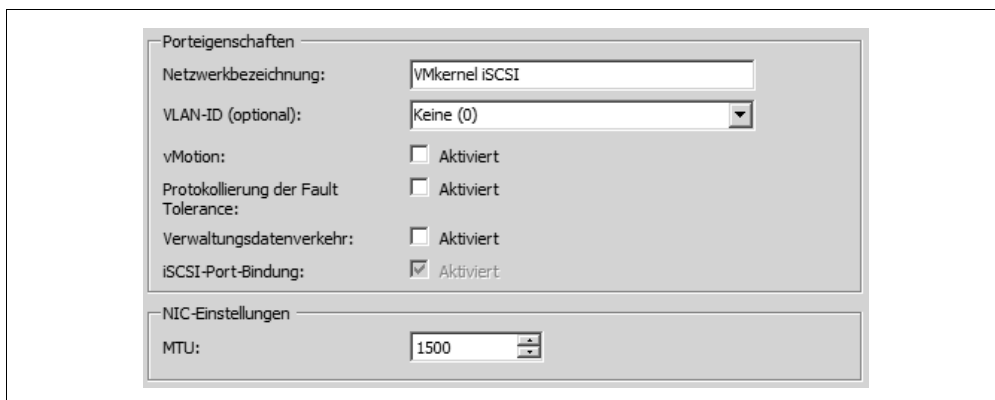


Abbildung 6-11: Portgruppe für den VMkernel auf dem ESXi Server

Die benötigten Angaben für die IP-Adressinformationen können Sie im nächsten Fenster machen. Die IP-Adresse muss eine andere sein als für den Remote-Zugriff, sie können aber dasselbe Gateway benutzen. Bei ESXi haben Sie nicht die Möglichkeit, ein anderes Gateway für den VMkernel zu wählen, können aber trotzdem IP-Adressen aus anderen Subnetzen verwenden.

Haben Sie auf dem Host IPv6 aktiviert und ihn ggf. neu gestartet, bekommen Sie eine weitere optionale Auswahlmöglichkeit, ob der Datenverkehr nur über IPv4 (IP Standardwert), nur über IPv6 oder über beides laufen soll.

Routing-Informationen von VMkernel-Ports anzeigen lassen

Nach der Erstellung einer Portgruppe können Sie sich über die Eigenschaften des vSwitch die Routing-Tabelle anzeigen lassen (siehe Abbildung 6-12). Klicken Sie dazu auf den Port und dann auf den blauen Link **ROUTING TABELLE ANZEIGEN**. Es öffnet sich ein neues Fenster mit drei Spalten: Die erste Spalte zeigt den Netzwerknamen (üblicherweise mit einer 0 am Ende) und in der zweiten steht die Subnetzmaske im gekürzten Format (die Zahl 24 bedeutet beispielsweise 24 Einsen für die Netz-ID und 8 für die Host-ID – hier also 255.255.255.0). In Spalte drei steht die Adresse für das Standardgateway.

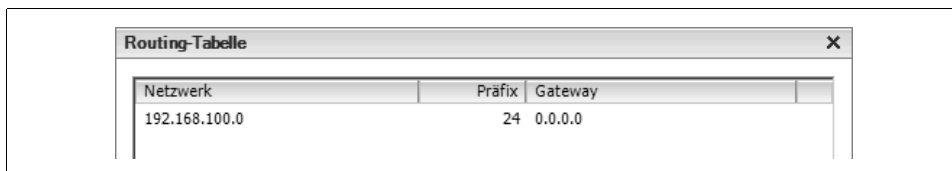


Abbildung 6-12: Routing-Tabelle auf dem ESXi Server

Konfiguration des Management Network

Auch das Management Network – also z.B. der Remote-Zugriff auf den ESXi Server über den vSphere Client oder den vCenter Server – ist ein VMkernel-Port und verwendet virtuelle Ethernet-Adapter zur Anbindung an einen vSwitch, um darüber Zugriff auf Netzwerke zu bekommen.

Wenn Sie nur einen Management Network Port angelegt haben, können Sie dessen Netzwerkeinstellungen zwar über die grafische Oberfläche ändern – sind Sie aber aktuell darüber mit dem Client verbunden, bekommen Sie eine Fehlermeldung und verlieren den Zugriff. Schließen Sie anschließend das Fenster und melden Sie sich erneut mit der geänderten IP-Adresse an. Auf der Kommandozeile ist diese Änderung ebenfalls möglich. Wollen Sie die Änderungen grafisch durchführen, ohne die Verbindung unterwegs zu verlieren, erstellen Sie eine zweite Management-Portgruppe, verbinden sich mit dieser und stellen die erste Verbindung neu ein oder löschen sie.

Einrichten des Managementnetzwerks

Während des Installationsvorgangs des ESXi Hosts wird bereits ein vSwitch mit Management Network und einem Netzwerk für die virtuellen Maschinen erstellt. Nachdem Sie sich mit dem ESXi Server verbunden haben, können Sie auch zusätzliche Portgruppen hinzufügen, ändern oder löschen.

Die Vorgehensweise ist ähnlich wie bei einem VMkernel-Port mit anderen Aufgaben, daher wird sie hier nicht nochmals beschrieben.



Es ist immer eine gute Idee, sich einen zweiten Management-Port einzurichten. Sollte mal eine NIC ausfallen, mit der Sie sich sonst verbunden haben, bleiben Ihnen nur noch der Weg in den Serverraum und das manuelle Erstellen einer neuen Verbindung auf der Kommandozeile oder über die direkte Konsole.

Wenn Sie Ihren ESXi Server über den vCenter Server in ein HA-Cluster nehmen wollen, ist ein zweiter Management-Port oder zwei NICs am ersten Pflicht.

Das Standardgateway festlegen

Für alle VMkernel-Portgruppen zusammen können Sie leider nur ein Standardgateway konfigurieren.

Beachten Sie dabei die folgenden wichtigen Punkte:

- Stellen Sie sicher, dass Ihre Netzwerkeinstellungen richtig sind, bevor Sie Änderungen speichern. Wenn Sie Netzwerkeinstellungen falsch konfigurieren, kann die Konnektivität zwischen Benutzeroberfläche und Host verloren gehen. In diesem Fall muss der Host über die Kommandozeile (direkte Konsole/ESXi-Shell) oder mit dem Menü erneut konfiguriert werden.

- Beim Management Network ist ein Gateway nur notwendig, wenn mindestens zwei Netzwerkadapter dasselbe Subnetz verwenden oder Sie HA einsetzen wollen. Das Gateway-Gerät bestimmt, welcher Netzwerkadapter für die Standardroute verwendet wird.
- Da Management Network und VMkernel für andere Aufgaben beim ESXi Server häufig nicht an dasselbe Netzwerk angeschlossen sind, müssen Sie Gateway-Informationen für das Management Network belassen.
- Wenn das zweite Management Network im selben Subnetz ist, verwendet diese den vSwitch des ersten Management Network. Das heißt: Sollte die erste Netzwerkkarte ausfallen, kommen Sie auch nicht mehr über die zweite dran, auch wenn das Bild auf der grafischen Oberfläche etwas anderes suggeriert! Das lässt sich nur auf der Kommandozeile beheben, indem Sie die Route manuell ändern.

So schaffen Sie Abhilfe:

1. Lassen Sie sich die Informationen zu den Portgruppen des VMkernel mit dem Befehl `esxcfg-vswitch -l` anzeigen.
2. Geben Sie in der Kommandozeile `esxcfg-route -l` ein, um sich die Routeninformationen anzeigen zu lassen.
3. Löschen Sie die Route, die falsch gesetzt ist, z.B. mit `esxcfg-route -d 192.168.50.0/24 192.168.50.10` (Kurzform) oder
4. `esxcfg-route -d 192.168.50.0 255.255.255.0 192.168.50.10` (Langform).

Übersicht über die Portgruppen

Die zwei möglichen Portgruppen auf einem vSwitch beim ESXi Host haben unterschiedliche Aufgaben zu bewältigen. Nicht immer ist auf den ersten Blick eindeutig klar, welche Aktivität in einem Cluster über welche Portgruppe abgewickelt wird. In Tabelle 6-1 finden Sie eine Auflistung der wichtigsten Aufgaben der Portgruppen.

Tabelle 6-1: Aufgaben der Portgruppen

Portgruppe	Aufgabe
virtuelle Maschinen	Anschluss der VMs an einen virtuellen Switch ggf. mit »Outbound-Adapter« an das physische LAN angebunden
VMkernel-Port – Management Network	Zugriff über den vSphere Client auf den ESXi Server Zugriff des vCenter Servers auf den ESXi Server Heartbeat des ESXi Servers zum vCenter Server High-Availability-Kommunikation der ESXi Server untereinander Storage vMotion auf andere Datenträger
Andere VMkernel-Ports	vMotion (Migration) zwischen den ESXi Servern Zugriff auf IP-Storages wie NFS und iSCSI Fault-Tolerance-Synchronisierung

Storage vMotion benötigt übrigens keinen aktivierten vMotion VMkernel Port.

Eigenschaften der Standardswitches

Die Standardeinstellungen eines vSwitch steuern alle Einstellungen für die Portgruppen. Durch die individuellen Portgruppeneinstellungen können Sie diese aber wieder außer Kraft setzen.

1. Klicken Sie auf den Link EIGENSCHAFTEN an dem Switch, den Sie konfigurieren wollen.
2. Klicken Sie auf vSWITCH und anschließend auf BEARBEITEN (siehe Abbildung 6-13). Im nun folgenden Fenster können Sie auf vier Registerkarten Einstellungen vornehmen.

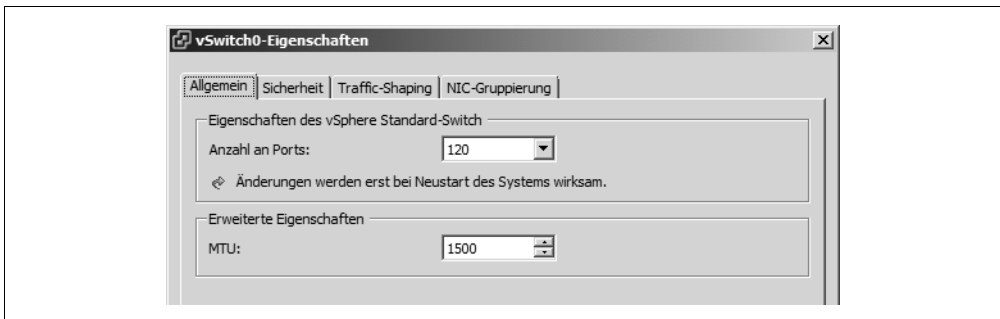


Abbildung 6-13: Eigenschaften des vSwitch

3. Wenn Sie die Anzahl der Ports in einem Bereich von 8 bis 4088 ändern, müssen Sie den Host anschließend neu starten, beim Erstellen oder Löschen eines vSwitch brauchen Sie das nicht.
4. Unter RICHTLINIENAUSNAHMEN können Sie drei sicherheitsrelevante Einstellungen vornehmen:
 - PROMISCUOUS-MODUS – Der Promiscuous-Modus deaktiviert jegliche Empfangsfilterung, die der virtuelle Netzwerkadapter normalerweise ausführen würde, so dass das Gastbetriebssystem den gesamten Datenverkehr aus dem Netzwerk empfängt. Zwar kann der Promiscuous-Modus für die Beobachtung der Netzwerkaktivitäten nützlich sein, aber er ist ein unsicherer Betriebsmodus, da jeder Adapter im Promiscuous-Modus Zugriff auf alle Pakete hat, auch wenn manche Pakete nur für einen spezifischen Netzwerkadapter bestimmt sind. Das bedeutet, dass ein Administrator oder *root*-Anwender in einer virtuellen Maschine rein theoretisch den Datenverkehr einsehen kann, der für andere Gast- oder Hostbetriebssysteme bestimmt ist.



Unter bestimmten Umständen ist es notwendig, einen virtuellen Switch in den Promiscuous-Modus zu setzen – zum Beispiel wenn Sie eine Software zur Netzwerkeinbruchserkennung oder einen Paketmitschneider (Network-Sniffer, beispielsweise Wireshark) verwenden wollen.

- **MAC-ADRESSÄNDERUNGEN (MAC ADDRESS CHANGES)** – In der Standardeinstellung ist diese Option auf AKZEPTIEREN (ACCEPT) gesetzt; der ESXi Server-Host akzeptiert also Anfragen, die geltende MAC-Adresse in eine andere als die ursprünglich zugewiesene Adresse zu ändern. Die Einstellungen der Option MAC-ADRESS-ÄNDERUNG beeinflusst den Datenverkehr, den eine virtuelle Maschine empfängt. Zum Schutz gegen MAC-Imitation können Sie diese Option auf REJECT (ABLEHNEN) setzen. In diesem Fall lehnt der ESXi Server-Host alle Anfragen ab, die geltende MAC-Adresse in eine andere als die ursprünglich zugewiesene Adresse zu ändern. Stattdessen wird der Port deaktiviert, der vom virtuellen Adapter zum Senden der Anfrage verwendet wird. Als Folge erhält der virtuelle Adapter keine weiteren Datenpakete mehr, bis er die geltende MAC-Adresse so ändert, dass sie mit der ursprünglichen MAC-Adresse übereinstimmt. Das Gastbetriebssystem erkennt nicht, dass die Änderung der MAC-Adresse nicht angenommen wurde.
- **GEFÄLSCHTE ÜBERTRAGUNGEN (FORGED TRANSMITS)** – In der Standardeinstellung ist diese Option auf AKZEPTIEREN (ACCEPT) gesetzt; der ESXi Server-Host vergleicht also nicht die Quelladresse und die geltende MAC-Adresse. Die Einstellungen der Option GEFÄLSCHTE ÜBERTRAGUNGEN ändern den Datenverkehr, der von einer virtuellen Maschine versandt wird. Zum Schutz gegen MAC-Imitation können Sie diese Option auf REJECT (ABLEHNEN) setzen. In diesem Fall vergleicht der ESXi Server-Host die Quell-MAC-Adresse, die vom Betriebssystem übertragen wird, mit der geltenden MAC-Adresse des Adapters, um festzustellen, ob beide übereinstimmen. Wenn die Adressen nicht passen, verwirft der ESXi Server das Paket. Das Gastbetriebssystem erkennt nicht, dass der virtuelle Netzwerkadapter die Pakete mit der imitierten MAC-Adresse nicht senden kann. Der ESXi Server-Host fängt alle Pakete mit imitierten Adressen vor der Auslieferung ab. Das Gastbetriebssystem geht gegebenenfalls davon aus, dass die Pakete verworfen wurden.



In bestimmten Situationen ist es tatsächlich notwendig, dass mehrere Adapter in einem Netzwerk dieselbe MAC-Adresse haben – zum Beispiel wenn Sie Microsoft-Netzwerklastausgleich (NLB) im Unicast-Modus verwenden. Bei der Verwendung von Microsoft NLB im Standard-Multicast-Modus haben die Adapter nicht dieselbe MAC-Adresse.

5. **TRAFFIC-SHAPING:** Über die Einstellungen DURCHSCHNITTliche BANDBREITE, SPITZENBANDBREITE und BURSTGRÖÖE (höchstmögliche Datenübertragung) können Sie den ausgehenden Datenverkehr beschränken, wenn Sie den STATUS auf AKTIVIERT gesetzt haben. Den eingehenden Datenverkehr können Sie nur über den neuen verteilten vSwitch vornehmen.
6. **NIC-GRUPPIERUNG:** Sie können an einen vSwitch bis zu acht Netzwerkkarten hängen und diese als Team Daten übertragen lassen. Die Einstellungsmöglichkeiten sind dabei nicht ganz trivial und hängen natürlich auch vom physischen Switch ab, der

die Leitungen von diesem Team entgegennimmt. Beim Lastenausgleich sind die folgenden vier Möglichkeiten gegeben.

- a. ANHAND DER QUELLE DER PORT-ID ROUTEN (*Route based on the originating virtual port ID*): Dabei werden die virtuellen Maschinen einfach auf die Netzwerkkarten aufgeteilt: VM1 → NIC1, VM2 → NIC2, VM3 → NIC3, VM4 → NIC1, VM5 → NIC2 usw.
- b. ANHAND DES IP-HASHES ROUTEN (*Route based on ip hash*): Das nennt sich auch *Link Aggregation*, *EtherChannel* oder *IEEE 802.3ad*. Hierfür muss der physische Switch konfiguriert werden. Die Pakete werden anhand der IP-Adresse über die NICs verteilt.
- c. ANHAND DES QUELL-MAC-HASHS ROUTEN (*Route based on source MAC hash*): Hier wird ähnlich wie bei IEEE 802.3ad gearbeitet, nur auf Basis der MAC-Adresse. Das hat aber einen Nachteil: Wenn z. B. viele Clients über einen Router angeschlossen sind – die ja alle die gleiche MAC-Adresse haben –, werden sie hiermit schlechter verteilt.
- d. AUSDRÜCKLICHE FAILOVER-REIHENFOLGE VERWENDEN (*Use explicit failover order*): Hier ist eine NIC aktiv, die anderen sind passiv.

Die weiteren Einstellungen auf der Registerkarte NIC-GRUPPIERUNG sind für Netzwerker (und nur die sollte man hier etwas einstellen lassen) selbsterklärend. Lediglich bei SWITCHES BENACHRICHTIGEN sollte man im Zusammenhang mit einem Cisco-Switch vorsichtig sein: Stellen Sie hier nur JA ein, wenn kein produktives LAN an diesem Switch angeschlossen ist, um es zu testen. (In der Praxis habe ich diesbezüglich Probleme gehabt.)

Die Geschwindigkeit eines Uplink-Adapters ändern

Die Verbindungsgeschwindigkeit und die Duplexeinstellung (Vollduplex = Senden und Empfangen gleichzeitig, Halbduplex = nacheinander) eines physischen Netzwerkadapters lassen sich nur über die Anzeige eines vSwitch oder auf der Kommandozeile ändern.

Zum Ändern gehen Sie folgendermaßen vor:

1. Klicken Sie im Bestandslistenfenster auf den Host, dann auf die Registerkarte KONFIGURATION und anschließend auf NETZWERK.
2. Wählen Sie einen vSwitch aus und klicken Sie auf den Link EIGENSCHAFTEN.
3. Klicken Sie hier auf die Registerkarte NETZWERKADAPTER.
4. Um die eingestellte Geschwindigkeit und den Duplexwert eines Netzwerkadapters zu ändern, markieren Sie den Netzwerkadapter und klicken auf BEARBEITEN.
5. Um die Verbindungsgeschwindigkeit manuell einzustellen, wählen Sie die Geschwindigkeits- und Duplexeinstellung im Drop-down-Menü aus. Die Verbindungsgeschwindigkeit muss manuell eingestellt werden, wenn die Netzwerkkarte oder ein physischer Switch die tatsächliche Verbindungsgeschwindigkeit nicht erkennt.

Anzeichen für falsche Geschwindigkeit und Duplex sind niedrige Bandbreite und fehlende Konnektivität. Der Adapter und der physische Switch, an den der Adapter

angeschlossen ist, müssen auf den gleichen Wert gesetzt werden, also entweder AUTO/AUTO oder GK/DM (wobei DM für den Duplexmodus Halb oder Voll und GK für die Geschwindigkeit steht), aber nicht AUTO/DM.

6. Klicken Sie auf OK.

Warum man eine Netzwerkkarte, die an keinem Switch angeschlossen ist, nicht ändern kann, entzieht sich meiner Logik. Falls in Ihrem Netz Probleme mit falsch eingestellten physischen NICs bekannt sind, erstellen Sie sich einfach einen Dummy-Switch, fügen alle freien Netzwerkkarten hinzu, konfigurieren sie und löschen den temporären Switch einfach wieder. Machen Sie das bei jedem vorhandenen ESXi Server oder nutzen Sie die Hostprofilfunktion, die in Kapitel 11 beschrieben wird.

Hinzufügen von Uplink-Adaptern

Im selben Fenster wie oben können Sie einem einzelnen vSwitch mehrere Adapter zuweisen, um NIC-Gruppierung zu bewirken. Die Gruppe kann den Datenverkehr gemeinsam verarbeiten und/oder Ausfallsicherheit gewährleisten.

Klicken Sie auf HINZUFÜGEN, um den Assistenten zum Hinzufügen eines Adapters aufzurufen. Wählen Sie mindestens einen Adapter in der Liste aus und klicken Sie auf WEITER. Optional können Sie die Netzwerkkarten einer anderen Kategorie zuordnen (STANDBY oder AKTIVE ADAPTER). Der Abschnitt NETZWERK auf der Registerkarte KONFIGURATION zeigt dann die Netzwerkadapter in der von Ihnen festgelegten Reihenfolge und den gewählten Kategorien.

Beachten Sie auch die Hinweise am Ende des Kapitels zur bestmöglichen Wahl der virtuellen Switches bei zwei, drei und mehr physischen Netzwerkkarten.

Cisco Discovery Protocol

Mit dem Cisco Discovery Protocol (CDP) können Sie den Cisco-Switchport bestimmen, mit dem ein bestimmter vSwitch verbunden ist. Wenn CDP für einen bestimmten vSwitch aktiviert ist, können Sie im vSphere Client die Eigenschaften des Cisco-Switch anzeigen (z.B. Geräte-ID, Softwareversion und Zeitlimit).

CDP auf einem ESXi Host aktivieren

vSwitches werden als Standard so eingestellt, dass sie Cisco-Portinformationen erkennen. Sie können auf der Kommandozeile des ESXi Servers auch den CDP-Modus so einstellen, dass ein vSwitch dem Cisco-Switch-Administrator Informationen bereitstellt. Gehen Sie dafür folgendermaßen vor:

1. Melden Sie sich direkt an der Konsole Ihres ESXi Hosts an.
2. Zeigen Sie den aktuellen CDP-Modus für den vSwitch an, indem Sie den Befehl `esxcfg-vswitch -b <vSwitch>` eingeben. Ist CDP deaktiviert, wird der Modus als down angezeigt.
3. Sie können den CDP-Modus ändern, indem Sie den Befehl `esxcfg-vswitch -B <mode> <vSwitch>` eingeben.

In Tabelle 6-2 werden die vier verschiedenen Modi aufgelistet und erklärt.

Tabelle 6-2: Cisco Discovery Protocol-Modi

Modus	Beschreibung
down	CDP ist deaktiviert.
Überwachen (listen)	ESXi erkennt und zeigt dem Administrator des Cisco-Switch Informationen zum verknüpften Cisco-Switchport an, jedoch stehen keine Informationen über den vSwitch zur Verfügung.
Werben (advertise)	ESXi stellt dem Cisco-Switch-Administrator Informationen zum vSwitch zur Verfügung, ohne jedoch Informationen zum Cisco-Switch zu erkennen bzw. anzuzeigen.
Beide (both)	ESXi erkennt Informationen zum verknüpften Cisco-Switchport, zeigt sie dem Administrator des Cisco-Switchs an und gibt Informationen über den vSwitch an den Cisco-Port weiter.

Cisco-Switch-Informationen anzeigen

Wenn CDP auf *Überwachen* oder *Beide* festgelegt ist, können Sie Cisco-Switch-Informationen über die grafische Oberfläche folgendermaßen anzeigen lassen:

1. Melden Sie sich am vSphere Client an und klicken Sie im Bestandslistenfenster auf den Host.
2. Klicken Sie auf die Registerkarte KONFIGURATION und anschließend auf NETZWERK.
3. Klicken Sie auf das Infosymbol (blaue Sprechblase) rechts neben dem vSwitch, und Sie bekommen eine Anzeige, wie sie in Abbildung 6-14 ist.

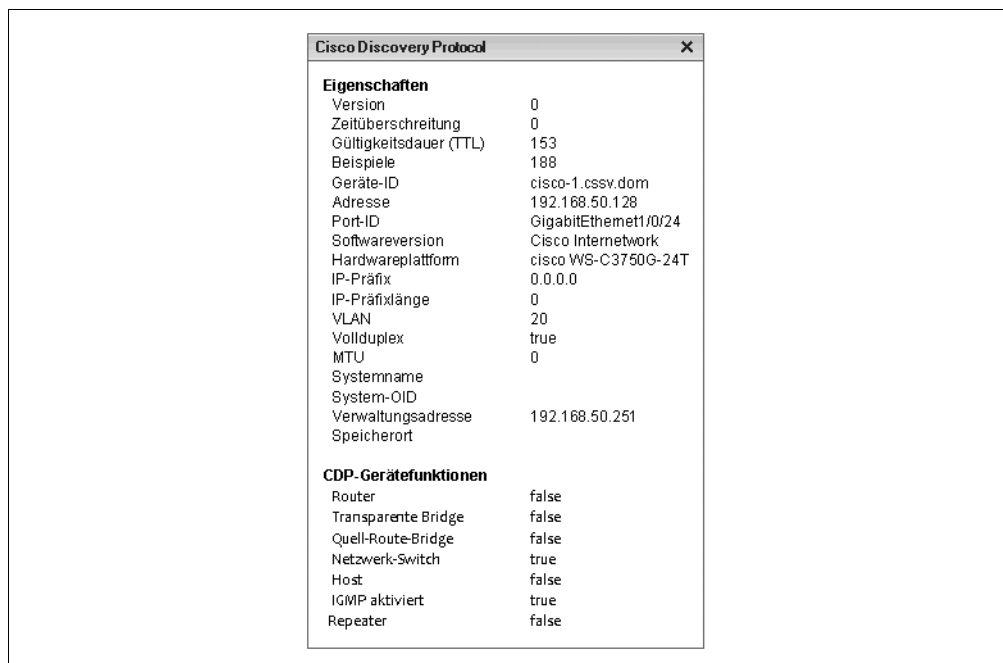


Abbildung 6-14: Cisco Discovery Protocol



Da die CDP-Hinweise zu Cisco-Geräten in der Regel einmal pro Minute generiert werden, kann es zwischen der Aktivierung von CDP für ESXi und der Verfügbarkeit von CDP-Daten auf dem vSphere Client zu einer spürbaren Verzögerung kommen. Auch mit der Taste F5 (aktualisieren) bekommen Sie die Anzeige nicht eher.

Sollte das bei Ihnen angezeigte Fenster auf der rechten Seite keine Einträge zeigen, ist an dem vSwitch entweder kein Cisco-Gerät angeschlossen, oder der Protokollmodus ist auf down (deaktiviert) gesetzt.

vSwitches optimieren

Es gibt im Wesentlichen zwei Möglichkeiten, vSwitches noch leistungsfähiger zu machen:

- Wie bei einer normalen GBit-Netzwerkkarte können Sie auch für einen vSwitch sogenannte Jumbo-Frames mit einer MTU-Größe (*Maximum Transmission Unit*) von bis zu 9.000 Bytes erstellen. Standardmäßig sind alle Netzwerkkomponenten bei vSphere5 auf die Standard-Ethernet-Größe von 1.500 Bytes gesetzt. Jumbo-Frames beschleunigen nicht nur den Datentransfer, sondern entlasten auch die CPU.
- Weiterhin besteht die Möglichkeit, das sogenannte *TCP Segmentation Offload* (TSO) einzusetzen, das die CPU stark entlastet.

TCP Segmentation Offload aktivieren

Bei der Standard-Ethernet-Größe von 1.500 Bytes müssen größere Pakete vor dem Versenden von der CPU in kleinere Stücke aufgeteilt und zur Netzwerkkarte geschickt werden. Beim TCP Segmentation Offload kann eine moderne NIC diese Arbeit selbst übernehmen. Wenn Sie einen VMkernel-Port erstellen, wird für diesen automatisch TSO eingerichtet. Auf der Kommandozeile können Sie das mit dem Befehl `esxcfg-vmknic -l` überprüfen. In der Spalte TSO steht dann ein Wert von 64 KByte, also 65.535 Byte.

Auch von einigen anderen Betriebssystemen wird die TSO-Technik unterstützt. Microsoft rät bei Windows 2000 und XP allerdings davon ab. Als virtuelle Maschine muss das unterstützte Betriebssystem eine VMXNET 2 (ERWEITERT)-Karte haben. VMware gibt in seinen Unterlagen nur vier Betriebssysteme an, bei denen TSO dann automatisch aktiviert ist:

- Microsoft Windows 2003 Enterprise Edition SP2 (32 und 64 Bit)
- Red Hat Enterprise Linux 4 (64 Bit)
- Red Hat Enterprise Linux 5 (32 und 64 Bit)
- SUSE Linux Enterprise Server 10 (32 und 64 Bit)

Überprüfen können Sie das im Betriebssystem der VM bei den Netzwerkkarteneinstellungen.

Jumbo-Frames aktivieren

Voraussetzung für Jumbo-Frames ist, dass *alle* beteiligten Komponenten (vom Sender bis zum Empfänger und zurück) die Rahmengröße (*Framesize*) unterstützen. Um dies bei einem vSwitch einzustellen, gehen Sie auf seine Eigenschaften und klicken Sie auf den Link BEARBEITEN. Im folgenden Fenster können Sie bei den erweiterten Eigenschaften die MTU auf z.B. 9.000 setzen, indem Sie den Wert dort eingeben. Damit ändern Sie die MTU für alle angeschlossenen Outbound-Adapter.

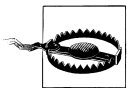
Über die Kommandozeile geht das auch: Dafür erstellen Sie einen neuen vSwitch mit Portgruppe, z.B. über die grafische Oberfläche, und setzen anschließend die MTU mit dem Befehl `esxcfg-vswitch`.

Beispiel:

```
esxcfg-vswitch -l                # zeigt die Switches an
esxcfg-vswitch -m 9000 vSwitch2  # MTU auf 9000 setzen
```

Die meisten `esxcfg`-Befehle können Sie mit einem kleinen `l` (list) aufrufen.

Übrigens: Auf den ESXi können Sie auch mit der Remote CLI (*Command Line Interface*) zugreifen. Dort lauten die Befehle allerdings meist ein wenig anders. Der Befehl `esxcfg-vswitch` heißt über Remote beispielsweise `vicfg-vswitch`, die Parameter sind aber die gleichen.



Die MTU für das Management Network und die VMs sollten Sie nicht unter 1.500 setzen, sonst kann die Konnektivität verloren gehen.

Bei VMware ist der Maximalwert für die MTU 9.000 Byte (9 KB).

Bei einer virtuellen Maschine können Sie natürlich auch Jumbo-Frames einsetzen: Die virtuelle Maschine muss dafür eine VMXNET 2 (ERWEITERT)-Karte haben und an einen dafür konfigurierten vSwitch angeschlossen sein. Im Betriebssystem selbst können Sie dann die MTU auf z.B. 9.000 setzen.

Sollte der zugewiesene Adapter nicht VMXNET 2 (ERWEITERT) sein, können Sie die Netzwerkkarte bei den Eigenschaften der VM löschen und ihm eine neue Karte hinzufügen. Achten Sie ggf. vor dem Löschen auf die MAC-Adresse. Kopieren Sie sich diese vorher und verwenden Sie die Zwischenablage, um sie der VMXNET 2 (ERWEITERT)-Karte wieder zuzuweisen.

Jumbo-Frames für VMkernel

Selbstverständlich kann auch die VMkernel-Schnittstelle mit Jumbo-Frames arbeiten. Gerade wenn Sie auf NFS- oder iSCSI-Storages zugreifen wollen oder die Schnittstelle für vMotion nutzen möchten, macht das an der Performance einiges aus. Der vSwitch, an den der VMkernel angeschlossen ist, muss ebenfalls für Jumbo-Frames eingerichtet sein, und natürlich auch alle physischen Switches und gegebenenfalls Router sowie die Schnittstelle des Storage bzw. der Gegenseite.

Die Einrichtung erfolgt entweder über die Kommandozeile auf dem ESXi Server, die Remote CLI für den ESXi oder über die grafische Oberfläche. Über den Befehl `esxcfg-vmknic -l` (kleines L) können Sie sich die Liste der VMkernel-Netzwerkkarten mit ihren Konfigurationen anzeigen lassen. Um nun die Jumbo-Frames auf der gewünschten Schnittstelle zu aktivieren, müssen Sie die Portgruppe mit dem VMkernel löschen und neu anlegen. Geben Sie folgenden Befehl ein:

```
esxcfg-vmknic -d <Portgruppenname>
esxcfg-vmknic -a -i <IP-Adresse> -n <Subnetzmaske> -m <MTU-Wert> <Portgruppenname>
```

Mit dem Befehl `esxcfg-vmknic -l` können Sie überprüfen, ob alles richtig eingegeben wurde.

Um die Einstellungen über den vSphere Client zu machen, gehen Sie wie oben beschrieben vor.

NetQueue auf ESXi aktivieren

Durch die Unterstützung von NetQueue durch die Netzwerkkarten können eingehende Datenpakete aus dem Netzwerk von mehreren CPUs gleichzeitig abgearbeitet werden. Das erhöht die Performance aber nur bei eingehenden Paketen und entlastet einen einzelnen Prozessor. Diese Einstellung ist auf dem ESXi normalerweise automatisch aktiviert. Um das zu überprüfen, müssen Sie auf dem ESXi Server **ERWEITERTE EINSTELLUNGEN** aufrufen:

1. Klicken Sie auf Ihren Host und dann auf die Registerkarte **KONFIGURATION**.

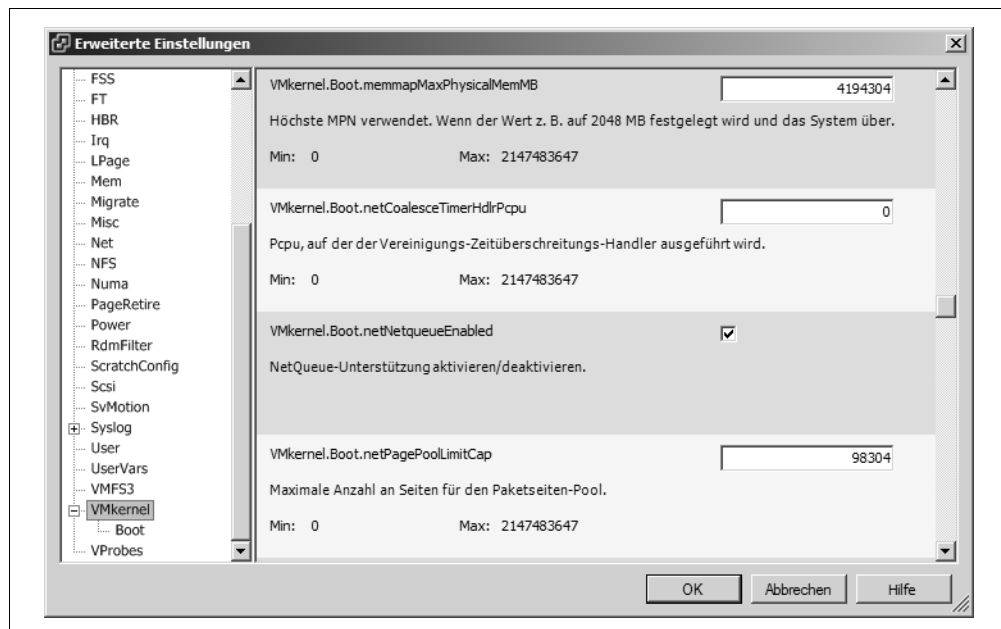


Abbildung 6-15: Erweiterte Einstellungen zum Netzwerk

2. Wählen Sie unter der Rubrik SOFTWARE die ERWEITERTEN EINSTELLUNGEN aus. Es öffnet sich ein neues Fenster.
3. Suchen Sie in der Liste auf der linken Seite den Eintrag VMKERNEL.
4. Rollen Sie auf der rechten Seite nach unten, bis Sie den Eintrag VMkernel.Boot.net-NetqueueEnabled sehen (siehe Abbildung 6-15). Das Häkchen muss gesetzt sein.



Die Einträge sind alphabetisch sortiert.

Wenn Sie bei den erweiterten Einstellungen Änderungen vorgenommen haben, muss der Host für die Übernahme neu gestartet werden.

Empfehlungen zu Netzwerkoptimierungen

VMware empfiehlt in seinen Publikationen einige Vorgehensweisen zum Optimieren der Netzwerkleistung. In der Praxis hat sich das meiste davon als überaus sinnvoll erwiesen. Auch im Internet finden sich nach langem Suchen einige Seiten, die durchaus gute Empfehlungen dafür bereithalten. Beachten Sie auch, dass einige Storage-Lösungen (wie iSCSI und NFS) ihre Daten über die Netzwerkkarten senden.



Wer sich nicht scheut, englische Dokumentationen zu lesen, dem empfehle ich zu diesem Thema die Seite <http://blog.scottlowe.org>. Unter ARCHIVES → NETWORKING oder auch STORAGE finden Sie einige Beispiele und Hinweise für die optimierte Konfiguration. Scott Lowe hat sich mit den Erklärungen sehr viel Mühe gegeben und dringt tief in die Materie ein.

Für kleinere bis mittlere Umgebungen sollten aber die Schilderungen zur Optimierung des Netzwerks bezüglich Performance und Sicherheit genügen, die VMware in seiner deutschsprachigen Dokumentation *vSphere-Netzwerk – ESXi 5.0.0.PDF* ab Seite 83 auflistet.

Fehlerbehebung auf der Konsole

Wenn bestimmte Teile der Netzwerkkonfiguration falsch eingestellt wurden oder ein Adapter ausgefallen ist, können Sie über den vSphere Client nicht mehr auf den ESXi Server zugreifen. In diesem Fall können Sie versuchen, die Netzwerkeinstellungen im Menü direkt am Server neu zu konfigurieren, oder Sie gehen mit der Tastenkombination Alt+F1 auf die erste Konsole und verwenden die VMware-Befehle. Funktioniert der Zugriff über SSH, z. B. putty, gibt es die gleichen Befehle wie direkt an der Konsole:

`esxcfg-vswitch -l`

Gibt eine Liste der bestehenden Konfigurationen für die virtuellen Switches aus. Prüfen Sie, ob der Uplink-Adapter, der für das Management Network konfiguriert wurde, mit dem geeigneten physischen Netzwerk verbunden ist.

`esxcfg-nics -l`

Gibt eine Liste der aktuellen Netzwerkadapter aus. Prüfen Sie, ob der Uplink-Adapter, der für das Management Network konfiguriert wurde, läuft und ob Geschwindigkeit und Duplex stimmen.

`esxcfg-nics -s <speed> <nic>`

Ändert die Geschwindigkeit eines Netzwerkadapters.

`esxcfg-nics -d <Duplex> <NIC>`

Ändert den Duplex eines Netzwerkadapters.

`esxcfg-vmknic -i <neue IP-Adresse> -n <Subnetzmaske> <Portgruppenname>`

Ändert die IP-Adresse und die Subnetzmaske des Management Networks.

`esxcfg-vmknic -a -i <neue IP-Adresse> -n <Subnetzmaske> <Portgruppenname>`

Fügt dem Management Network einen Adapter mit IP-Adresse und Subnetzmaske hinzu.

`esxcfg-vmknic -n <neue Subnetzmaske> <Portgruppenname>`

Ändert die Subnetzmaske des Management Networks.

`esxcfg-vswitch -U <alte vmnic> <vSwitch>`

Entfernt den Uplink für das Management Network.

`esxcfg-vswitch -L <neue vmnic> <vSwitch>`

Ändert den Uplink für das Management Network.



Wenn Sie bei `esxcfg`-*-Befehlen lang warten müssen, kann das an einer falschen DNS-Einstellung liegen. Die `esxcfg`-*-Befehle setzen voraus, dass DNS so konfiguriert ist, dass die Namensauflösung des lokalen Servers ordnungsgemäß funktioniert. Das wiederum setzt voraus, dass die `/etc/hosts`-Datei einen Eintrag für die konfigurierte IP-Adresse und die Adresse 127.0.0.1 des lokalen Servers enthält.

Problemlösungen bei Netzwerkadaptern

Das Hinzufügen eines neuen Netzwerkadapters kann in bestimmten Fällen zum Verlust des Management Networks und der Verwaltungs- und Wartungsfreundlichkeit mit dem vSphere Client führen, was daran liegt, dass die Netzwerkadapter neu benannt werden. Wenn das der Fall ist, müssen Sie die betroffenen Netzwerkadapter umbenennen, die das Management Network nutzen.

Gehen Sie zum Umbenennen dieser Netzwerkadapter folgendermaßen vor:

1. Melden Sie sich direkt an Ihrer ESXi Server-Konsole an.
2. Verwenden Sie den Befehl `esxcfg-nics -l`, um sich anzeigen zu lassen, welche Namen Ihren Netzwerkadaptern zugewiesen wurden.

3. Verwenden Sie den Befehl `esxcfg-vswitch -l`, um sich anzeigen zu lassen, welche vSwitches – sofern überhaupt – jetzt den Gerätenamen zugewiesen sind, die nicht mehr durch `esxcfg-nics` angezeigt werden.
4. Verwenden Sie den Befehl `esxcfg-vswitch -U <old vmnic name> <vswitch>`, um Netzwerkadapter zu entfernen, die umbenannt worden sind.
5. Verwenden Sie den Befehl `esxcfg-vswitch -L <new vmnic name> <vswitch>`, um die Netzwerkadapter wieder hinzuzufügen, und geben Sie ihnen dabei die richtigen Namen.

Problemlösungen bei Portgruppen

Das Umbenennen einer Portgruppe bei bereits mit dieser Portgruppe verbundenen virtuellen Maschinen kann dazu führen, dass die Netzwerkkonfiguration der virtuellen Maschinen nicht mehr stimmt, die so konfiguriert sind, dass sie sich mit dieser Portgruppe verbinden.

Die Verbindung von virtuellen Netzwerkadaptern mit den Portgruppen erfolgt über den Namen, und der Name wird in der Konfiguration der virtuellen Maschinen gespeichert. Das Ändern des Namens einer Portgruppe führt nicht zu einer automatischen Massen-Neukonfiguration aller virtuellen Maschinen, die mit dieser Portgruppe verbunden sind.

Virtuelle Maschinen, die bereits eingeschaltet sind, werden weiterhin funktionieren, bis sie ausgeschaltet werden, da ihre Verbindungen zum Netzwerk bereits hergestellt sind. Schalten Sie eine Maschine ein, die noch die veralteten Informationen hat, bekommen Sie keine Fehlermeldung über den vSphere Client.

Der optimale Ansatz besteht darin, ein Umbenennen der Netzwerke nach ihrer Verwendung zu vermeiden. Nach dem Umbenennen einer Portgruppe müssen Sie jede zugeordnete virtuelle Maschine neu konfigurieren, die die Portgruppe verwendet, um den neuen Portgruppennamen entsprechend zu berücksichtigen.

Haben Sie einen vCenter Server, können Sie die beteiligten VMs in der Übersicht des Netzwerks sehen und anschließend konfigurieren. Arbeiten Sie direkt auf einem ESXi Server ohne den vCenter Server, müssen Sie jede virtuelle Maschine einzeln anklicken und sehen dann auf dem Kartenreiter ÜBERSICHT rechts unten unter NETZWERK den Namen der jeweils zugewiesenen Portgruppe.

Probleme bei der Namensauflösung

Auf der Registerkarte KONFIGURATION des ESXi Hosts können Sie die DNS-KONFIGURATION über den vSphere Client ändern. Im Namensfeld ist standardmäßig der Hostname eingetragen. Auch die DNS-Serveradressen und die Domäne, die während der Installation angegeben wurden, werden automatisch eingetragen. Überprüfen Sie, ob es sich um einen korrekten Eintrag handelt, der auch ein DNS-Suffix benötigt. Der ESXi Server

benötigt einen FQDN für die korrekte Namensauflösung und für HA. Notfalls editieren Sie die Datei `/etc/hosts` über die Kommandozeile des ESXi Servers und geben dort die beteiligten anderen Server inklusive des vCenter Servers ein.

Netzwerkpakete tracen über vSwitch

Sowohl das Management Network als auch die anderen Funktionen des VMkernels verwenden virtuelle Ethernet-Adapter zur Anbindung an einen vSwitch und zum Zugriff auf Netzwerke über diesen vSwitch.

Es gibt zwei häufig auftretende notwendige Konfigurationsänderungen für das Management Network: die Änderung von Netzwerkkarten (NICs) und die Änderung von Einstellungen für eine bestehende, in Verwendung befindliche Netzwerkkarte.

Eine Änderung der Management Network-Konfiguration ist nicht ratsam, wenn nur ein Management Network-Anschluss vorhanden ist. Möchten Sie eine neue Verbindung herstellen, sollten Sie die Netzwerkeinstellungen so ändern, dass eine weitere Netzwerkkarte verwendet wird. Nach der Überprüfung der Funktionsfähigkeit des neuen Anschlusses kann der alte Anschluss entfernt werden. Im Prinzip wird also die Netzwerkkarte gewechselt.

Wollen Sie beispielsweise die IP-Einstellungen des einzigen Management Networks über den vSphere Client ändern, bekommen Sie keine Warnmeldung. Unter KÜRZLICH BEARBEITETE AUFGABEN sehen Sie, dass die Änderung noch in Arbeit ist. Kurze Zeit später verlieren Sie den Kontakt über den vSphere Client. Sie können sich dann aber erneut mit den neuen IP-Informationen anmelden.



Es besteht das Risiko der Fehlkonfiguration, wodurch die Anwenderschnittstelle die Anbindung an den Host verlieren kann. In diesem Fall muss der Host über die Befehlszeileingabe der Kommandozeile neu konfiguriert werden.

Wollen Sie die IP-Pakete über diese Schnittstelle mitprotokollieren, müssen Sie den PROMISCUOUS MODE auf ACCEPT stellen, weil sich der Switch sonst wie ein Switch und nicht wie ein Hub verhält.

Das Ganze könnte dann zum Beispiel so aussehen:

```
esxcfg-vswitch -l                                # zum Anzeigen der Portgruppen
esxcfg-vswif --add --ip 192.168.50.12 -n 255.255.255.0 -p "VM Network" vswif1
                                                    # zum Hinzufügen
tcpdump -i vswif1                                # zum Überprüfen
```

Abbildung 6-16 veranschaulicht diese Einstellungen.

Für das Mitprotokollieren eignet sich z. B. das Programm *WireShark*, ehemals *ethereal*.

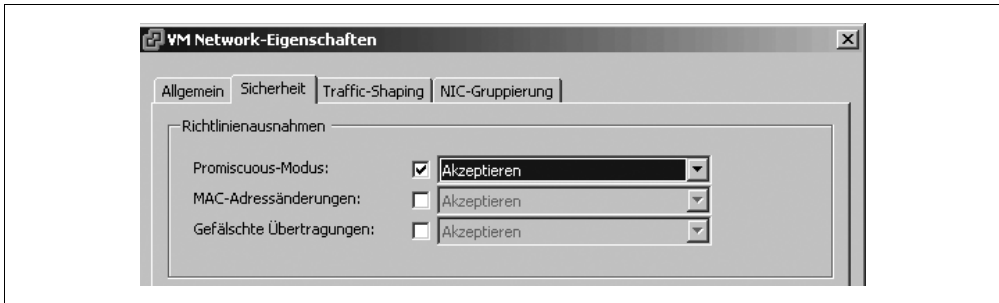


Abbildung 6-16: Die Portgruppe in den Hub-Modus setzen

Netzwerkkarten bestmöglich zuweisen

Die Mindestvoraussetzung für einen ESXi Host sind unter anderem zwei Netzwerkkadapter. Damit steht man dann vor dem Problem, wie die beiden Netzwerkkarten am besten auf die virtuellen Switches bzw. die notwendigen Portgruppen aufgeteilt werden können. Die Dokumentation von VMware lässt sich darüber leider nicht aus – es wird nur empfohlen, für verschiedene Aufgaben wie vMotion, Fault Tolerance, iSCSI und NFS jeweils einen eigenen Adapter zu nehmen. Bei nur zwei oder drei Karten ist das nicht möglich. Was macht man also, um bestmögliche Sicherheit, Performance und Redundanz zu bekommen? Und wie sieht es bei mehr Netzwerkkarten aus? Soll man diese zu einem Team zusammenschalten oder doch lieber einzeln lassen? Damit beschäftigt sich dieser Abschnitt.

Nehmen wir an, dass Sie insgesamt vier Portgruppen brauchen: Management Network, vMotion, iSCSI- oder NFS-Speicher und natürlich eine für die virtuellen Maschinen. Haben Sie Ihre ESXi Server in einem HA-Cluster, brauchen Sie noch eine Redundanz für das Management Network.

Zwei physische NICs

Bei der Mindestanzahl an Netzwerkkarten konfigurieren Sie einen einzigen virtuellen Switch mit allen notwendigen Portgruppen und fügen Sie diesem beide Adapter hinzu. Achten Sie darauf, dass beide Adapter beim vSwitch als aktiv gekennzeichnet sind, keiner nur als Standby.

Jetzt konfigurieren Sie die einzelnen Portgruppen und teilen die physischen Adapter folgendermaßen auf:

- *vmnic0 als aktiver Adapter und vmnic1 als Standby-Adapter für das Management Network und vMotion*
- *Der Storage-Zugriff für iSCSI darf keine Standby-Adapter haben. Konfigurieren Sie diese Portgruppe nur mit einer aktiven NIC.*
- *vmnic1 als aktiver Adapter und vmnic0 als Standby-Adapter für VM Network (Portgruppe der VMs)*

Dabei löschen Sie nicht den jeweils zweiten Adapter, sondern setzen nur die Failover-Reihenfolge des vSwitch außer Kraft. Damit ist *vmnic1* der Standby-Adapter von *vmnic0* und umgekehrt. Abbildung 6-17 veranschaulicht das nochmals für die Portgruppe der virtuellen Maschinen.

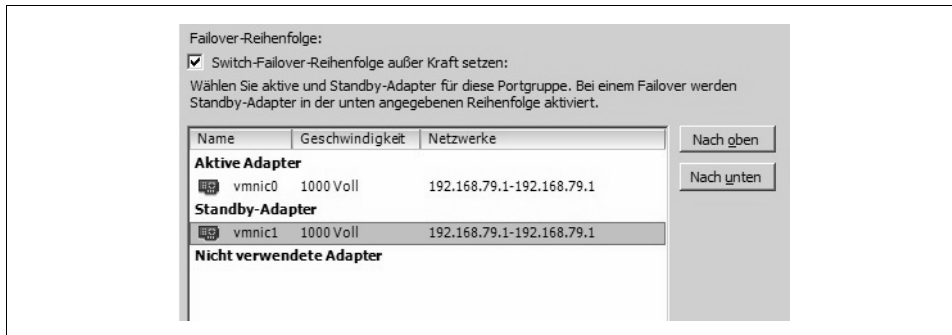


Abbildung 6-17: Die Failover-Reihenfolge außer Kraft setzen

Gerade wenn Sie VLANs nutzen wollen, empfehle ich genau diese Konstellation. Achten Sie bei einem möglichen Ausfall aber darauf, dass die noch arbeitende Karte auch auf die notwendigen VLANs Zugriff hat, z. B. über einen Trunkport.

Drei physische NICs

Wir gehen hier von den gleichen Voraussetzungen wie bei zwei Adaptern aus. Es werden also insgesamt vier Portgruppen gebraucht und es muss ggf. eine Redundanz für High Availability eingerichtet werden. Das geht entweder mit zwei Netzwerkkarten an einem vSwitch mit dem Management Network oder zwei Portgruppen auf zwei vSwitches verteilt.

Für dieses Szenario gibt es zwei Ansätze: Man kann drei vSwitches konfigurieren oder auch nur einen mit drei Adaptern verwenden.

Die Entscheidung zwischen einem oder drei Switches kann ich Ihnen nicht abnehmen. Das liegt am jeweiligen Datendurchsatz, den die einzelnen Portgruppen benötigen, und dem gewünschten Maß an Ausfallsicherheit.

Drei vSwitches: Möchte man lieber drei Netzwerkschwitches einrichten oder muss man verschiedene getrennte Subnetze nehmen, ohne VLANs einsetzen zu wollen, geht man wie folgt vor:

vmnic0 wird an *vSwitch1* gehängt und dort werden als Portgruppe ein Management Network und ein VM Network eingerichtet.

vmnic1 kommt an den zweiten Switch, dort richtet man den Zugriff auf den Storage ein.

vmnic2 schließt man an den dritten vSwitch an und macht dort die Portgruppe für vMotion und eine für die zweite Management-Portgruppe, als HA-Failover.

Damit hat man allerdings verloren, wenn eine der Netzwerkkarten ausfällt, weil keine Backupadapter mehr am jeweiligen vSwitch vorhanden sind. Die Gefahr, dass eine der NICs ausfällt, ist allerdings sehr gering.

Ein vSwitch: Bei diesem Vorgehen schließen wir alle drei Outbound-Adapter als aktive an einen vSwitch und konfigurieren alle vier Portgruppen nacheinander. Dann heben wir für die einzelnen Portgruppen wieder die Failover-Reihenfolge des Switch auf und teilen diese wie folgt neu zu:

- *vmnic0* wird als aktiver Adapter an die Portgruppe des VM Network angeschlossen, die anderen beiden Adapter kommen als Failover zu dieser Portgruppe hinzu.
- *vmnic1* ist der aktive Adapter für den Storage-Zugriff und *vmnic0* und *vmnic2* sind nicht als Ausfallsicherheit gedacht. Der Storage-Zugriff für iSCSI darf keine Standby-Adapter haben. Konfigurieren Sie diese Portgruppe nur mit einer aktiven NIC.
- *vmnic2* wird als aktive NIC an die Portgruppe für vMotion angeschlossen, *vmnic0* und *vmnic1* sind hierfür als Failover gedacht. Das zeigt Abbildung 6-18.

Falls Sie hier keine Netzwerkkarte für iSCSI oder NFS benötigen, weil Sie z.B. ein Fibre Channel SAN haben, teilen Sie die Portgruppen für vMotion und Management Network dementsprechend auf.

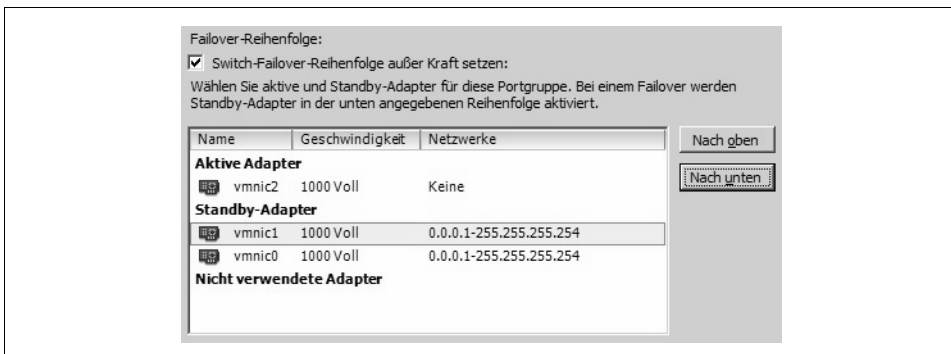


Abbildung 6-18: Die Failover-Reihenfolge außer Kraft setzen bei drei NICs

Sie haben außerdem die Möglichkeit, eine weitere Portgruppe für den Storage-Zugriff zu konfigurieren und diesen den Adapter der vMotion Portgruppe zuzuweisen.

Vier physische NICs

Wir gehen hier von den gleichen Voraussetzungen wie bei zwei und drei Adaptern aus. Es werden also wieder vier Portgruppen gebraucht und es muss ggf. eine Management Network-Redundanz für HA berücksichtigt werden.

Auch hier gibt es mehrere Möglichkeiten, eine Aufteilung zu machen. So kann man je eine Netzwerkkarte an einen vSwitch mit je einer Portgruppe hängen. Damit wären aber

keine Ausfallsicherheit gewährleistet und die Möglichkeiten des einen oder anderen Adapters nicht ausgeschöpft. Die dabei noch zu berücksichtigende HA-Redundanz könnte man erreichen, indem man einen zweiten Management Network Port auf demselben vSwitch erstellt, wo der vMotion Port liegt. Die Datenübertragungsrate für den Heartbeat liegt bei nur wenigen Bits, und vMotion wird ja eher selten gebraucht. Beim Zugriff auf einen Storage kommen hingegen ständig Datenpakete an und werden verschickt. Die Netzwerkkonnektivität der virtuellen Maschinen darf man natürlich auch nicht außer Acht lassen.

Bei dieser Betrachtungsweise – und wenn man zusätzliche Ausfallsicherheit haben möchte – gibt es eigentlich nur einen relevanten Ansatz: zwei vSwitches mit jeweils zwei Netzwerkkarten.

Dabei nehmen wir den ersten vSwitch für die Portgruppe der virtuellen Maschinen. Dann sind beide Adapter aktiv und wir lassen es bei den Einstellungen unter NIC-Gruppierung: Anhand der ursprünglichen ID des virtuellen Ports routen.

Beim zweiten vSwitch konfigurieren wir die Portgruppen für das Management Network, Storage-Zugriff und vMotion dann wie folgt:

- *vmnic2* ist aktiver Adapter für das Storage und *vmnic3* ist nicht sein Failover-Partner. Der Storage-Zugriff für iSCSI darf keine Standby-Adapter haben. Konfigurieren Sie diese Portgruppe nur mit einer aktiven NIC.
- *vmnic3* ist der aktive Adapter für vMotion und das Management Network und *vmnic2* ist sein Backup.

Überlegen Sie sich, ob Sie bei dieser Konstellation unterschiedliche Subnetze für vMotion und Management Network oder lieber VLANs einsetzen möchten.

Fünf physische NICs

In diesem Beispiel empfehle ich wie bei vier Karten, zwei vSwitches zu erstellen. Der erste wird mit zwei Adaptern und einer Portgruppe für die virtuellen Maschinen genommen. Die Einstellungen übernehmen wir von oben, wie bei vier Karten beschrieben.

Der zweite vSwitch bekommt drei Netzwerkkarten und wird über die Portgruppen wie folgt aufgeteilt:

- *vmnic2* ist aktiver Adapter für das Management Network.
- *vmnic3* ist aktiver Adapter für vMotion.
- *vmnic4* ist aktiver Adapter fürs Storage.

Die jeweils anderen Outbound-Adapter nehmen wir für das Failover, also *vmnic3* und *vmnic4* als Backup für das Management Network und so weiter. Der Storage-Zugriff für iSCSI darf keine Standby-Adapter haben, deshalb konfigurieren Sie diese Portgruppe nur mit einer aktiven NIC.

Auch hier sollten Sie unterschiedliche Subnetze oder VLANs nehmen, um den Datenverkehr aufzuteilen, wie in Abbildung 6-19 zu sehen ist.

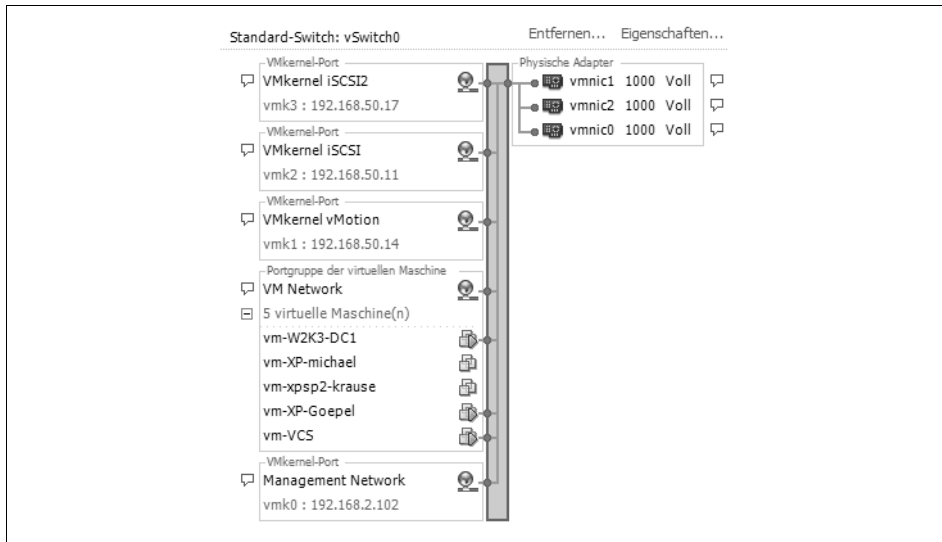


Abbildung 6-19: Der zweite vSwitch bei fünf NICs

Sechs physische NICs

In diesem Beispiel empfehle ich, drei vSwitches zu erstellen. Wir nehmen jeweils zwei physische Karten pro vSwitch und teilen die Portgruppen ähnlich wie bei fünf NICs auf.

Der erste Switch wird mit zwei Adaptern und einer Portgruppe für die virtuellen Maschinen genommen. Dabei belassen wir beide NICs auf aktiv und nehmen wie oben die Einstellungen zum NIC-Teaming.

Das Gleiche machen wir mit dem zweiten vSwitch und erstellen dort eine VMkernel-Portgruppe für den Storage.

Bei beiden vSwitches ist das Failover durch die zweite Karte gegeben und die Last wird schön aufgeteilt.

Anders sieht es beim dritten vSwitch aus. Hier nehmen wir ebenfalls zwei Karten, haben aber zwei Portgruppen zu bedienen. Deshalb setzen wir *vmnic4* als aktive Karte an die Portgruppe für vMotion und *vmnic5* als Standby. Umgekehrt beim Management Network: Hier ist *vmnic5* die aktive und *vmnic4* dient der Ausfallsicherheit.

Auch wenn hier viele physische Adapter auf die Portgruppen aufgeteilt werden können, empfehle ich, unterschiedliche Subnetze oder VLANs einzusetzen.

Hat man mehr als sechs Netzwerkkarten zur Verfügung, geht man wie in den obigen Beispielen vor. Überlegen Sie sich, welche Netzwerkdatenübertragungen zu erwarten sind und teilen Sie die Karten dementsprechend logisch auf.

Beachten Sie dabei, dass das Management Network für High Availability zwar redundant vorhanden sein muss, dass aber hier nur sehr geringer Datenverkehr herrscht. vMotion wird in produktiven Umgebungen nicht sehr häufig vorkommen, sollte aber ebenfalls eine Redundanz haben. Am wichtigsten bleiben aber die Netzwerkverbindungen zu den virtuellen Maschinen: Fallen diese aus, können die User nicht mehr auf ihre Server zugreifen. Dasselbe gilt natürlich für den Zugriff der VMs auf ihre Festplatten. Ist diese Verbindung unterbrochen, hängen sich die meisten Betriebssysteme auf und lassen sich nur über einen harten Reset wieder reaktivieren.

Sehr wichtig ist natürlich auch der Heartbeat der ESXi Server bei HA im Cluster untereinander samt richtiger Einstellung dazu. Dazu erfahren Sie mehr in Kapitel 10, *Der vCenter Server*.

Storage-Konfiguration

Bevor Sie weitere virtuelle Maschinen auf den ESXi Servern erstellen, sollten Sie die Storage-Zugriffe der Hosts konfigurieren. In diesem Kapitel gehe ich detailliert auf dieses wichtige Thema ein.

Insgesamt kann der ESXi Server auf fünf verschiedene Storage-Lösungen zugreifen:

- lokal angeschlossene SCSI-, SAS- und SATA-Laufwerke
- iSCSI SAN über Netzwerkkarten oder HBAs
- NFS über Netzwerkkarten
- Fibre Channel SAN über spezielle Adapter
- VSA, lokaler Speicher von zwei oder drei ESXi Servern

Alle fünf Möglichkeiten werden hier mehr oder weniger detailliert behandelt. Zusätzlich wird erklärt, wie man sich einen günstigen Storage anlegt und worauf man dabei besonders achten sollte. Die letzten vier Typen in der obigen Aufzählung sind Speichermöglichkeiten, auf die alle beteiligten Hosts zugreifen können. Über den vCenter Server hat man dann erst die Möglichkeiten, Technologien wie vMotion, High Availability, DRS (Load Balancing) und Fault Tolerance zu nutzen.

Auch das Thema Storage-Alignment darf natürlich nicht zu kurz kommen. Ohne eine Anpassung der Cluster auf einem Volume kann die Übertragungsgeschwindigkeit erheblich leiden.

Allgemeine Richtlinien

Bevor Sie eine weitere Festplatte lokal an den ESXi Server anschließen oder die Verbindung zu einem externen Storage aufbauen, sollten Sie einige Überlegungen zum neuen Speicher anstellen. Mit dem folgenden Absatz möchte ich Ihnen dabei helfen, die richtigen Entscheidungen bei Ihrer Wahl zu treffen.

Lokale Platten

Eine SATA- oder SCSI-Festplatte, Fibre-Channel-LUN oder RAID-LUN mit nicht partitioniertem, mindestens 5 GByte großen Bereich gelten als Mindestvoraussetzung für die Installation des ESXi Servers. In diesem Laufwerk oder RAID-Verbund werden die Dateien für den Hypervisor und gegebenenfalls später die Dateien der virtuellen Maschinen abgelegt. Da Sie für die Installation nur eine kleine Platte brauchen, sollten Sie während der Installation auch nur diese benutzen. Nach der Installationsroutine hinzugefügte Laufwerke können sie über den vSphere Client konfigurieren – und dabei findet das Disk-Alignment an der 64-K-Grenze für das VMFS-Dateisystem automatisch statt.

Ein einziges Volume hätte den Nachteil, dass das ESXi-System gleichzeitig mit den virtuellen Maschinen denselben Plattenplatz nutzt und sich damit die Übertragungsleistung mit diesen teilt. Dieses zu trennen, ist also sinnvoll. Leider verkaufen namhafte Serverhersteller ihre Geräte z.B. mit sechs 300-GB-Platten an einem RAID-Controller angeschlossen und konfigurieren damit ein RAID 6. Dabei geht nicht nur Performance verloren, sondern auch sehr viel Plattenplatz. Betrachtet man dagegen die Möglichkeiten, die man seit dieser Version von vSphere 5 mit VSA (siehe unten) hat, ergibt so eine Konfiguration gar keinen Sinn.

Beachten Sie auch die Namensgebung des lokalen Storage: Standardmäßig heißt er nach der Installation *datastore1*. Daran ist so lange nichts auszusetzen, wie der ESXi Server nicht zu einem Cluster gehört. Der erste ins Cluster aufgenommene Host behält den Namen des Speichers, beim zweiten wird dieser zu *datastore1(1)*, beim dritten zu *datastore1(2)* usw. Hinterher ist es dann schwierig, den lokalen Speicherplatz einem ESXi Server zuzuordnen. Benennen Sie ihn doch gleich in *esx1-datastore1* um.

Externe Platten

Wie bei den lokalen Platten gelten natürlich auch hier die Überlegungen zur Namensgebung. Gerade wenn Sie mehrere unterschiedliche externe Systeme haben, ist es meist schwer zu sagen, ob es sich bei einem Volume nun um das FibreChannel- oder iSCSI-SAN handelt. Man sollte natürlich auch nicht übertreiben und seinen Storage z.B. *NFS-Server-2008-R2-Storage-2-TB-Volume-001* nennen. Haben Sie davon z.B. drei Stück, können Sie in keiner Tabelle mehr das *001*, *002* oder *003* sehen.

Gedanken sollte man sich auch über die anzulegende Größe machen. Die Grenze von 2 TByte pro Volume ist ab dieser Version nicht mehr relevant. Die neue Obergrenze liegt jetzt bei 64 TByte. Wählen Sie das geeignete Maß für Ihre Anwendungen. Beachten Sie ggf. die Möglichkeit, in den externen Systemen mehrere unterschiedliche RAID-Levels für die Volumes zu nutzen und diese sinnvoll an Ihre VMs zu verteilen.

Viele kleine LUNs schränken Sie bei der eventuell notwendigen Vergrößerung einer Datenfestplatte unnötig ein. Auch für Snapshots – zum Beispiel bei der Datensicherung – muss noch genügend Platz vorhanden sein. Weiterhin haben Sie dann eine sehr lange Liste mit Datastore-Namen. Im Gegensatz dazu bieten kleinere Volumes den Vorteil, dass verschiedene RAID-Level für die Speicherplätze genutzt werden können und die Leistung höher ist als bei großen, gemeinsam von VMs genutzten Volumes.

Auf jeden Fall müssen Sie die LUNs (Nummern) im Auge behalten. Vergeben Sie für jede LUN eine eigene Nummer, am besten aufsteigend von 0 angefangen.

Bei wichtigen virtuellen Maschinen können Sie eine Spiegelung einrichten. Diese muss nicht vom Hersteller des externen Speichers unterstützt werden. Einem Windows-Server können Sie beispielsweise zwei Festplatten auf unterschiedlichen Volumes geben, diese im Betriebssystem auf »dynamischer Datenträger« setzen und eine Spiegelung (RAID-Level 1) dafür einrichten.

iSCSI-Speicher anschließen

Speicher, der über das Netzwerk mit dem SCSI-Protokoll angeschlossen wird, hat in der jüngeren Vergangenheit immer mehr Einsatz in kleinen und mittleren Umgebungen gefunden. Das liegt nicht nur am deutlich günstigeren Preis gegenüber einem Fibre Channel-SAN, sondern auch an der mittlerweile recht guten Performance. Bei einigen Linux-Distributionen gehört die Möglichkeit, einen vorhandenen Festplattenplatz als iSCSI-Target zur Verfügung zu stellen, schon länger zur Grundausstattung. Nicht immer wird diese Möglichkeit bei einer Standardinstallation schon zum Umfang gehören, aber sie lässt sich ohne große Probleme nachrüsten.

Wer sich mit Solaris auskennt, kann hier zusätzlich das neue Dateisystem ZFS nutzen, das zusammen mit iSCSI enorme Leistungswerte erzielt.

Es werden aber auch von einigen namhaften Herstellern günstige komplette Storage-Lösungen auf Basis von »SCSI over IP« angeboten. Meistens bekommt man für 2.000 bis 3.000 Euro schon eine stabile Plattform im 19-Zoll-Rahmen mit 2 TByte Speicherplatz und 4-GBit-Anbindung.

Unter Windows gibt es bei den neueren Versionen lediglich eine Zugriffsmöglichkeit auf iSCSI-Speicher von Microsoft (iSCSI-Initiator), aber nicht das Bereitstellen von Platz über die Netzwerkkarte. Dafür gibt es aber diverse andere Softwarehersteller, die für Windows-Betriebssysteme einen solchen Zugriff zur Verfügung stellen.

Unter Server 2008 gibt es allerdings den sogenannten *Storage Server*. Dieser kann iSCSI-Targets auch für die ESXi Server zur Verfügung stellen – doch möchte man das wirklich? Um damit einen einigermaßen reibungslosen Zugriff zu bekommen, muss man den *User Name Mapping Service* von Microsoft installieren, damit keine Fehlermeldungen wie in Abbildung 7-1 die Logs vollschreiben.

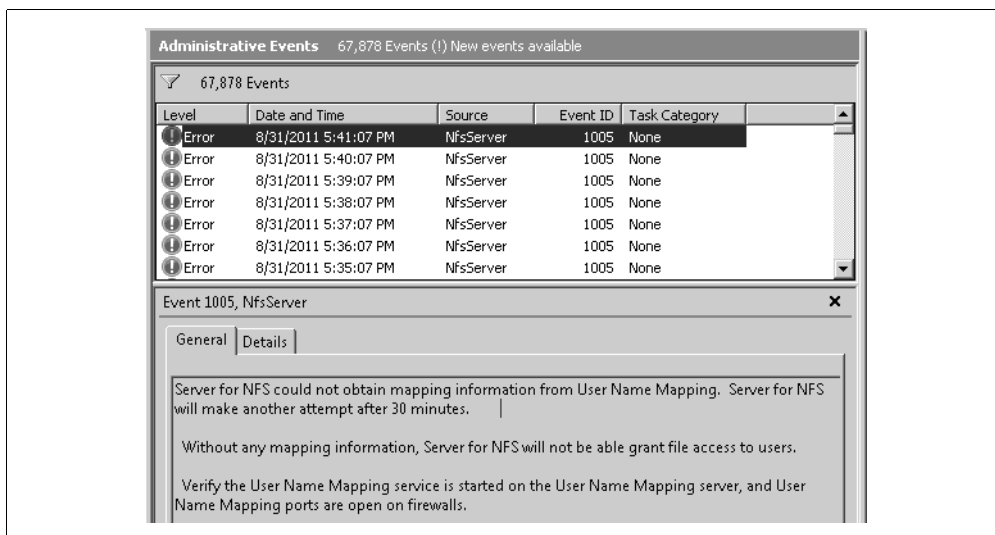


Abbildung 7-1: Fehlermeldungen in Logdateien unter Server 2008

Weiterhin möchte ein Windows-Server ständig aktualisiert werden und Patches sowie Updates bekommen. Dafür muss man den Server neu starten, was bedeutet, dass alle darauf liegenden VMs und alle ESXi Server heruntergefahren sein müssen – wollen Sie das? Das Schlimme ist, dass einige Storage-Hersteller solche Konfigurationen anbieten, ohne darauf hinzuweisen, dass es sich um Microsoft-Betriebssysteme handelt.

Auf Linux basierende Storages brauchen keine Aktivierung, keine Updates oder Service-Packs und auch weder Firewall noch Antivirensoftware. Ein Beispiel für die Einrichtung finden Sie am Ende dieses Kapitels.

Bei iSCSI werden also SCSI-Datenpakete in einen Ethernet-Frame gepackt und an den Empfänger geleitet. Vom Empfänger werden die Netzwerkinformationen entfernt und die eigentlichen Datenpakete an den Storage geliefert. Auf dem ESXi Server erledigt das eine VMkernel-Schnittstelle in Zusammenarbeit mit einem iSCSI-Softwareadapter oder auch ein iSCSI-Hardwareadapter.



In ESXi steht softwareinitiiertes iSCSI auch über 10-GBit-Ethernet-Adapter zur Verfügung. Sie können aber auch das Netzwerkteaming mit bis zu acht 1-GBit-Adaptern dafür nutzen.

iSCSI-Konfiguration unter Windows

Trotz der oben aufgeführten Bedenken kann ein iSCSI-Speicher unter Windows für kleine Umgebungen oder Tests recht einfach und kostengünstig eingerichtet werden. Wenn Sie Ihr Storage in einem Subnetz platzieren, das sonst nicht genutzt wird oder keine Verbindung ins Internet hat, entfallen auch die meisten der oben genannten Bedenken.

Gerade Benutzer von Windows haben oft erhebliche Berührungängste mit Linux. Deshalb kommt nun zunächst ein Beispiel mit iSCSI Targets unter Windows und später folgt dann eines für Linux.

Als beispielhafte Konfiguration für einen iSCSI-Speicher für mehrere ESXi Server schildere ich den genauen Ablauf unter Windows (64 Bit empfohlen) mit der kostenlosen Software *StarWind* von Rocket Division. Auf der Internetseite <http://www.starwindsoftware.com> können Sie sich nach einer kurzen Registrierung das Programm herunterladen und bekommen einen Lizenzschlüssel für einen Host sowie eine ausführbare Datei zum Download. Diese kostenlose Version hat keine Beschränkung bezüglich der Größe oder Anzahl der Volumes, und die maximale Anzahl gleichzeitiger Verbindungen und Netzwerkarten ist ebenfalls unbeschränkt. Zu Testzwecken können Sie sogar einen deduplizierten Speicher erstellen. Auf der Website zum Buch finden Sie die aktuelle Beschreibung der Software zur Einrichtung als PDF-Datei der Firma Rocket Division.

Voraussetzungen

Was brauchen wir nun als Mindestvoraussetzung für den Storage? Da wäre zunächst ein Windows-Rechner mit freiem Plattenplatz zu nennen. Als Betriebssystem sollten Sie ein aktuelles Windows mit 64 Bit einsetzen, das ist aber nicht zwingend notwendig. Vista braucht allein schon zu viel Ressourcen und lässt sich nicht so gut konfigurieren. Bei XP und Server 2003 müssen Sie noch den iSCSI Initiator von Microsoft installieren. Den bekommen Sie unter <http://www.microsoft.com/download/en/details.aspx?id=18986> (Dateigröße 2,3 MByte). Bei der freien Variante können Sie keine ganze Festplatte zur Verfügung stellen, sondern nur eine Imagedatei auf einem bereits formatierten Datenträger. Möchten Sie mehr Durchsatz erreichen, ist es hilfreich, die 64-Bit-Version des Betriebssystems mit viel RAM und mehrere 1 GBit- oder 10 GBit-Netzwerkadapter zu nutzen. Weiterhin kann ein RAID nicht schaden, um größere Datenmengen zu liefern.



Um die Konfiguration und den Anschluss der ESXi Server zu testen, können Sie auch eine virtuelle Maschine nutzen.

Auf der ESXi-Seite brauchen wir mindestens eine Netzwerkkarte für den VMkernel und müssen den Software-iSCSI-Adapter konfigurieren. Beachten Sie bei diesem Beispiel auch die Schilderungen oben für die Einrichtung von Jumbo-Frames und Teaming.



Sie können natürlich auch mehrere VMkernel-Portgruppen auf unterschiedlichen vSwitches erstellen, müssen dann aber auch unterschiedliche Subnetze nehmen, da es sonst zu bösen Überraschungen kommen kann. Konfigurieren Sie mehrere Portgruppen für iSCSI auf einem vSwitch, müssen Sie die Adapter-Teaming-Einstellungen auf Portebene in aktive und passive *vmnics* aufteilen.

Installation auf der Windows-Seite: Starten Sie die Software, die Sie sich von der Internetseite heruntergeladen haben, und akzeptieren Sie die Lizenzvereinbarung. Suchen Sie sich den Installationspfad aus und wählen Sie anschließend FULL INSTALLATION. Lassen Sie sich bei Bedarf eine Verknüpfung im Startmenü und auf dem Desktop erstellen und klicken Sie auf NEXT. Nach kurzer Zeit ist die Installation erledigt, und Sie können die Software gleich vom Assistenten starten lassen: LAUNCH STARWIND. Klicken Sie auf FINISH. Neben der Uhr befindet sich jetzt ein neues Icon, das anzeigt, dass die StarWind-Software läuft.

Konfiguration auf der Windows-Seite. Über das Icon im Tray oder auf dem Desktop können Sie die Managementkonsole starten und die Konfiguration beginnen.

Im Menü klicken Sie auf OPTIONS → LANGUAGE und stellen Deutsch als Sprache ein.

1. Als Erstes müssen Sie den lokalen Rechner zum Management hinzufügen. Das können Sie über den Link auf dieser Seite oder über das Menü HOST erledigen.
2. Im folgenden Fenster wird der lokale Host über die IP-Adresse 127.0.0.1 angezeigt (siehe Abbildung 7-2). Das bedeutet, dass alle vorhandenen Netzwerkadapter für iSCSI eingerichtet werden. Über ERWEITERT → AUTHENTIFIZIERUNG können Sie auch CHAP für die sichere Kommunikation benutzen. Ich empfehle aber, das erst nach erfolgreicher Einrichtung abzuändern, damit man eventuell auftauchende Fehler schneller eingrenzen kann.

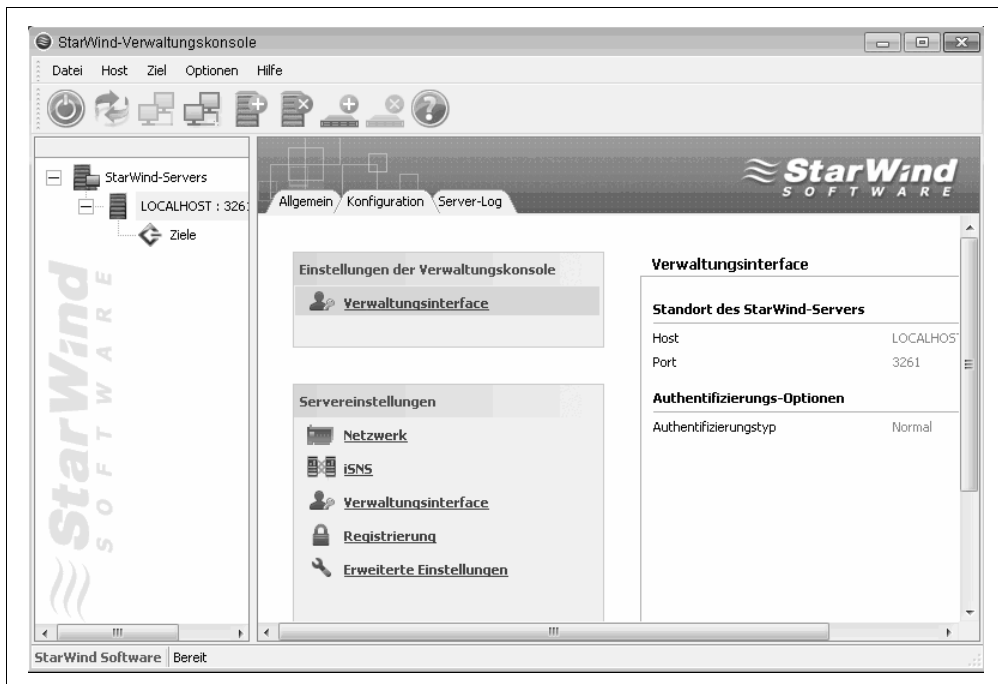


Abbildung 7-2: Starwind-Verwaltungskonsolle

3. Als Nächstes müssen Sie sich mit dem eingerichteten Server *Localhost* verbinden. Für die Standardanmeldedaten verwenden Sie als Username *root* und als Passwort *starwind*.
4. Klicken Sie anschließend auf der linken Seite des Fensters auf Ihren Server und in der rechten Hälfte auf KONFIGURATION, um die Registrierung mit der Lizenzdatei durchzuführen, die Sie per Mail bekommen haben.
5. Jetzt können Sie eine neue Imagedatei erstellen, die den ESXi Servern dann über den Port 3260 auf allen lokalen Netzwerkkarten zur Verfügung stehen wird. Klicken Sie dazu mit der rechten Maustaste auf ZIELE und wählen Sie ZIEL HINZUFÜGEN aus.
6. Geben Sie eine Zeichenkette als ALIAS für das Image an und wählen Sie im nächsten Fenster FESTPLATTE aus. In der freien Version ist es nicht möglich, eine ganze Festplatte zur Verfügung zu stellen, sondern nur eine Datei auf einem formatierten Datenträger. Auch die Optionen OPTISCHES LAUFWERK und BANDLAUFWERK erlauben nur virtuelle Geräte.
7. Wählen Sie im nächsten Fenster IMAGE-LAUFWERK aus (siehe Abbildung 7-3) und klicken Sie auf WEITER.



Abbildung 7-3: Image-Laufwerk erstellen

8. Im folgenden Fenster nehmen Sie die mittlere Option NEUES VIRTUELLES LAUFWERK ANLEGEN und klicken auf WEITER.
9. Über die Schaltfläche mit den drei Punkten können Sie nun auf Ihren Rechner browsen und einen Namen für die Datei eingeben.
10. Als Nächstes müssen Sie die OPTIONEN DES IMAGE-LAUFWERKS einstellen (siehe Abbildung 7-4). Achten Sie darauf, dass Sie das Häkchen bei MEHRERE GLEICHZEITIGE ISCSI-VERBINDUNGEN ZULASSEN (CLUSTERBILDUNG) setzen, sonst kann statt der bei dieser Version möglichen vier beteiligten ESXi Server immer nur einer auf das Image zugreifen.

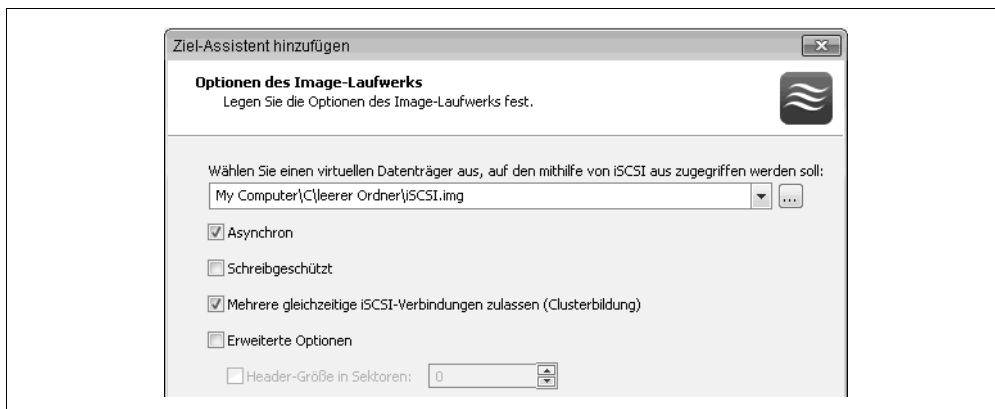


Abbildung 7-4: Optionen des Laufwerks

11. In den beiden nächsten Fenstern brauchen Sie nichts einzustellen, können aber gegebenenfalls das *write-through caching* ausprobieren – auf manchen Rechnern bringt es noch ein bisschen mehr Durchsatz. Nachträglich lässt sich dieser Punkt übrigens nur ändern, indem man das Image entfernt und neu hinzufügt. Die Daten bleiben dabei erhalten.

Auf der Windows-Seite sind wir damit so weit fertig. Lediglich die Einstellungen zu Ihrer Firewall sollten Sie überprüfen und gegebenenfalls die installierte Software zu den Ausnahmen hinzufügen bzw. den Port freigeben.

Konfiguration auf der ESXi-Seite

Überprüfen Sie zunächst, ob Ihr ESXi Server bereits einen Software-iSCSI-Adapter hat:

1. Melden Sie sich mit vSphere Client an einen Host an und klicken Sie im BESTANDSLISTENFENSTER auf den ESXi Server.
2. Klicken Sie auf die Registerkarte KONFIGURATION und anschließend auf SPEICHERADAPTER.
3. Klicken Sie auf den Link HINZUFÜGEN.
4. Wählen Sie SOFTWARE-ISCASI-ADAPTER HINZUFÜGEN aus (siehe Abbildung 7-5) und klicken Sie auf OK. Auf der Seite SPEICHERADAPTER erscheint der neue, softwarebasierte Adapter.

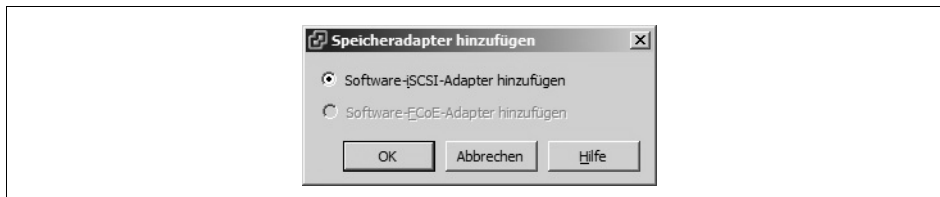


Abbildung 7-5: Software-iSCSI-Adapter hinzufügen

Wie schon erwähnt, brauchen Sie einen VMkernel-Port für die Datenübertragung, den Sie wie folgt einrichten:

1. Melden Sie sich mit vSphere Client an einem Host an (falls noch nicht geschehen) und klicken Sie im BESTANDSLISTENFENSTER auf den ESXi Server.
2. Klicken Sie auf die Registerkarte KONFIGURATION und anschließend auf NETZWERK.
3. Klicken Sie auf den Link NETZWERK HINZUFÜGEN.
4. Wählen Sie VMKERNEL aus und klicken Sie auf WEITER. Auf der Seite NETZWERKZUGRIFF können Sie den VMkernel an das physische Netzwerk anschließen.
5. Wählen Sie den vSwitch aus, den Sie verwenden möchten (siehe Abbildung 7-6) oder klicken Sie auf EINEN VIRTUELLEN SWITCH ERSTELLEN.

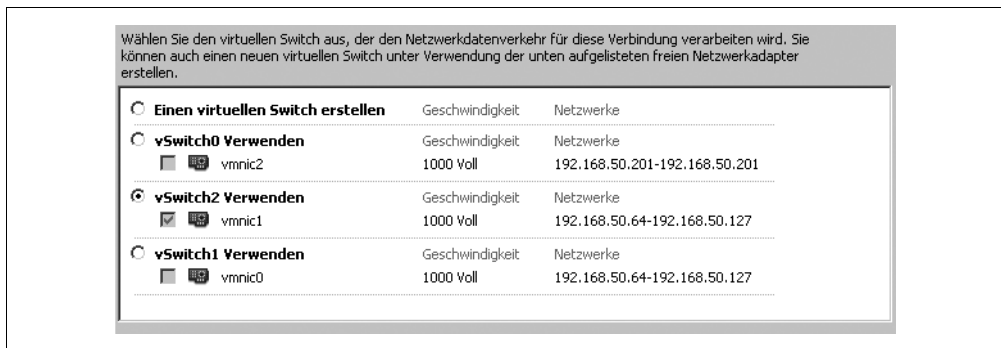


Abbildung 7-6: Netzwerkkonfiguration für iSCSI



Wenn unter EINEN VIRTUELLEN SWITCH ERSTELLEN keine Adapter angezeigt werden, bedeutet das, dass alle Adapter von vorhandenen vSwitches verwendet werden. Die Auswahlmöglichkeiten werden im Bereich VORSCHAU angezeigt.



Verwenden Sie iSCSI aus Gründen der Performance nicht bei Netzwerkadaptern mit 100 MBit/s oder weniger. Adapter mit 10 GBit/s werden mittlerweile unterstützt.

6. Klicken Sie auf WEITER.
7. Wählen Sie unter PORTGRUPPENEIGENSCHAFTEN eine Netzwerkbezeichnung und optional eine VLAN-ID aus bzw. geben Sie diese ein. Klicken Sie auf WEITER.
8. Geben Sie eine noch nicht vergabene IP-Adresse und eine Subnetzmaske ein (empfohlen) oder lassen Sie sie automatisch vom DHCP-Server abrufen. Klicken Sie unter IP-EINSTELLUNGEN auf BEARBEITEN, um das optionale Standardgateway des VMkernel für iSCSI anzugeben. Das Management Network und der VMkernel-Port besitzt

zen leider immer dasselbe Gateway. Ändern Sie es besser nicht, denn der iSCSI-Zugriff benötigt kein eigenes Gateway.

9. Klicken Sie auf OK und dann auf WEITER.
10. Klicken Sie gegebenenfalls auf ZURÜCK, um Änderungen vorzunehmen.
11. Überprüfen Sie die Änderungen im Dialogfeld BEREIT ZUM ABSCHLIEßEN und klicken Sie auf BEENDEN.

Nun geht es an die Software-iSCSI-Schnittstelle.

1. Klicken Sie unter HARDWARE auf derselben Seite auf SPEICHERADAPTER.
2. Wählen Sie auf der rechten oberen Seite iSCSI-SOFTWAREADAPTER aus und anschließend im unteren Teil des Fensters auf den Link EIGENSCHAFTEN.
3. Im neuen Fenster klicken Sie auf der Registerkarte ALLGEMEIN zunächst auf die Schaltfläche KONFIGURIEREN.
4. Setzen Sie bei STATUS das Häkchen bei AKTIVIERT und klicken Sie dann auf OK.



iSCSI-Namen und -Alias brauchen Sie nicht einzugeben, da das automatisch geschieht, nachdem Sie auf OK geklickt haben. Wenn Sie aber bereits feste Namen bei Ihrem Storage eingetragen haben, können Sie hier anschließend diese Namen auch manuell eintragen. Üblicherweise fängt der Name, den sich der ESXi Server nimmt, mit *iqn.1998-01.com.vmware:* an. Dann folgen der Kurzname des Rechners und anschließend eine ID – komplett also z. B. *iqn.1998-01.com.vmware:esx1-0cb64f32*.



iSCSI-Namen fangen entweder mit *iqn* oder *eui* an. *iqn* steht dabei für »iSCSI Qualified Name«. Anschließend folgt das Jahr und der Monat, an dem die Registrierung des Domännennamens stattfand, bei VMware also Januar 1998, und die registrierte Domäne ist *vmware.com*, wieder in umgekehrter Reihenfolge. *eui*, die andere Möglichkeit, steht für »Extended Unique Identifier«. Diese wird von der IEEE vergeben und sieht z. B. so aus: *eui.0102ba03ce04cdef*. Dabei wird der Registrierungsname – ähnlich wie bei einer MAC-Adresse – verschlüsselt hinterlegt.

5. Eventuell müssen Sie auf der Registerkarte NETZWERKKONFIGURATION noch die gerade erstellte iSCSI-Portgruppe auswählen. Betätigen Sie dazu die Schaltfläche HINZUFÜGEN und wählen Sie die Portgruppe und anschließend OK.
6. Auf der Registerkarte DYNAMISCHE ERKENNUNG tragen Sie nun die statische IP-Adresse des konfigurierten Windows-Rechners ein. Haben Sie mehrere Netzwerkkarten auf dem iSCSI-Target-PC, können Sie diese z. B. unter den ESXi Servern aufteilen. Klicken Sie auf OK. Nach einer kurzen Zeit sollte der Eintrag im Fenster sichtbar werden.
7. Klicken Sie anschließend auf die Schaltfläche SCHLIEßEN.

- Sie werden aufgefordert, den iSCSI-Host-Bus-Adapter erneut prüfen zu lassen (siehe Abbildung 7-7). Das ist notwendig, damit eine Verbindung zum iSCSI-Target aufgebaut werden kann. Klicken Sie auf JA.

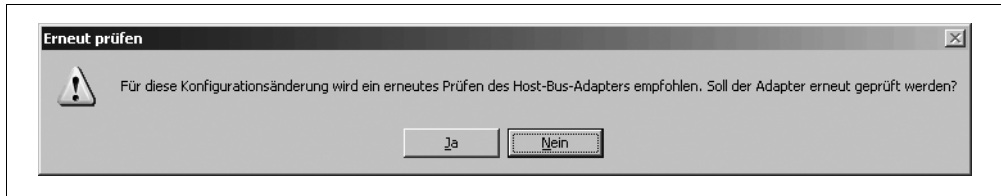


Abbildung 7-7: Prüfen der Verbindung bestätigen

- Wenn Sie im oberen Teil des Fensters den Fokus auf den iSCSI-Adapter setzen, sollten Sie im unteren Teil bei DETAILS die oder den eingerichteten Netzwerkspeicher sehen können (siehe Abbildung 7-8).

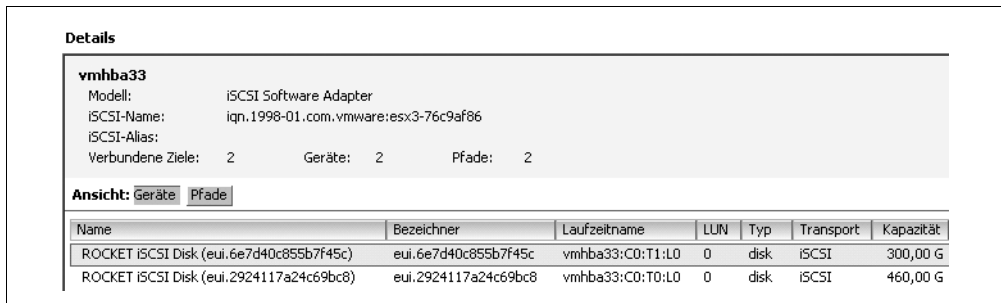


Abbildung 7-8: iSCSI-Ziele werden angezeigt.

- Überprüfen Sie anschließend, ob die dafür vorgesehene Portgruppe das Häkchen bei iSCSI-PORT-BINDUNG hat, indem Sie nochmals in die Eigenschaften des vSwitch gehen und die Portgruppe für iSCSI anklicken. Auf der rechten Seite müsste dann AKTIVIERT stehen. Überlegen Sie sich, ob Sie die MTU bei dieser Portgruppe auf 9000 setzen wollen und können. Bedenken Sie, dass alle beteiligten Geräte zwischen Sender und Empfänger diese Jumbo-Frames unterstützen müssen. Das Datenpaket bei normalen Frames ist 1.500 Bytes groß und sein Header fasst 76 Bytes. Bei Jumbo-Frames sind es ebenfalls 76 Bytes für die Informationen, aber der Rest sind reine Daten.

Damit haben Sie erst den vorletzten Schritt erledigt, denn das Volume (bzw. die Volumes) muss erst noch mit dem VMFS-Dateisystem formatiert werden, damit dort virtuelle Maschinen erstellt werden können.

iSCSI-Datenspeicher hinzufügen

Wenn die Konnektivität zwischen den ESXi Servern und dem iSCSI-Target hergestellt ist und das Volume unter dem iSCSI-Softwareinitiator angezeigt wird, muss es trotzdem noch zum ESXi Server hinzugefügt und bei einem ESXi Server formatiert werden.

1. Klicken Sie unter **HARDWARE** auf derselben Seite auf **SPEICHER**.
2. Wählen Sie rechts oben den Link **SPEICHER HINZUFÜGEN** aus.
3. Im folgenden Fenster klicken Sie **FESTPLATTE/LUN** an (siehe Abbildung 7-9) und dann auf **WEITER**.

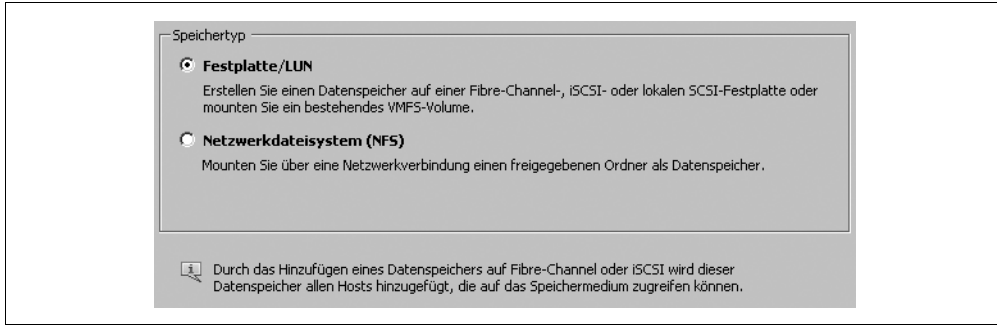


Abbildung 7-9: Speichertyp festlegen

4. Im nächsten Fenster sollten Sie das Volume sehen, das Sie zur Verfügung gestellt haben. Wählen Sie es aus und klicken Sie auf **WEITER**.
5. Überprüfen Sie das Festplattenlayout und klicken Sie auf **WEITER**.
6. Geben Sie einen Namen für den Datenträger ein. Das kann ein beliebiger noch nicht vergebenen Name sein, da es sich nur um einen Alias handelt.
7. Klicken Sie auf **WEITER** und dann auf **BEENDEN**.

Kurze Zeit später sollte der neue Datenträger in Ihrer Liste auftauchen.



Beim zweiten und allen weiteren ESXi Servern sollten Sie beim Hinzufügen der Festplatte nicht dazu aufgefordert werden, einen Aliasnamen einzugeben oder das Volume zu formatieren. Wenn das dennoch geschieht, brechen Sie den Vorgang ab, warten einen Moment, bis der erste ESXi Server mit dem Formatieren fertig ist, und wiederholen den Vorgang.

Probleme bei Software-iSCSI

ESX Server 3.x und neuer unterstützen die iSCSI-Technologie, die es dem Hostsystem ermöglicht, beim Zugriff auf entfernten Speicher ein IP-Netzwerk zu verwenden. Bei iSCSI werden die SCSI-Speicherbefehle, die die virtuelle Maschine an ihre virtuelle Festplatte ausgibt, in TCP/IP-Protokollpakete umgewandelt und an ein entferntes Gerät – das Ziel – übertragen, auf dem die virtuelle Festplatte gespeichert ist. Aus Sicht der virtuellen Maschine erscheint das Gerät als lokal angeschlossenes SCSI-Laufwerk.

Auf der Registerkarte **ROUTING** über den vSphere Client sind das Management Network und der VMkernel oft nicht an dasselbe Subnetz angeschlossen. Für iSCSI braucht der VMkernel-Port kein Gateway. Ein Gateway ist zur Anbindung an Computer notwendig,

die sich nicht im selben IP-Subnetz wie das Management Network befinden. Speicherzugriffe dürfen nicht geroutet werden.

Alle NAS- und iSCSI-Server müssen deshalb über dasselbe Übertragungsgebiet (Subnetz) wie die zugeordneten vSwitches zu erreichen sein.

Zum Zugriff auf entfernte Ziele verwendet der ESXi Server-Host iSCSI-Initiatoren. Die Initiatoren transportieren hardwarebasierte und softwarebasierte SCSI-Anfragen und -Antworten zwischen dem ESXi Server-System und dem Zielspeichergerät über das IP-Netzwerk, deshalb müssen diese Einstellungen korrekt eingestellt werden. Auch der vCenter Server muss über den oder die ESXi Server auf das Target zugreifen können!

Im ersten Beispiel der iSCSI-Speicherkonfiguration in Abbildung 7-10 verwendet das ESXi Server-System einen Hardware-iSCSI-Adapter. Dieser spezielle Adapter sendet iSCSI-Pakete über ein LAN an eine Festplatte.

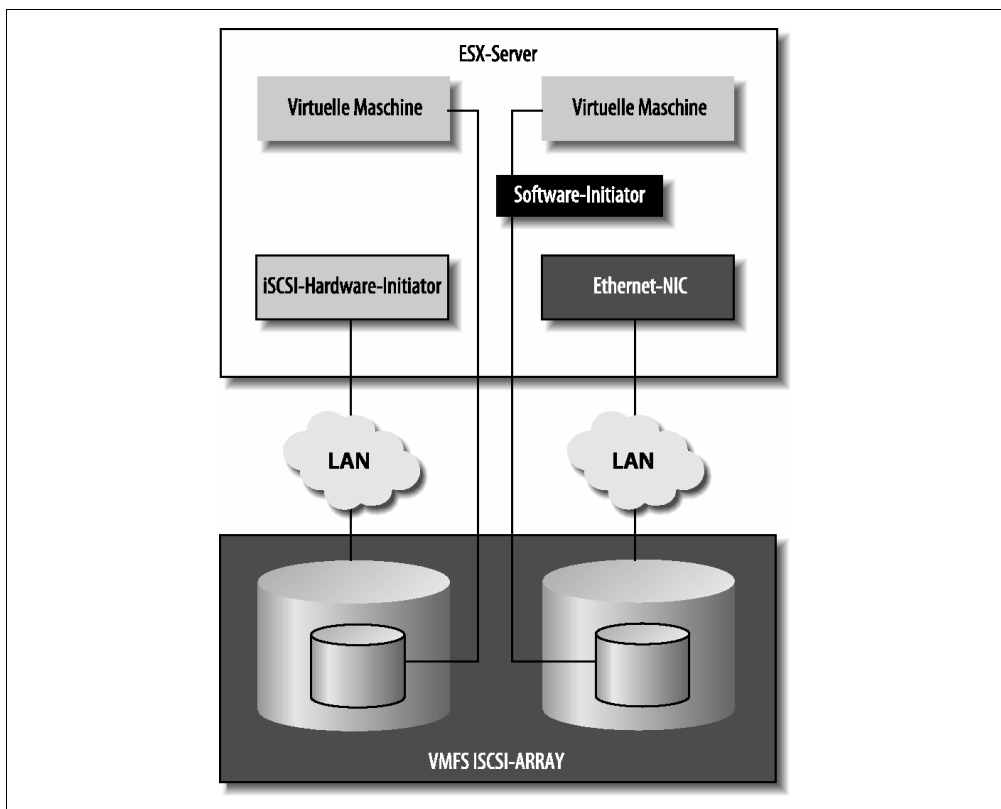


Abbildung 7-10: Varianten des iSCSI-Zugriffs

Im zweiten Beispiel verfügt das ESXi Server-System über einen Software-iSCSI-Initiator. Unter Verwendung des Software-Initiators stellt das ESXi Server-System die Verbindung zu einem LAN über eine vorhandene Netzwerkkarte her.

Steht eine neue LUN über einen Adapter neu zur Verfügung, registriert der ESXi Server dieses neue virtuelle Gerät zur Verwendung durch die virtuellen Maschinen.



Achten Sie bei der Zuweisung der Datenspeicher auf die fortlaufende Nummerierung der LUNs (Logical Unit Numbers). Der ESXi Server sollte keine LUN-Nummer pro Gerät doppelt sehen.

Wenn eine bestehende LUN nicht mehr verwendet wird und nicht mehr da zu sein scheint, wird sie von der Liste der für die virtuellen Maschinen zur Verfügung stehenden Geräte entfernt.

Ein erneuter Scan wird in folgenden Fällen empfohlen:

- Wenn Änderungen an den Speicherfestplatten oder LUNs vorgenommen wurden, die dem ESXi Server zur Verfügung stehen.
- Wenn Änderungen an den Speicheradaptern vorgenommen wurden.
- Wenn neue Datastores erstellt wurden.
- Wenn bestehende Datastores bearbeitet oder entfernt wurden.

Überprüfen Sie auf der Kommandozeile des ESXi Servers mit dem Befehl `vmkping`, ob sich der VMkernel-TCP/IP-Stack meldet. Er wird genau so wie der normale `ping`-Befehl benutzt. Antwortet dieser, aber nicht das Management Network, kann ein Hardware-netzwerkproblem bestehen. Versuchen Sie es auch mit einem `ping`-Befehl auf den iSCSI-Anschluss und untersuchen Sie gegebenenfalls die Firewall-Einstellungen des Targets.

iSCSI-Pfade überprüfen

Ich rate Ihnen dringend dazu, sich die Pfade zu den Volumes nochmals genauer anzusehen, wenn das iSCSI-Storage fertig eingerichtet und in der Liste der Datenspeicher aller ESXi Server aufgelistet ist. In der Praxis hat sich herausgestellt, dass die eingetragenen IP-Adressen, die beim Host angegeben werden, von VMware ignoriert werden.

Dazu ein Beispiel: In einer Umgebung für zwei ESXi Server, die später auf vier Hosts ausgebaut werden sollte, wurde ein Storage mit vier Mal 1-GBit-Ethernet Anschlüssen angeschafft. Der VMkernel-iSCSI-Port wurde auf den ESXi Servern mit den IP-Adressen 192.168.50.15 und 16 eingerichtet. Der Storage bekam die Adressen 192.168.50.201 bis 204, es wurden aber nur die Karten mit der 201 und der 202 mit dem Netzwerk verbunden.

Nach der Konfiguration des iSCSI-Adapters auf den Hosts schien alles in Ordnung – nur die Performance war nicht wie erwartet. Das Dilemma wurde deutlich, wenn man mit rechts auf das erste Volume klickte, dann EIGENSCHAFTEN auswählte und anschließend auf den Button PFADE VERWALTEN klickte: Beide Hosts benutzten für beide Volumes als bevorzugten Pfad die nicht angeschlossene IP-Adresse 192.168.50.204, wie in Abbildung 7-11 zu sehen ist.

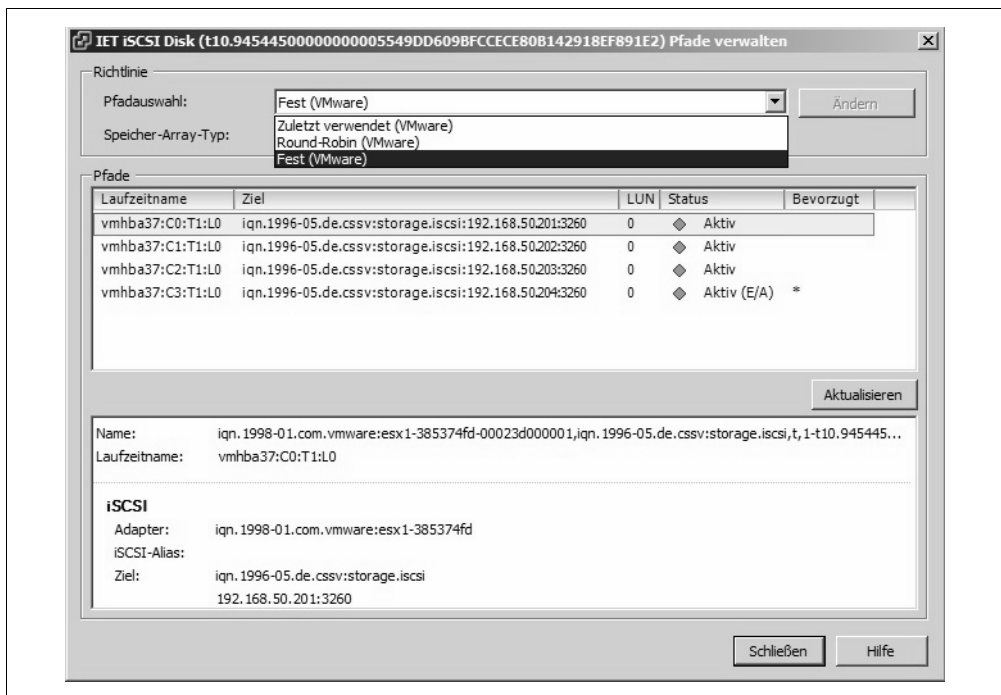


Abbildung 7-11: iSCSI Pfade verwalten

Um ein derartiges Problem zu beheben, klicken Sie mit der rechten Maustaste auf den Eintrag mit der richtigen IP und wählen aus dem Kontextmenü BEVORZUGT aus. Wiederholen Sie das für jedes Volume und jeden ESXi Server, der auf einen iSCSI-Storage zugreift.

NFS-Speicher anschließen

In mittelständischen und größeren Unternehmen findet man zwar fast ausschließlich Fibre Channel- oder iSCSI-Speicher, aber es gibt einige interessante Möglichkeiten bei NFS-Zugriffen (*Network File System*), die ich hier nicht unerwähnt lassen möchte – zumal der Zugriff auf Seiten des ESXi Servers noch einfacher geht, als ich es bei iSCSI geschildert habe.

Grundsätzlich kann jeder ESXi Server über das NFS-Protokoll Version 3 auf im Netzwerk verfügbaren Speicher zugreifen. Dafür benötigen wir wie bei Software-iSCSI für jeden beteiligten ESXi Host eine VMkernel-Portgruppe. Ob Sie diese auf einem schon bestehenden Switch oder einem neuen anlegen, spielt nur für die zu erwartende Übertragungsgeschwindigkeit eine Rolle. Da ich die Vorgehensweise zum Erstellen einer VMkernel-Portgruppe oben schon ausgiebig beschrieben habe, gehe ich hier nur auf die Besonderheiten ein:

- Achten Sie beim Erstellen der VMkernel-Portgruppe auf den Namen. Dieser sollte bei allen beteiligten ESXi Servern gleich sein.
- vMotion und NFS-Datenverkehr sollten nicht über dieselbe Portgruppe bzw. denselben Adapter gehen.
- Legen Sie die Portgruppe mit Jumbo-Frames an, wenn es möglich ist.



Wenn Sie auf NFS-Storages zugreifen wollen, macht eine MTU von 9.000 einiges an Performance aus. Auch der vSwitch, an den der VMkernel angeschlossen ist, muss für Jumbo-Frames eingerichtet sein, und natürlich auch alle physischen Switches und gegebenenfalls Router sowie die Schnittstelle des Storage bzw. der Gegenseite.

Haben Sie so weit alles erledigt, geht es an das Hinzufügen des im Netzwerk zur Verfügung stehenden Speicherplatzes. Dafür gehen Sie beim ESXi Server auf die Registerkarte KONFIGURATION und wählen im Abschnitt HARDWARE den SPEICHER (STORAGE) aus. Klicken Sie oben rechts auf den blauen Link SPEICHER HINZUFÜGEN. Auf die Frage »Welcher Typ Speicher darf's denn sein?« wählen Sie den unteren Punkt NETZWERKDATEISYSTEM (NFS) aus.

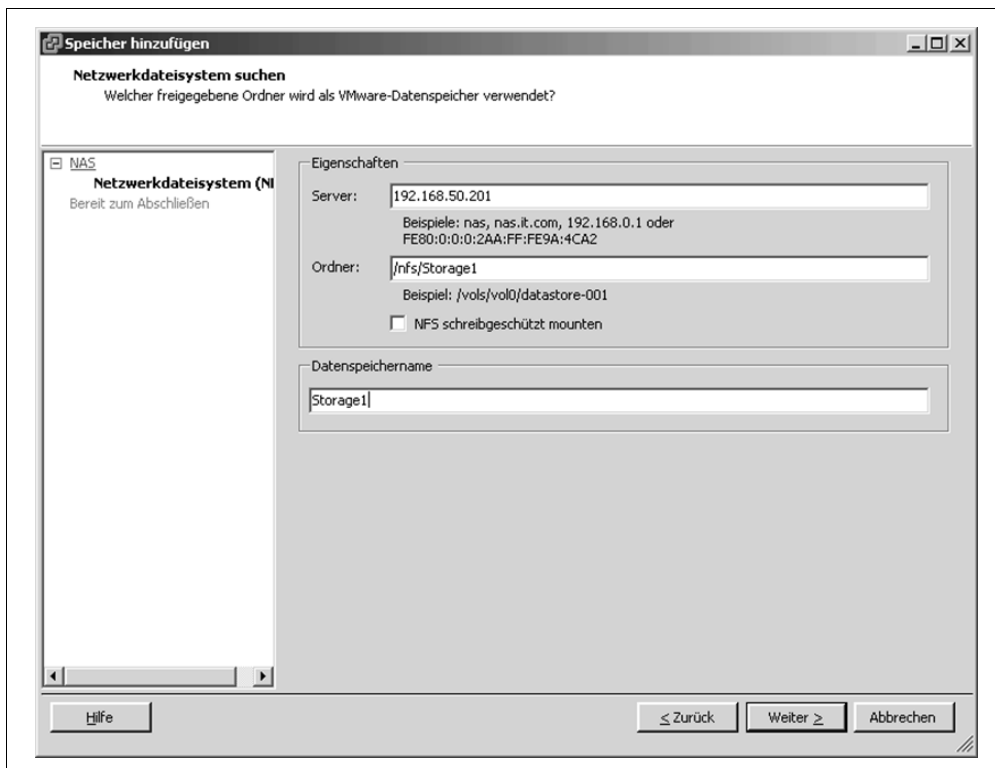


Abbildung 7-12: NFS-Speicher hinzufügen

Im nächsten Fenster NETZWERKDATEISYSTEM SUCHEN (siehe Abbildung 7-12) geben Sie die relevanten Daten ein. Achten Sie bitte darauf, dass der Datenspeichername eindeutig ist und auch bei den anderen ESXi Servern exakt so eingetragen wird, sonst gibt es später gegebenenfalls Fehler bei vMotion und Storage vMotion.

NFS-Speicher auf der Kommandozeile anlegen

Auf der Kommandozeile des ESXi Servers gibt es den VMware-Befehl `esxcfg-nas`, um einen NFS-Storage anzuschließen. Über den Parameter `--h` bekommen Sie die Syntax und die möglichen Optionen für diesen Befehl angezeigt:

- ```
esxcfg-nas <options> [<label>]
```
- a|--add  
Ein neues NFS-Dateisystem zum Mountpoint */vmfs/volumes* hinzufügen. Die Parameter `--host` und `--share` müssen mit angegeben werden. Zusätzlich können Sie die Option `--readonly` für den Nur-lesen-Modus angeben.
  - o|--host <host>  
Angabe des Namens oder der IP-Adresse des Servers, auf dem der NFS-Speicher liegt
  - s|--share <share>  
Name der Freigabe auf dem entfernten Server
  - y|--readonly  
Den Speicher im Nur-lesen-Modus anfügen
  - d|--delete  
Abhängen und Löschen des angehängten Dateisystems
  - l|--list  
Auflisten der gerade angeschlossenen NFS-Dateisysteme
  - r|--restore  
Alle in der Konfigurationsdatei aufgeführten NAS/NFS-Dateisysteme erneut anschließen
  - h|--help  
Diese Hilfe anzeigen

Die Ausgabe des Befehls `esxcfg-nas -l` (kleines L) zeigt beispielsweise den folgenden Eintrag:

```
Storage1 is /nfs/Storage1 from 192.168.50.201 mounted
```

Um einen neuen Speicher in das System über die Kommandozeile einzubinden, können Sie entsprechend folgenden Befehl angeben:

```
esxcfg-nas -a -o 192.168.50.202 -s /nfs2 Storage2
```

### Vorteile des NFS-Speichers

Sie können NFS-Speicher nicht mit dem VMFS-Dateisystem formatieren. Der ESXi Server greift also auf das vorhandene Dateisystem zu, das *ext3*, *ext4*, *ntfs*, *zfs* oder irgende-

was anderes sein kann. Aus Sicht des ESXi Servers erscheint dieses wie ein lokaler Storage, der bereits formatiert ist (und das ist er ja auch). Dieser Umstand macht auch den Vorteil dieses Speichers aus:

- Sie können mit Ihrem Hostsystem, auf dem sich die Freigabe befindet, auf die Dateien direkt zugreifen.
- Auch für eine Datensicherung ergeben sich damit ganz neue Aspekte.
- Virtuelle Maschinen können so aufgesetzt werden, dass sie auf dem ESXi Server virtuell laufen oder vom selben NFS-Storage als physische Maschine booten.
- Das Vergrößern und Verkleinern der Netzwerkfreigabe ist deutlich einfacher als bei anderen Verfahren. Beim ESXi Server müssen Sie lediglich die Ansicht aktualisieren.

## Fibre-Channel-Storage

Bei mittleren bis großen Unternehmen findet man vor allem diese Lösung eines gemeinsamen Storage für die ESXi Hosts. Für die Realisierung so eines gemeinsamen Plattenplatzes bedarf es spezieller Fibre-Channel-Adapter (HBA, Host Bus Adapter) für die Hosts, entsprechender Anschlüsse am Storage und spezieller Kabel – meist aus Glasfaser. Um das Ganze redundant, also ausfallsicher zu realisieren, sollte man besser zwei Adapter pro Host nehmen und diese an zwei unabhängige Hubs oder Switches anschließen, die wiederum über mindestens zwei Leitungen mit einem ausfallsicheren SAN-Speicher verbunden sind. Dabei spricht man dann von einer »Fibre Channel Fabric mit Multipathing«, also mehreren Pfaden zu den einzelnen Volumes oder LUNs. Pro Pfad wird eine serielle Datenübertragungsrate mit SCSI-Kommandos von bis zu 400 MByte/s erreicht. Neuere Technologien mit 16 GBit/s schaffen im Vollduplex-Modus 1,6 GByte/s. Die Glasfaserstränge können auch für eine Spiegelung von Daten über bis zu 10 km genutzt werden, und mit speziellen Kabeln können sogar Distanzen von bis zu 120 km erreicht werden.

Die Hersteller dieser Speichersysteme stellen mittlerweile nicht mehr nur Plattenplatz zur Verfügung, sondern bieten zusätzlich Redundanzen, Spiegelungen, Snapshots, Backups, deduplizierten Speicher und mehr (siehe Abbildung 7-13).

Bei der Einrichtung auf der SAN-Seite müssen meist Berechtigungen (Zoning oder LUN-Maskierung) für einzelne Hosts oder eine Gruppe davon angelegt werden. Wählen Sie auch den richtigen Speichertyp für Ihr System aus:

- *Aktiv-Aktiv* bedeutet, dass alle Pfade gleichzeitig genutzt werden
- *Aktiv-Passiv* bedeutet, dass nur eine Verbindung genutzt wird und alle anderen nur bei Ausfällen zur Verfügung stehen.
- *Asymmetrisch* (ALUA, Asymmetric Logical Unit Access) bedeutet, dass der Host die Pfade automatisch wählt. Davon können einige aktiv und andere passiv sein.

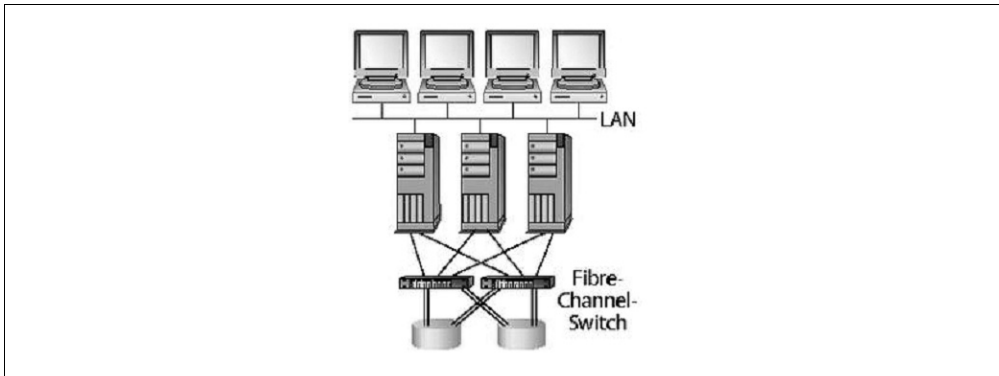


Abbildung 7-13: Redundanter SAN-Speicher

Ein Disk-Subsystem fasst seine physischen Festplatten mit RAID zu virtuellen Festplatten zusammen und bietet so den gleichen Schutz vor Plattenfehlern wie ein im Server eingebauter RAID-Controller. In modernen Disk-Subsystemen sind darüber hinaus alle weiteren Komponenten redundant ausgelegt.

Bleibt das Speichernetz selbst als »single point of failure«, kann man ein sogenanntes »Dual Fabric« einsetzen: Der Server wird über zwei getrennte I/O-Pfade mit dem Speicher verbunden. Bei einem Dual Fabric sind Fibre-Channel-Adapter, Switches und Kabel redundant ausgelegt, so dass der Datenzugriff auch bei Ausfall einer Komponente im I/O-Pfad gewährleistet ist. Durch die Redundanz der Disk-Subsysteme und die Redundanz des I/O-Pfades zu den Subsystemen sind die Daten und der Zugriff vom Host auf die Daten gut geschützt. Ist für eine Anwendung hohe Verfügbarkeit unverzichtbar, kommt man um den Einsatz einer Dual Fabric kaum herum.

Meistens bekommen Sie heutzutage ausführliche Handbücher der jeweiligen Systeme auf Papier oder einem optischen Datenträger mitgeliefert. Halten Sie sich möglichst an die dortigen Empfehlungen der Hersteller. Die Beschreibung in diesem Kapitel kann nur allgemein gehalten werden, weil sie sonst den Umfang des Buches sprengen würde.

## VSA-Storage

Eine ganz neue Technologie wurde mit der Version 5 von VMware vSphere für einen gemeinsamen Storage eingeführt: VSA (vSphere Storage Appliance). Das Besondere daran ist die gemeinsame Nutzung von lokalen Platten der beteiligten ESXi Server.

Und wie funktioniert das Ganze? Der Name »Appliance« sagt aus, dass es sich um eine vorgefertigte virtuelle Maschine handelt. Diese wird auf jedem Host (zwei oder drei) installiert bzw. als OVF-Vorlage bereitgestellt. Diese VM nimmt sich den gesamten lokalen VMFS-Speicher und teilt ihn in zwei Bereiche auf. Der sogenannte »VSA-StorageCluster« repliziert einen Bereich jeweils auf den Nachbarhost und stellt damit dem jeweils anderen Host einen gespiegelten NFS-Storage zur Verfügung. Bei einem Ausfall eines

ESXi Servers steht der gespiegelte Bereich weiterhin dem anderen Host zur Verfügung, so dass HA weiterhin funktioniert.

Um einen VSA-StorageCluster einrichten zu können wird, allerdings der vCenter Server benötigt, deshalb finden Sie die genaue Beschreibung erst in Kapitel 11.

## Storage Alignment

Eines der wichtigsten Themen im Zusammenhang mit der korrekten Konfiguration des Speichers ist das Alignment. In Kapitel 3, *Der Hypervisor* und am Anfang dieses Kapitels wurde es schon kurz erwähnt. Die zu erwartende Performance hängt unweigerlich mit der richtigen Angleichung der Abschnitte auf den zur Verfügung gestellten Speichern ab.

Worum es dabei geht? Lassen Sie mich mit einem Beispiel aus der Praxis anfangen: Eine physische Festplatte ist in logische Blöcke aufgeteilt. Diese Blöcke haben bei Laufwerken unter 2 TByte eine Größe von 512 Byte und reihen sich nacheinander bis zum Ende der Festplatte so fort. Ab 2 TByte beträgt die Blockgröße 4 KByte. Windows XP legt seine Partition ab dem Sektor 126 mit 4.096 Bytes (4 KByte) an. Damit das Betriebssystem einen Block lesen kann, muss die Festplatte bei dieser Überschneidung aber 2 Blöcke durchsuchen anstatt nur einen.

In einer virtuellen Umgebung kann es zu noch größeren Performanceeinbußen kommen, weil hier zunächst der Storage, darin das VMFS-Volume und darin wiederum die virtuelle Maschine mit NTFS-Dateisystem liegt, was in Abbildung 7-14 schematisch dargestellt ist.

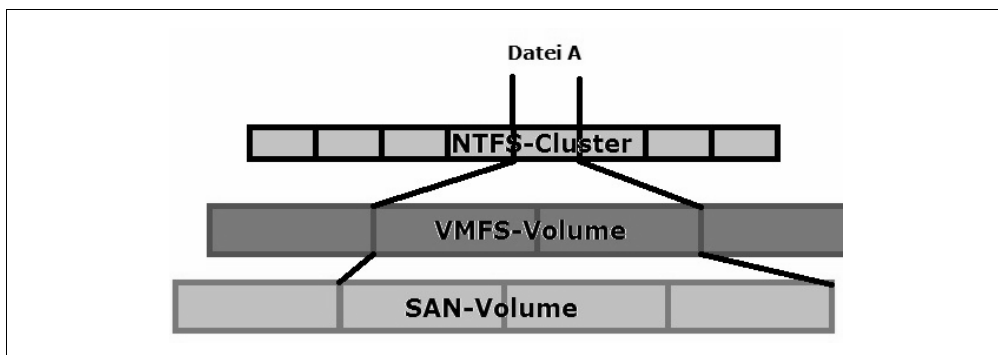


Abbildung 7-14: Storage Alignment

Die Clustergrößen von SAN- und VMFS-Volume sind hier zwar gleich groß – bei vSphere 5 immer 1 MByte –, aber die Anfänge der Blöcke stimmen nicht überein. Bei NTFS handelt es sich meist um 4-KByte-Blöcke. Um in diesem Beispiel die Datei A zu lesen, werden zwei Blöcke à 1 MByte beim VMFS-Volume benötigt, und sogar drei Blöcke auf dem Storage. Das SAN muss also dreimal mehr lesen als notwendig. Wären alle Systeme an einer

Blockgrenze ausgerichtet, bräuchte der Storage nur 1 MByte zu lesen und zu liefern. Da aber meist mehrere Blöcke hintereinander gelesen werden müssen, liegt die Performanceeinbuße insgesamt bei ca. 10–15 %.

Wie oben bereits erwähnt, werden VMFS-Volumes am besten über den vSphere Client angelegt. Dieser fängt den ersten Block bei 64 KByte an und macht die Blöcke genau 1 MByte groß. Sie sollten in der Dokumentation des Herstellers Ihres Storage nachschlagen, wie dort die Blöcke angelegt und wie sie verschoben werden können. Meistens fangen sie ebenfalls an der 64-KByte-Marke an.

Bei den virtuellen Maschinen müssen Sie sich ab Windows Vista, also auch bei Windows 7 und 2008, keine Gedanken mehr darum machen. Diese Betriebssysteme fangen bei 1.024 KByte an, also an der gleichen Grenze wie das VMFS-Volume – nur später. Bei älteren Betriebssystemen von Microsoft sieht es leider anders aus, wie oben bereits geschildert. Haben Sie eine physische Maschine über den VMware Converter importiert, brauchen Sie sich hier ebenfalls keine Gedanken zu machen, denn dieser erledigt das Alignment automatisch.

Bei allen anderen Systemen können Sie diverse Tools von Microsoft (DiskPart, wmic) oder Vizioncore/Quest Software (vOptimizer WasteFinder) nehmen, um das Alignment zu untersuchen. Legen Sie eine neue VM z. B. unter Windows Server 2003 an, können Sie ebenfalls DiskPart verwenden, um die Partitionsgröße auf 64 KByte festzulegen. Bei bereits existierenden Maschinen können Sie den VMware Converter nehmen, der sogar in der Lage ist, zu kleine Partitionen zu vergrößern oder zu große zu verkleinern. Eine andere Möglichkeit bietet Quest Software mit der nicht freien Variante vOptimizer Pro.

Wenn Sie einen älteren Server auf 2008 updaten, sollten Sie darauf achten, dass das Alignment dann ebenfalls notwendig ist. Bei Linux-Distributionen brauchen Sie sich nur um den SAN-Storage und das VMFS-Volume zu kümmern. Innerhalb des Betriebssystems ist bereits alles OK.

## Vergleich: NFS, iSCSI und Fibre Channel

Die Unterschiede zwischen den drei Möglichkeiten, einen externen Storage anzuschließen, möchte ich hier kurz erwähnen, um Ihnen die Entscheidung für eines der drei Verfahren zu erleichtern. Rein vom Preis her gesehen sind wohl NFS und iSCSI die günstigeren Verfahren, weil die Preise für Fibre Channel noch sehr hoch sind. Die Leistungsfähigkeit bezüglich der Datenübertragungsgeschwindigkeit ist durch 10-Gbit/s-Netzwerkarten bei NFS und iSCSI mittlerweile schon sehr hoch, bei Fibre Channel aber doch noch besser. Fibre Channel und iSCSI übertragen die Daten blockweise, bei NFS wird je eine Datei übertragen, was insgesamt gesehen etwas langsamer ist. NFS ist dafür am einfachsten einzurichten, gefolgt von iSCSI und schließlich Fibre Channel mit seinen komplexen Konfigurationsmöglichkeiten. Ausfallsicherer Plattenplatz für den gemeinsamen Zugriff ist bei Fibre Channel durch redundante Switches und RAIDs eigentlich schon von Grund auf gegeben. Bei iSCSI kann man das ebenfalls erreichen, wenn man

manuell die entsprechende Einrichtung vornimmt. Wie oben bereits erwähnt, kann hier sogar eine Spiegelung mit dem kostenlosen Tool DBRD unter Linux erreicht werden. NFS kann nicht so einfach redundant ausgelegt werden, aber man kann zwei Storages zur Verfügung stellen und der jeweiligen VM eine zweite Platte auf dem anderen Volume zuweisen. Innerhalb des Betriebssystems kann man diese Platten dann spiegeln – und erreicht damit fast das Gleiche.

Fälschlicherweise werden NAS und SAN immer wieder als gegensätzliche Konzepte dargestellt. Tatsächlich handelt es sich jedoch um zwei Techniken, die für unterschiedliche Anforderungen gedacht sind und sich hervorragend miteinander kombinieren lassen. Speichernetze verbinden Server und Speichergeräte auf Blockebene, der Datenaustausch erfolgt über das SCSI-Protokoll. NAS-Server dagegen arbeiten auf Dateiebene: Sie stellen ihren Nutzern die Daten mit Protokollen wie NFS, CIFS und HTTP bereit.

## Vergleich von SAN und NAS

SAN und NAS unterscheiden sich bei einigen Details. Die Unterschiede sind in Tabelle 7-1 aufgeführt.

Tabelle 7-1: Gegenüberstellung SAN und NAS

|                          | SAN                      |                          | NAS                                         |
|--------------------------|--------------------------|--------------------------|---------------------------------------------|
|                          | Fibre Channel            | iSCSI                    |                                             |
| verbindet                | Server und Speichergerät | Server und Speichergerät | Client oder Anwendungsserver und NAS-Server |
| über                     | eigenes Speichernetz     | eigenes Speichernetz     | LAN                                         |
| überträgt                | Datenblöcke              | Datenblöcke              | Dateien                                     |
| Netz                     | Fibre Channel            | TCP/IP                   | TCP/IP                                      |
| Protokoll                | FCP                      | iSCSI                    | NFS, CIFS, HTTP                             |
| integriertes Dateisystem | nein                     | nein                     | ja                                          |
| Eignung für Datenbanken  | ja                       | bedingt                  | eher nein                                   |

## Installation & Konfiguration eines Debian iSCSI-Storages

*[Die folgenden Ausführungen hat mein Freund Christian Schneider für dieses Buch geschrieben.]*

Mit iSCSI ist es möglich, das herkömmliche SCSI-Protokoll zum direkten Ansprechen von Datenträgern und für die Übermittlung der Daten über ein Netzwerk zu nutzen. Im Folgenden werden wir ein Debian-Linux-System installieren und konfigurieren und daran angebotenen Speicher mit unserem ESXi Server verbinden.



## SCSI und iSCSI

Das *Small Computer System Interface*, kurz SCSI, wurde 1979 von Alan Shugart als parallele Schnittstelle für die Anbindung von Datenträgern eingeführt. Gegenüber anderen Technologien wie ATA/SATA stach es vor allem durch die Möglichkeit hervor, mehr als zwei Geräte gleichzeitig über einen einzelnen Controller zu betreiben. Die Kommunikation bei SCSI-Verbindungen erfolgt immer mithilfe eines Controllers, des sogenannten *Initiators*, der diese Kommunikationen zwischen den einzelnen Storages steuert, den Targets.

Die Spezifikation des *Internet Small Computer System Interface*, kurz iSCSI, verfolgt die gleichen Richtlinien, die auch bei der herkömmlichen SCSI-Spezifikation bekannt sind; die Übertragung und der Betrieb der Speicherprotokolle laufen allerdings nativ über das TCP/IP-Protokoll. Die SCSI-Daten werden in TCP/IP-Paketen verpackt und über IP-Netzwerke übertragen.

## Installation eines Debian-Systems

Debian ist eine freie Linux-Distribution, die seit ihrem Erscheinen maßgeblich Wert auf Stabilität legt, wobei die Aktualität der verfügbaren Pakete stark in den Hintergrund gedrängt wird. Dieser entscheidende Faktor macht es natürlich zu einer hervorragenden Distribution vor allem von Serverbetriebssystemen, bei denen die Sicherheit ganz klar an erster Stelle stehen sollte. Ein weiterer großer Vorteil von Debian ist die hohe Verfügbarkeit auf den unterschiedlichen Rechnerarchitekturen, was es deutlich erleichtert, für ein Netzwerk mit virtuellen Maschinen eine Umgebung mit iSCSI-Festplatten zu erzeugen. Ein großer Nachteil lässt sich allerdings nicht so einfach verschweigen: Die Installation von Debian gehört nicht zu den einfachsten, wenn man sich im Dschungel der Distributionen einmal umsieht (auch wenn es sich im Laufe der Jahre sehr gebessert hat).

Mit dem Erscheinen dieses Buches liegt die Version 6.0.3 von Debian mit dem Spitznamen »Squeeze« vor, die Sie über unterschiedliche Wege beziehen können. Die einfachste und wahrscheinlich auch schnellste Möglichkeit stellt bei den heutigen Bandbreiten natürlich das Herunterladen von den verschiedenen Mirror-Servern dar. Die Webseite <http://www.debian.org/CD/http-ftp/#stable> bietet eine Übersicht über einige verfügbare Server; um unnötiger Überlastung vorzubeugen, ist es ratsam, sich einen zum Standort passenden Server auszusuchen – was auch Ihnen eventuell eine schnellere Verbindung bescheren kann.

Die Auswahl an verschiedenen Installationswegen ist groß. Sie können wählen zwischen einer minimalen Imagedatei, bei der während der Installation die restlichen benötigten Pakete geladen werden, einer kompletten DVD-Installation mit ca. 49 CDs und einer mit dem Programm Jigdo für Sie angepassten Imagedatei. Sogar eine Netzwerkinstallation ist möglich. Wir beziehen uns im Folgenden auf die Standardvariante von einer über den oben genannten Link geladenen CD.

Nachdem Sie also eine oder mehrere CDs passend für Ihre Architektur geladen (z.B. <ftp://ftp5.gwdg.de/pub/linux/debian/debian-cd/6.0.3/i386/iso-cd/debian-6.0.3-i386-netinst.iso>), gebrannt und in Ihr CD-Laufwerk eingelegt haben, passen Sie bitte Ihre BIOS-Einstellungen entsprechend an, um auch von dieser zu booten. Wenn Sie nun einen Startbildschirm von Debian sehen (siehe Abbildung 7-15), können Sie getrost weitermachen. Sollte es hier bereits zu Problemen kommen, kann es sein, dass in dieser frühen Phase der Installation Ihr Laufwerk von Linux nicht richtig erkannt wird. Versuchen Sie dann bitte, ein anderes Installationsmedium zu wählen und davon zu booten. Eventuell klappt es ja mit einem USB-Stick.



Abbildung 7-15: Startbildschirm zur Installation

Der Installer von Debian besteht aus einer Reihe von Komponenten, die jede für sich eine bestimmte Aufgabe bei der Installation übernehmen. Wenn Sie die Standardinstallation wählen, werden Sie nur bei Aufgaben mit hoher Priorität aufgefordert, eine Benutzereingabe durchzuführen. Bei allen anderen Aufgaben versucht Debian, automatisch Standardwerte zu übernehmen. Welche Komponenten nun für Sie angezeigt werden, hängt in der Regel u.a. von Ihrer Hardware ab, so dass nicht genau voraussagen ist, welche Schritte genau durchgeführt werden müssen. Dafür geben wir Ihnen im Folgenden aber eine Übersicht aller verfügbaren Komponenten samt der Aufgaben, die sie im Installationsprozess übernehmen können.

#### main-menu (Hauptmenü)

Zeigt die Liste der Komponenten während des Installationsvorgangs an und startet eine ausgewählte Komponente, wenn diese an der Reihe ist. Die Fragen des Haupt-

menüs sind auf die Prioritätsstufe *medium* gesetzt, so dass Sie das Mustermenü nicht sehen, wenn die Prioritätsstufe auf *high* oder *critical* steht (*high* ist der Standard). Wenn andererseits ein Fehler auftritt, der einen Eingriff von Ihnen verlangt, kann die Prioritätsstufe vorübergehend herabgesetzt werden, um Ihnen zu ermöglichen, das Problem zu lösen; in diesem Fall kann das Menü erscheinen.

Sie können zum Hauptmenü gelangen, indem Sie wiederholt den Zurück-Button drücken, um die gerade laufende Komponente abubrechen.

#### localechooser (Lokalisierungsauswahl)

In dieser Komponente können Sie Ihre Lokalisierungswünsche treffen. Das betrifft z.B. die Sprache, das Land und den sogenannten *Locale-Code*. Die Auswahl, die Sie hier treffen, beeinflusst sowohl die Sprachpakete, die bei der Installation der Pakete gewählt werden (z.B. Deutsch für Ihre Benutzeroberfläche), als auch die Sprache der weiteren Installationsschritte.

#### kbd-chooser (Tastatur-Auswahl)

Hier können Sie ein Tastaturmodell wählen (siehe Abbildung 7-16). Haben Sie Umlaute oder schreiben Sie mit einer englischen QWERTY-Tastatur? Auch das Keyboard eines Mac sieht anders aus.

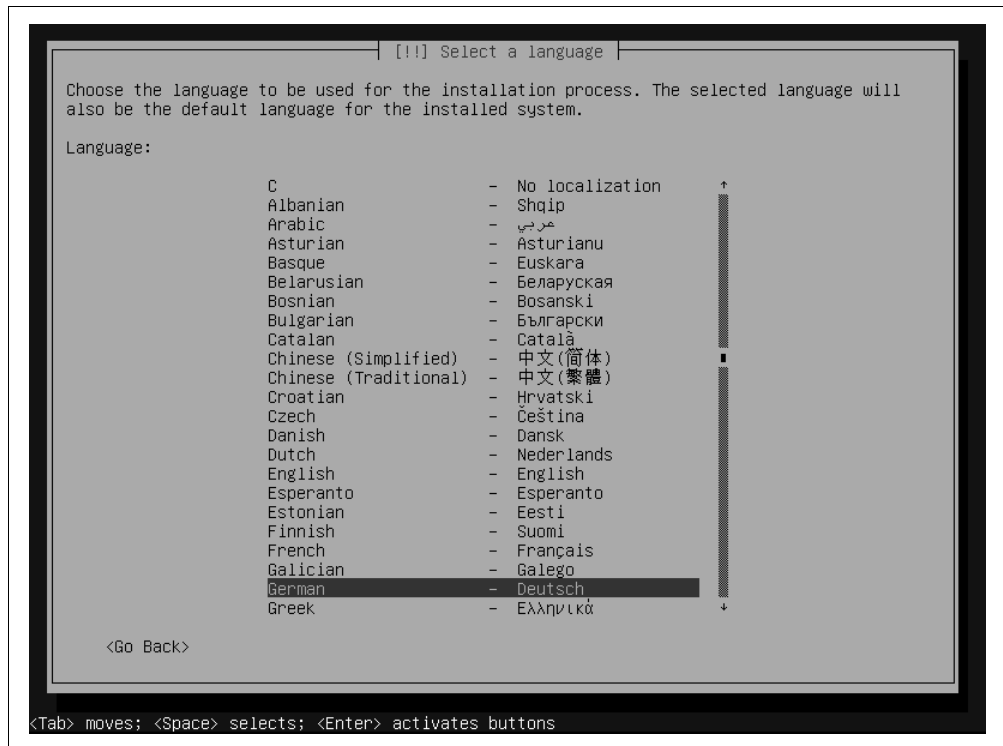


Abbildung 7-16: Auswahl des Tastaturlayouts

#### hw-detect (Hardwareerkennung)

Dies ist wohl eine der mächtigsten Komponenten für die Installation. Hier wird Ihre Hardware erkannt (z.B. CD-ROM-Laufwerk, Festplatten, Netzwerk- und Soundkarten), solange es sich nicht um irgendwelche Exoten handelt. Nachjustieren können Sie nach der Installation immer, falls irgendetwas nicht richtig funktionieren sollte.

#### cdrom-detect (Suche nach einer Debian-CD)

Es wird lediglich nach einer Debian-CD gesucht und versucht, diese in den Verzeichnisbaum einzubinden. (Linux kennt, anders als Windows, nicht verschiedene Laufwerksbuchstaben.)

#### netcfg (Netzwerkkonfiguration)

Die Netzwerkkarte, die mit der automatischen Hardwareerkennung ermittelt wurde, wird in diesem Dialog konfiguriert. Vor allem bei der netzwerkabhängigen Installation ist es wichtig, dass dieser Schritt funktioniert, da ansonsten keine weiteren Pakete aus dem Internet geladen werden können.

#### iso-scan (Suche nach ISO-Dateisystemen)

Nicht nur auf CDs können sich weitere Installationsquellen befinden. Mit *iso-scan* lassen sich die vorhandenen Festplatten nach ISO-Dateien suchen, in denen sich ggf. weitere Debian-Images befinden.

#### choose-mirror (Auswahl eines Debian-Spiegelserver)

Zeigt eine Liste von Debian-Archiv-Spiegelservern an. Hier kann der gewünschte Server für die Downloads der Paketarchive gewählt werden. Das benötigen wir später noch für das iSCSI-Target.

#### cdrom-checker (Überprüfung der CD)

Wem ist es noch nicht passiert – die Installations-CD ist defekt und das Betriebssystem kann nicht mehr gebootet werden. *cdrom-checker* überprüft die Unversehrtheit des Installationsmediums.

#### lowmem (Erkennung von zu wenig Arbeitsspeicher)

Mit der Komponente *lowmem* versucht Debian, Systeme zu erkennen, auf denen sehr wenig Arbeitsspeicher vorhanden ist. Das System kann dann durch einige Kunstgriffe – allerdings auf Kosten von Funktionalität – unnötige Teile des Debian-Installers aus dem Speicher entfernen.

#### anna (Ein Tool zur Paketinstallation)

*Anna's Not Nearly APT* (»Anna ist nicht mal annähernd APT«, ein APT-Ersatz für die Installation) ist das eigentliche Installationsprogramm für die Pakete.

#### clock-setup (Uhr konfigurieren)

Legt fest, ob die Uhr auf UTC (Universal Coordinated Time, koordinierte Weltzeit) eingestellt werden soll oder nicht, und versucht, über einen Zeitserver die Uhrzeit zu aktualisieren. Hier ist natürlich auch eine Internetverbindung notwendig, wenn die richtige Uhrzeit gesetzt werden soll. Ein PDC-Emulator in einer Active-Directory-Domäne kann dafür ebenfalls verwendet werden.

tzsetup (Zeitzone einrichten)

Hier sollte man seinen Wohnort (besser gesagt *Europe/Berlin* für Deutschland) auswählen, um die Zeitzone einzustellen.

partman (Festplattenpartitionierer)

Diese Komponente erlaubt es, die an das System angeschlossenen Festplatten zu partitionieren und den Mountpunkt für die einzelnen Partitionen zu bestimmen. Darüber hinaus ermöglicht sie es, LVM-Unterstützung zu aktivieren. Für nicht ganz so versierte Benutzer empfiehlt sich auf alle Fälle der automatische Modus.

partconf (Dateisysteme erstellen)

Mit *partconf* ist es möglich, die Dateisysteme für die entsprechenden Partitionen festzulegen.

partman-lvm (Konfigurieren von LVM)

Unterstützt bei der Konfiguration des LVM (Logical Volume Manager).

mdcfg (Software-RAID einrichten)

Mithilfe von *mdcfg* ist es möglich, ein Software-RAID (Redundant Array of Inexpensive Disks) einzurichten. Das Software-RAID ist auf alle Fälle vielen billigen IDE-Hardwarecontrollern vorzuziehen. Es bietet wesentlich mehr Stabilität bei einem größeren Funktionsumfang.

base-installer (Basissystem installieren)

Die grundlegenden Programme, die zum minimalen Betrieb eines Debian-Systems notwendig sind, werden installiert.

user-setup (Benutzer einrichten)

Hier wird lediglich ein normaler Benutzer angelegt sowie das Passwort für den *root*-Benutzer eingestellt.

apt-setup (apt konfigurieren)

Die Komponente *apt-setup* läuft weitestgehend automatisch ab, je nachdem, welches Installationsmedium gewählt wurde. Hier können z.B. weitere Installationsquellen wie Repository-Server eingestellt werden.

pkgset (Paketauswahl)

Benutzt *tasksel*, um Auswahl und Installation zusätzlicher Software zu ermöglichen.

os-prober (Andere Betriebssysteme erkennen)

Dies ist vor allem nützlich, wenn noch weitere Betriebssysteme auf dem Rechner installiert sind. Diese werden erkannt und an den Bootloader-Installer weitergereicht.

[bootloader]-installer (Installation des Bootloaders)

Die Bootload-Installer unterscheiden sich geringfügig, je nachdem, welche Architektur verwendet wird. Sie installieren aber alle ein Bootloader-Programm auf der Festplatte, das zum Starten des Systems ohne CD-ROM oder Diskette notwendig ist.

shell (Starten einer Shell/Eingabeaufforderung)

Wenn doch mal etwas schief läuft oder der automatische Installer nicht genau das tut, was man will, kann man mit der Komponente *shell* auf ein zweites Terminal

wechseln und versuchen, diverse Einstellungen von Hand vorzunehmen. Das ist allerdings nur für versierte Benutzer zu empfehlen.

save-logs (Logdateien sichern)

Zu guter Letzt kann man noch die verschiedenen Logdateien auf ein externes Medium sichern oder sie über das Netzwerk an ein entferntes Laufwerk senden. Fehler bei der Installation sind jetzt umso leichter aufzuspüren und können bei Bedarf den Debian-Entwicklern zur Behebung von Bugs zur Verfügung gestellt werden.

Wenn die einzelnen Schritte abgearbeitet sind, können wir uns an das machen, was wir Informatiker oft als »Smoke Test« bezeichnen: Wir machen einfach mal drauf los und sehen dann, ob es qualmt. Nein, mal im Ernst: Es kann hier nicht viel schiefgehen, außer dass der Rechner nicht bootet. Wir haben dann aber immer noch eine Installations-CD, von der wir erneut booten können. Dabei kann nichts kaputtgehen. Die erste Hürde haben Sie geschafft, wenn Sie nach dem POST (Power on Self Test) GRUB sehen, den Linux-Bootloader, Ihr Tor in die neue Welt. Hier sollten Sie nun in der Lage sein, Ihre neue Linux-Installation auszuwählen und zu booten. Wählen Sie nun also Ihr Linux mit den Cursortasten aus und starten Sie das System (siehe Abbildung 7-17).



Abbildung 7-17: GRUB-Bootmenü

In der Regel sollte alles gut verlaufen, wenn die Installation bis hierher noch nicht abgebrochen ist. Sollten Sie trotzdem Ihr System nicht booten können, keine Panik! Hier handelt es sich im Normalfall nur um kleinere Fehler, die mithilfe des Rettungsmodus auf der Installations-CD behoben werden können. Sie müssen also nicht die komplette Prozedur wiederholen und das System neu installieren. Für weitere Hilfe zur Funktionsweise

dieses Rettungsmodus schauen Sie bitte in der Debian-Hilfe unter <http://d-i.alioth.debian.org/tmp/de.i386/ch08s07.html> nach.

Geschafft! Sie sollten nun entweder eine grafische Oberfläche sehen (je nachdem, welche Installationsart bzw. welches Medium Sie gewählt haben), auf der Sie sich einloggen können, oder Sie befinden sich bereits im Textmodus. Alle weiteren Schritte werden wir im Textmodus durchführen – falls Sie sich also auf der grafischen Oberfläche befinden, drücken Sie einfach Strg+Alt+F1, um in den Textmodus zu gelangen. Was Sie nun sehen, ist der Login für Ihr Linux-System. Als Benutzernamen geben sie jetzt *root* ein, und dazu das Passwort, das Sie während der Installation gewählt haben.

## iSCSI konfigurieren

Wir kommen nun zur eigentlichen Aufgabe, dem Einrichten von iSCSI-Targets, die wir danach mit unserem ESXi Host für die virtuellen Maschinen verbinden wollen. Linux stellt hier spezielle Pakete bereit, die wir im ersten Schritt installieren müssen. Pakete – also zusätzliche Programme die in einem speziellen Archivformat ausgeliefert werden – lassen sich mitsamt ihrer Abhängigkeit mit dem Befehl *apt-get* installieren. *apt-get* muss dafür aber alle verfügbaren Paketquellen finden, damit diese auch installiert werden können. Führen Sie dafür bitte zunächst den Befehl

```
apt-get update
```

aus. Dadurch bekommt der Paketmanager alle neuen Pakete und die URLs mitgeteilt, unter der diese im Netz zu finden sind. Anschließend können Sie mit

```
apt-get install iscsitarget, iscsitarget-dkms
```

ein sogenanntes Kernel-Modul samt seinen Abhängigkeiten installieren (vergleichbar mit einem Treiber unter Windows). Die aktuelle Version von *iscsitarget-dkms* versucht nun, automatisch alle Abhängigkeiten zu erfüllen und zusätzlich u.a. die Pakete *iscsitarget* und *open-iscsi* zu installieren, sowie verschiedene Pakete, die für das Kompilieren des Moduls notwendig sind. Nach der Bestätigung mit Return beginnen einige Skripten, das Kernel-Modul passend für Ihr System zu kompilieren und in das System zu integrieren.

Im nächsten Schritt versuchen wir, die virtuellen Laufwerke anzulegen. Unter Linux haben wir den Vorteil, dass zunächst alles als Datei betrachtet werden kann. Das heißt, dass normale Geräte wie Festplatten normalerweise unter */dev* finden sind, z.B. */dev/sda* als erstes SCSI- oder SATA-Device, und */dev/sda1* als erste Partition. Diesen Vorteil machen wir uns zunutze, indem wir eine Datei anlegen, zunächst mit 0 befüllen und anschließend ein Dateisystem darauf erstellen. Mit dem Befehl *dd* (Disk Dump) erstellen wir zuerst so eine Datei im Verzeichnis *<Verzeichnisname>* mit einer Blockgröße von 1.048.576 Byte sowie 40.000 solcher Blöcke (macht zusammen 40 GByte).

```
dd if=/dev/zero of=/<Verzeichnisname>/lun0 bs=1048576 count=40000
```

Der Parameter *if* steht hier für ein Input-File, in unserem Fall */dev/null*, also ein virtuelles Gerät, das als Daten nur Nullen enthält. Der Parameter *of* (Output-File) gibt unsere Ziel-

datei an. Nach einigen Minuten haben wir also unser virtuelles Laufwerk erstellt, natürlich immer in Abhängigkeit von der Festplattengeschwindigkeit. Die Parameter bei `dd` können Sie nach Ihren Bedürfnissen und der Größe Ihres Laufwerks anpassen. Beachten Sie aber, dass der ESXi Server unter vSphere5 standardmäßig 1 MByte große Datenblöcke für das VMFS-Dateisystem anlegt und das iSCSI-Volume dem am besten entspricht.

Jetzt müssen wir nur noch in der Konfigurationsdatei `/etc/iet/ietd.conf` mit dem Editor unserer Wahl (z.B. `vim`) die virtuellen Devices konfigurieren. Dafür editieren wir diese mit dem Befehl

```
vim /etc/iet/ietd.conf
```

und geben nach dem Drücken der Taste `i` – um in den Eingabemodus zu springen – folgende Zeilen ein:

```
Target iqn.2011-12.de.cssv.storage:vm01-disk
Lun 0 Path=/<Verzeichnisname>/lun0,Type=blockio
IncomingUser vm01 geheim
Alias vm01-disk
```

Der Eintrag `Target` definiert so ein Speichergerät, von denen nach Belieben mehrere in beliebiger Größe in der Konfigurationsdatei eingetragen werden können. Als Adresse dient uns ein sogenannter *iSCSI Qualified Name*, kurz IQN. Dieser ist so etwas wie eine MAC-Adresse für Netzwerkkarten und eigentlich nur einmal auf der ganzen Welt verfügbar und muss bei einer zuständigen Stelle beantragt werden. Für Testzwecke können wir das aber getrost ignorieren und selbst einen Namen in folgender Form wählen:

```
iqn.<Aktivierungsdatum in JJJJ-MM>.<Rekursiver DNS Name>:[Freier Bezeichner]
```

also in unserem Fall

```
iqn.2011-12.de.cssv.storage:lvn.vm03-disk
```

Die Zeile

```
Lun 0 Path=/<Verzeichnisname>/lun0,Type=blockio
```

teilt dem Daemon nun mit, unter welcher Datei auf dem lokalen Verzeichnis unser Laufwerk zu finden ist (auch wenn es ein virtuelles ist). `Type` gibt nun zusätzlich einen Typ für die Übertragung der Daten an. Erfahrungsgemäß sollte man für kleine Blockgrößen mit weniger als 64 KByte den Typ *fileio* setzen, *blockio* eignet sich dagegen besser für große Blöcke ab 64 KByte. Sie erinnern sich, dass wir mit `dd` und dem Parameter `bs` eine Blockgröße von einem GByte gesetzt haben?

```
IncomingUser vm01 geheim
```

kann jetzt genutzt werden, um optional für einkommende Verbindungen mit dem Benutzernamen *vm01* das Passwort *geheim* zu verwenden, das dann von Clients für die Kommunikation genutzt werden muss.

Die letzte Zeile

```
Alias vm01-disk
```



vergibt einen alternativen Aliasnamen, unter dem die iSCSI-Geräte später unter VMware zu sehen sind.

Nachdem Sie das alles nun mit vim eingegeben haben, müssen Sie die Datei speichern und den Editor verlassen. Dafür drücken Sie bitte einmal die Esc-Taste gefolgt von der Zeichenkombination `:wq`. Ein Return bestätigt das Speichern, und der Editor wird geschlossen. Jetzt haben wir es fast geschafft. Die Geräte sind eingerichtet und iSCSI ist auf dem System installiert. Bevor wir unseren *iscsitarget*-Daemon starten können, müssen wir auf einem Debian-System noch die Datei */etc/default/iscsitarget* anlegen und dort einen Eintrag vornehmen. Wir bedienen uns hier einmal schnell der Ausgabeumleitung unter Linux und führen Folgendes aus:

```
echo "ISCITARGET_ENABLE=true" > /etc/default/iscsitarget
```

Jetzt müssen wir alles nur noch starten. Der Befehl

```
/etc/init.d/iscsitarget start
```

hilft uns dabei und startet das Init-V-Skript für den Dienst *iscsitarget* (siehe Abbildung 7-18).



```
root@debian:/var# /etc/init.d/iscsitarget start
Starting iSCSI enterprise target service:.
root@debian:/var# _
```

Abbildung 7-18: iSCSI Target starten

*[Ende der Ausführungen von Christian Schneiker]*

Nun können Sie – wie oben bereits ausführlich beschrieben – die Konfiguration des oder der ESXi Hosts vornehmen und auf das neue iSCSI-Ziel zugreifen. Sollten Sie später Änderungen z.B. am Netzwerk des Storage vornehmen wollen, können Sie sich über die Kommandozeile, PuTTY oder WinSCP die Datei */etc/network/interfaces* vornehmen und dort Änderungen eintragen, wie im folgenden Beispiel eines Rechners mit vier Netzwerkkarten:

```
This file describes the network interfaces available on your system
and how to activate them. For more information, see interfaces(5).

The loopback network interface
auto lo eth0 eth1 eth2 eth3
iface lo inet loopback

The primary network interface
allow-hotplug eth0
iface eth0 inet static
 address 192.168.150.1
```

```

netmask 255.255.255.0
network 192.168.150.0
broadcast 192.168.150.255
gateway 192.168.150.10
dns-* options are implemented by the resolvconf package, if installed
dns-nameservers 192.168.150.10
dns-search gfu.dom
mtu 9000

iface eth1 inet static
address 192.168.150.2
netmask 255.255.255.0
network 192.168.150.0
mtu 9000

iface eth2 inet static
address 192.168.150.3
netmask 255.255.255.0
network 192.168.150.0
mtu 9000

iface eth3 inet static
address 192.168.150.4
netmask 255.255.255.0
network 192.168.150.0
mtu 9000

```

Wer sich mit Solaris auskennt, kann hier zusätzlich das neue Dateisystem ZFS nutzen, das in Zusammenhang mit iSCSI enorme Leistungswerte erzielt. Auch die Erstellung eines RAID's über eine Zeile in der Eingabeaufforderung ist möglich, wie in Abbildung 7-19 gezeigt wird.

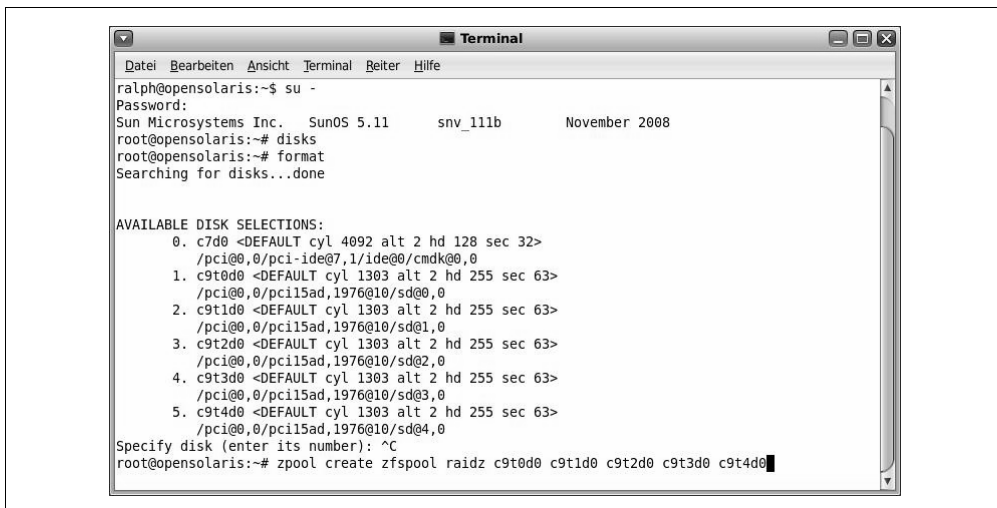


Abbildung 7-19: NFS oder iSCSI Storage unter Opensolaris mit ZFS

# Virtuelle Maschinen verschieben

Wenn Sie Ihren neuen Storage eingerichtet haben, auf den nun mehrere ESXi Server zugreifen können, und noch keinen vCenter Server einsetzen, können Sie Ihre VMs über den Datenspeicherbrowser kopieren oder verschieben. Ich empfehle Ihnen, zunächst die Maschine zu kopieren und auszutesten und anschließend die lokal abgespeicherte zu löschen oder als Sicherungskopie zu behalten.

Gehen Sie zum Verschieben von VMs auf einen anderen Datenspeicher folgendermaßen vor:

1. Klicken Sie auf die zu verschiebende virtuelle Maschine. Der Datenträger wird in der rechten Hälfte des Fensters angezeigt.
2. Klicken Sie mit der rechten Maustaste auf den Datenträger und wählen Sie aus dem Kontextmenü DATENSPEICHER DURCHSUCHEN.
3. Wählen Sie auf der rechten Seite des Fensters das Verzeichnis der gewünschten VM aus, klicken Sie mit der rechten Maustaste darauf und wählen Sie aus dem Kontextmenü KOPIEREN. Über die Schaltflächen können Sie sie nämlich nur verschieben oder herunterladen.
4. Klicken Sie anschließend in der Bestandsliste auf den ESXi Server, dann auf den Storage, auf den die Maschine kopiert werden soll, und dann im Kontextmenü wieder auf DATENSPEICHER DURCHSUCHEN.
5. In dem zweiten Browserfenster können Sie über ein weiteres Kontextmenü die Maschine einfügen (siehe Abbildung 7-20).



Abbildung 7-20: Die Datei wird kopiert

6. Wenn der Kopiervorgang abgeschlossen ist, klicken Sie auf die Original-VM in der Bestandsliste und wählen aus dem Kontextmenü AUS BESTANDSLISTE ENTFERNEN aus. Damit wird diese Maschine nicht gelöscht, sondern nur nicht mehr als registrierte VM aufgelistet.

7. Im Datenspeicherbrowser des externen Speichers gehen Sie in das Verzeichnis der VM, klicken mit der rechten Maustaste die `.vmx`-Datei an und wählen ZUR BESTANDSLISTE HINZUFÜGEN.
8. Übernehmen Sie die Voreinstellungen und klicken Sie auf BEENDEN.

Nun können Sie Ihre kopierte virtuelle Maschine einschalten und testen. Wenn alles okay ist, löschen Sie das Ausgangsverzeichnis von der lokalen Platte.



Beim Einschalten bekommen Sie eine Meldung, dass die VM kopiert oder verschoben wurde und dass gegebenenfalls Probleme im Netzwerk und beim Management auftreten können. Wenn Sie die Originalmaschine nicht gleichzeitig starten oder sogar löschen wollen, wählen Sie hier `I_MOVED IT`. Damit behält sie ihre ID und auch ihre MAC-Adresse. Wollen Sie beide Maschinen behalten und aus der kopierten eine neue VM machen, wählen Sie `I_COPIED IT` (siehe Abbildung 7-21). Damit müssen Sie im Betriebssystem nur noch den Namen und gegebenenfalls die IP-Adresse anpassen.

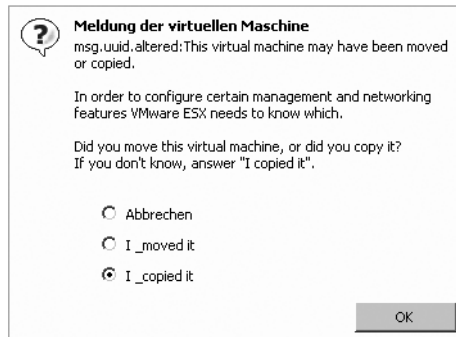


Abbildung 7-21: Meldung zur virtuellen Maschine

Vorsicht bei Microsoft-Betriebssystemen: Eventuell müssen Sie noch eine neue SID (*Security Identifier*) generieren – obwohl der Programmierer von NewSID, Mark Russinovich, am 3.11.2009 in seinem Blog geschrieben hat, dies sei in den meisten Fällen gar nicht notwendig! Siehe auch <http://blogs.technet.com/markrussinovich/archive/2009/11/03/3291024.aspx>.

Bis hierher haben Sie eine komplette Umgebung mit virtuellen Maschinen und allein stehenden ESXi Servern aufgebaut. Was man ohne vCenter Server noch so alles machen kann, folgt in den nächsten Kapiteln. Dazu gehört natürlich die Funktion der Snapshots, die im nächsten Kapitel besprochen wird.

# Snapshots

Mithilfe von *VMware Snapshots* können Sie den Status einer virtuellen Maschine »einfrieren« und anschließend bei Bedarf wiederherstellen. Das geht auch mehrfach und verschachtelt – und auch ohne den vCenter Server.

## Was ist ein Snapshot?

Ein Snapshot erfasst den gesamten Status einer virtuellen Maschine zum Zeitpunkt der Erstellung dieses Snapshots. Das beinhaltet

- den Arbeitsspeichereinhalt der virtuellen Maschine,
- die Einstellungen der virtuellen Maschine sowie
- den Status aller virtuellen Festplatten der virtuellen Maschine.



Snapshots von Raw-Festplatten (RDM, *Raw Device Mapping*) mit physischen Modi oder unabhängigen (dauerhaften und nicht dauerhaften) Festplatten werden nicht unterstützt.

Snapshots werden immer für eine einzelne virtuelle Maschine erstellt. In einer Gruppe von virtuellen Maschinen wird durch das Aufzeichnen eines Snapshots lediglich der Status der aktiven virtuellen Maschine festgehalten. Wenn Sie einen Snapshot wiederherstellen, versetzen Sie alle diese Objekte in den Zustand, in dem sie zum Zeitpunkt der Erstellung des Snapshots vorlagen. Wenn die virtuelle Maschine zum Zeitpunkt der Wiederherstellung angehalten, eingeschaltet oder ausgeschaltet sein soll, stellen Sie sicher, dass sich die VM beim Erstellen des Snapshots im gewünschten Zustand befindet.

Snapshots können Sie für viele Einsatzzwecke verwenden, z.B. wenn Sie ein Programm unter verschiedenen Bedingungen testen wollen und dafür nicht immer eine neue VM erstellen möchten oder wenn bei einer produktiven Maschine ein Update anliegt und Sie sich nicht sicher sind, ob jede Software anschließend noch läuft. Machen Sie einen

Snapshot, installieren Sie das Update und testen Sie Ihr System. Läuft alles, können Sie den Snapshot löschen – funktioniert das System anschließend aber nicht wie gewünscht, machen Sie einen *Revert*, und Ihre VM läuft wieder wie vor dem Upgrade. Das ist vergleichbar mit den Wiederherstellungspunkten unter Windows, aber zuverlässiger, weil die Ausgangssituation komplett unangetastet bleibt.

Auch für Programmierer, die viele verschiedene Voraussetzungen testen wollen, lohnt es sich, einen oder mehrere Snapshots zu erstellen, z.B. mit verschiedenen Browsern, Softwareständen oder Servicepacks fürs Betriebssystem.

## Wie funktioniert ein Snapshot?

Die Festplatte der virtuellen Maschine wird nur noch lesend geöffnet. Alle Änderungen am Datenbestand werden in einer neuen *.vmdk*-Datei (Deltadatei) abgespeichert. Wenn gewünscht, wird auch der Inhalt des Arbeitsspeichers mitgesichert. Bei einem weiteren Snapshot wird die alte und neue Festplattendatei quasi schreibgeschützt, weitere Änderungen laufen in eine neue Deltadatei usw. Sie können zu jedem Zeitpunkt zu jedem Zustand wechseln und dann auch einen neuen Snapshot machen – also *geschachtelte Snapshots* erstellen.

Die erste Snapshot-Deltafestplatte heißt z.B. *vm1-000001.vmdk*, die zweite dementsprechend *vm1-000002.vmdk*, usw.

Wenn Sie einen Snapshot löschen, werden die Inhalte aller aktiv beteiligten Deltadateien auf die Festplattendatei übernommen.



Beachten Sie, dass bei Snapshots auch die Konfigurationsdatei der VM mitgesichert wird. Haben Sie also einen Snapshot und ändern z.B. an der Hardware der VM etwas, ist das nach einem Revert ebenfalls rückgängig gemacht.

## Empfehlungen zu Snapshots

Grundsätzlich ist es das Beste, Snapshots dann zu erstellen, wenn gerade kein Datenaustausch zwischen einer Anwendung in der virtuellen Maschine und anderen Computern stattfindet. Wenn das vor allem in Produktionsumgebungen der Fall ist, z.B. während eines Updates, ist die Wahrscheinlichkeit hoch, dass Probleme auftreten können.

Behalten Sie Snapshots nur so lange wie unbedingt nötig (außer in Testumgebungen) und dokumentieren Sie, was Sie getan haben – und am besten noch, warum Sie es getan haben. Sie kennen sicherlich den Fall, dass Sie etwas in einer Plastikbox einfrieren und nach zwei Wochen nicht mehr wissen, was drin ist!

Wenn Sie den Arbeitsspeicher der VM nicht mit abspeichern und WIEDERHERSTELLEN wählen, ist die VM in einem Zustand, als hätten Sie sie hart abgeschaltet, ohne herunterzufahren.



Einige Datensicherungsprogramme und auch der Update Manager von VMware nutzen Snapshots, weil die Festplattendatei nur im Lesemodus geöffnet ist und somit kopiert oder gesichert werden kann. Snapshots sollten aber nicht zur Sicherung virtueller Maschinen eingesetzt werden, sondern nur die Ausgangsdatei. Den Snapshot von VM1 können Sie nicht bei VM2 einspielen.



Beachten Sie bitte, dass Sie bei Snapshots dynamisch wachsende Dateien haben, die nicht so performant sind wie Dateien mit fester Größe, und dass der ESXi Server dadurch mehr belastet wird.



Bei Domänencontrollern von Microsoft ist besondere Vorsicht geboten: Wenn Sie einen Revert machen, befindet sich die VM in dem Zustand zum Zeitpunkt der Erstellung. Liegt der Zeitraum zu weit in der Vergangenheit, kann das Probleme mit der Active Directory-Datenbank geben. Abhilfe schafft Folgendes: Nehmen Sie der VM so schnell wie möglich nach dem Wiederherstellen das »Netzwerkkabel« weg (NIC nicht verbunden). Fahren Sie die Maschine herunter und schalten Sie sie aus. Bitte keinen Neustart machen, weil sich der Rechner das merkt! Ist die Maschine wieder gestartet, verbinden Sie die Netzwerkkarte wieder über die Einstellungen.

## Einen Snapshot erstellen

Snapshots können im eingeschalteten, ausgeschalteten oder angehaltenen Zustand der virtuellen Maschine erstellt werden. Wenn Sie eine virtuelle Maschine gerade anhalten, dann sollten Sie warten, bis dieser Vorgang abgeschlossen ist, bevor Sie einen Snapshot erstellen.

Wenn eine virtuelle Maschine über mehrere Festplatten in unterschiedlichen Festplattenmodi verfügt, müssen Sie die virtuelle Maschine vor dem Erstellen eines Snapshots ausschalten oder den Arbeitsspeicher vom Snapshot ausnehmen. Ist beispielsweise eine Konfiguration für einen bestimmten Zweck vorhanden, die die Verwendung einer unabhängigen Festplatte erforderlich macht, müssen Sie die virtuelle Maschine vor dem Erstellen eines Snapshots ausschalten oder das Häkchen bei SNAPSHOT DES ARBEITSSPEICHERS DER VIRTUELLEN MASCHINE ERSTELLEN wegklicken, ansonsten bekommen Sie eine Fehlermeldung und es wird kein Snapshot erstellt.

### *Vorgehensweise*

1. Wählen Sie BESTANDSLISTE → VIRTUELLE MASCHINE → SNAPSHOT → SNAPSHOT ERSTELLEN (siehe Abbildung 8-1). Sie können auch mit der rechten Maustaste auf die virtuelle Maschine klicken und SNAPSHOT → SNAPSHOT ERSTELLEN wählen. – Das Fenster SNAPSHOT EINER VIRTUELLEN MASCHINE ERSTELLEN wird angezeigt.
2. Geben Sie einen Namen für den Snapshot ein.

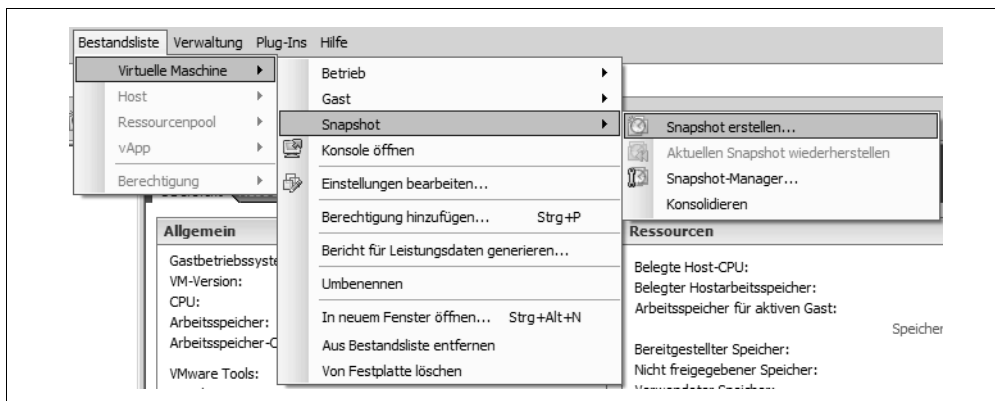


Abbildung 8-1: Snapshot-Menü

3. Wichtig: Geben Sie eine gute Beschreibung Ihres Snapshots, Ihren Namen und das aktuelle Datum samt Uhrzeit ein.
4. Überlegen Sie, ob Sie das Kontrollkästchen **SNAPSHOT DES ARBEITSSPEICHERS DER VIRTUELLEN MASCHINE ERSTELLEN** auswählen wollen, wenn Sie den Arbeitsspeicher der virtuellen Maschine mit einbeziehen möchten.
5. (Optional:) Aktivieren Sie das Kontrollkästchen **GAST-DATEISYSTEM STILLLEGEN** (VMWARE TOOLS MÜSSEN INSTALLIERT SEIN), um laufende Prozesse auf dem Gastbetriebssystem anzuhalten, so dass Dateisysteminhalte einen bekannten, konsistenten Status besitzen, wenn der Snapshot erstellt wird. Das gilt nur für eingeschaltete virtuelle Maschinen.
6. Klicken Sie auf OK. Wenn der Snapshot erfolgreich erstellt wurde, wird er im Feld **KÜRZLICH BEARBEITETE AUFGABEN** im unteren Bereich des vSphere Client-Fensters aufgeführt.
7. Klicken Sie auf die virtuelle Zielmaschine, um Aufgaben und Ereignisse für die betreffende Maschine anzuzeigen, oder klicken Sie, während die virtuelle Maschine noch ausgewählt ist, auf die Registerkarte **AUFGABEN & EREIGNISSE**.

## Virtuelle Festplatten von Snapshots ausschließen

Festplatten der VM, die sich im unabhängigen Modus befinden, werden von Snapshots nicht berücksichtigt. Es gibt dabei zwei Zustände, die in Tabelle 8-1 beschrieben werden.

Tabelle 8-1: Optionen von unabhängigen Festplatten

| Option    | Beschreibung                                                                                                                                                                                                                                     |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dauerhaft | Festplatten im dauerhaften Modus verhalten sich wie konventionelle Festplatten auf einem physischen Computer. Sämtliche Daten, die im dauerhaften Modus auf eine Festplatte geschrieben werden, werden permanent auf die Festplatte geschrieben. |



Tabelle 8-1: Optionen von unabhängigen Festplatten (Fortsetzung)

| Option          | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nicht dauerhaft | Änderungen, die im nicht dauerhaften Modus an Festplatten vorgenommen werden, werden beim Ausschalten oder Zurücksetzen der virtuellen Maschine verworfen. Der nicht dauerhafte Modus ermöglicht Ihnen, die virtuelle Maschine mit einer virtuellen Festplatte neu zu starten, die sich jedes Mal im selben Zustand befindet. Änderungen an der Festplatte werden tatsächlich in eine Redo-Protokolldatei geschrieben und daraus gelesen, die beim Ausschalten oder Zurücksetzen gelöscht wird. |

Sie können den Modus nur bei ausgeschalteten VMs ändern und alle vorhandenen Snapshots vorher löschen.

1. Wählen Sie BESTANDSLISTE → VIRTUELLE MASCHINE → EINSTELLUNGEN BEARBEITEN oder über das Kontextmenü auf der VM EINSTELLUNGEN BEARBEITEN.
2. Klicken Sie auf die Registerkarte HARDWARE und wählen Sie die auszuschließende Festplatte aus.
3. Wählen Sie unter MODUS die Option UNABHÄNGIG aus. Unabhängige Festplatten werden nicht in Snapshots einbezogen. Bei unabhängigen Festplatten stehen Ihnen die oben beschriebenen Optionen zur Verfügung.
4. Klicken Sie auf OK.

Beachten Sie, dass unabhängige Festplatten im nicht dauerhaften Modus zur Laufzeit der VM nicht geändert werden. Alle Änderungen werden in einer Deltadatei festgehalten, die dynamisch wächst. Dynamisch wachsende Festplatten sind erstens langsamer, zweitens belasten sie das System mehr, und drittens sind alle Änderungen weg, wenn Sie die Maschine herunterfahren und ausschalten. Der Arbeitsspeicher von laufenden VMs kann dann nicht mehr in den Snapshot einbezogen werden (siehe oben).

## Den Snapshot-Manager verwenden

Über den Snapshot-Manager können Sie alle Snapshots für die virtuellen Maschinen ansehen und behalten damit die Übersicht.

Im Fenster SNAPSHOT-MANAGER sehen Sie links die Hierarchie, unten die Befehlsschaltflächen und rechts den Detailbereich mit Namen und Beschreibung. In der Hierarchie sehen Sie anhand des Eintrags SIE BEFINDEN SICH HIER, in welchem aktuellen Betriebszustand sich die VM gerade befindet. Diese Felder sind leer, wenn kein Snapshot ausgewählt wurde.

Das Symbol SIE BEFINDEN SICH HIER ist immer ausgewählt und sichtbar, wenn Sie den Snapshot-Manager öffnen. Der Status SIE BEFINDEN SICH HIER kann weder angesteuert noch markiert werden. Er repräsentiert stets den aktuellen und aktiven Status.

In Abbildung 8-2 sehen Sie das Fenster für die Erstellung eines Snapshots.

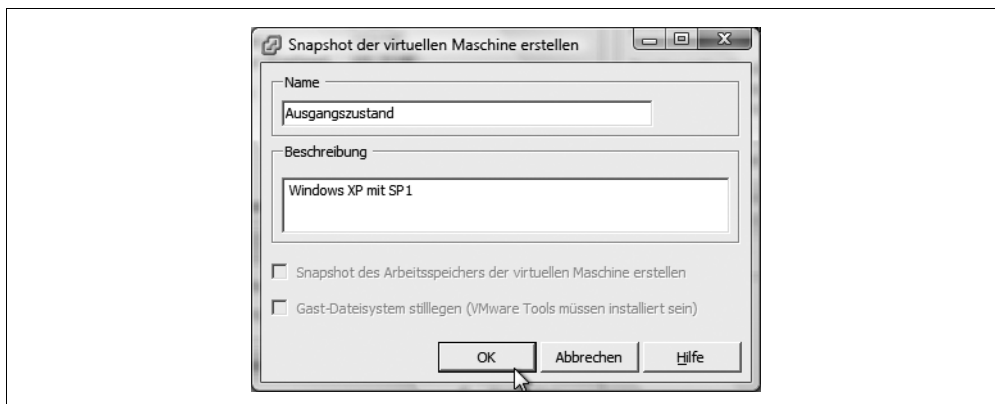


Abbildung 8-2: Erster Snapshot

Der Snapshot-Manager verfügt im linken Fenster über die drei Befehlsschaltflächen WECHSELN ZU, LÖSCHEN und ALLE LÖSCHEN. Diese Funktionen werden in den folgenden Abschnitten behandelt.

## Zu einem Snapshot wechseln

Mithilfe der Schaltfläche WECHSELN ZU können Sie zu jedem Status eines beliebigen Snapshots springen und dort weiterarbeiten.

1. Wählen Sie BESTANDSLISTE → VIRTUELLE MASCHINE → SNAPSHOT → SNAPSHOT-MANAGER.
2. Klicken Sie im Snapshot-Manager auf einen Snapshot, um ihn auszuwählen.
3. Klicken Sie auf die Schaltfläche WECHSELN ZU, um den Status der virtuellen Maschine wiederherzustellen, der einem beliebigen Snapshot entspricht.



Virtuelle Maschinen, die stark ausgelastet sind, benötigen unter Umständen mehrere Minuten, bevor sie wieder antworten, nachdem ein Snapshot wiederhergestellt wurde. Diese Verzögerung kann durch Vergrößern des Gastarbeitsspeichers reduziert werden.

4. Klicken Sie im Bestätigungsdialogfeld auf JA.

## Einen Snapshot löschen

Sie können einen beliebigen Snapshot vollständig entfernen:

1. Wählen Sie BESTANDSLISTE → VIRTUELLE MASCHINE → SNAPSHOT → SNAPSHOT-MANAGER.
2. Navigieren Sie im Snapshot-Manager auf den gewünschten Snapshot, um ihn auszuwählen.

3. Klicken Sie auf LÖSCHEN, um einen Snapshot permanent zu löschen. Wenn Sie auf ALLE LÖSCHEN klicken, werden alle Snapshots dauerhaft von der virtuellen Maschine entfernt.



Wenn Sie auf LÖSCHEN klicken, werden die Snapshot-Daten im übergeordneten Element festgeschrieben und der ausgewählte Snapshot entfernt. Durch Auswahl von ALLE LÖSCHEN werden alle unmittelbar vor dem aktuellen Status SIE BEFINDEN SICH HIER liegenden Snapshots auf die Basisfestplatte übernommen, und alle vorhandenen Snapshots für die betreffende virtuelle Maschine werden entfernt.

4. Klicken Sie im Bestätigungsdiaologfeld auf JA.

## Einen Snapshot wiederherstellen

Sie können einen (nicht gelöschten) Snapshot wiederherstellen, um eine virtuelle Maschine in ihren ursprünglichen Zustand zu versetzen. Führen Sie einen der folgenden Schritte aus:

1. Das Menü BESTANDSLISTE → VIRTUELLE MASCHINE → SNAPSHOT enthält den Befehl SNAPSHOT WIEDERHERSTELLEN.
- Der Snapshot-Manager enthält eine Schaltfläche WECHSELN ZU.

## Übergeordneter Snapshot

Der übergeordnete Snapshot ist die zuletzt gespeicherte Version des aktuellen Status der virtuellen Maschine. Der letzte Snapshot entspricht dem gespeicherten Status des übergeordneten Snapshot (SIE BEFINDEN SICH HIER). Wenn Sie einen Snapshot wiederherstellen oder zu ihm wechseln, wird er zum übergeordneten Element des aktuellen Status und wird mit SIE BEFINDEN SICH HIER angezeigt.



Der übergeordnete Snapshot ist immer der Snapshot, der im Snapshot-Manager direkt über dem SIE BEFINDEN SICH HIER-Symbol angezeigt wird.

Der übergeordnete Snapshot ist nicht immer der Snapshot, den Sie zuletzt erstellt haben, je nachdem, zu welchem Sie gewechselt sind.

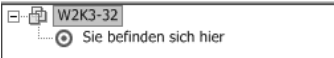
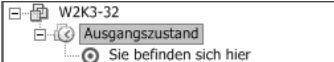
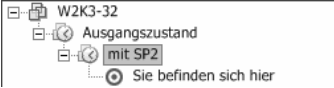
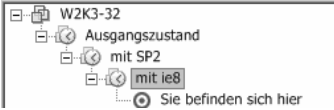
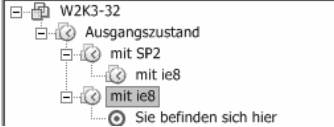
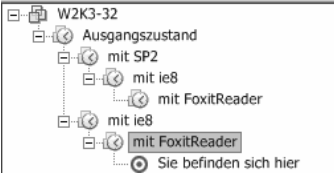
## Der Befehl »Snapshot wiederherstellen«

SNAPSHOT WIEDERHERSTELLEN ist eine Verknüpfung von SIE BEFINDEN SICH HIER zum übergeordneten Snapshot. Dieser Befehl aktiviert sofort den übergeordneten Snapshot der virtuellen Maschine. Der aktuelle Festplatten- und gegebenenfalls Arbeitsspeicherstatus werden aufgehoben, und der Zustand, in dem sich die Elemente zum Zeitpunkt der Aufnahme des Snapshots befanden, wird wiederhergestellt. Wenn der übergeordnete Snapshot erstellt wurde, während die virtuelle Maschine ausgeschaltet war, wird die ein-

geschaltete virtuelle Maschine durch Wählen der Option **SNAPSHOT** → **SNAPSHOT WIEDERHERSTELLEN** in diesen übergeordneten Status zurückversetzt, d.h. in den ausgeschalteten Zustand. War sie eingeschaltet und haben Sie den RAM mitgesichert, läuft sie wieder ab diesem Zeitpunkt weiter.

In Tabelle 8-2 sehen Sie Erstellung verschachtelter Snapshots einer Maschine. Sie können zu jedem Zeitpunkt zu jedem Zustand springen.

Tabelle 8-2: Snapshot-Manager mit verschachtelten Snapshots

|                                                                                    |                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | <p>Virtuelle Maschine ohne Snapshot</p>                                                                                                                                                                                                                                                 |
|   | <p>Der Snapshot <i>Ausgangszustand</i> ist der übergeordnete Snapshot des <i>Sie befinden sich hier</i>-Status. Der übergeordnete Snapshot des <i>Sie befinden sich hier</i>-Status ist der übergeordnete Snapshot der VM.</p>                                                          |
|   | <p>Wenn Sie einen Snapshot vom Status von <i>Ausgangszustand</i> erstellen, wird <i>Ausgangszustand</i> der übergeordnete Snapshot des neuen Snapshots <i>mit SP2</i>; <i>mit SP2</i> ist der übergeordnete Snapshot des <i>Sie befinden sich hier</i>-Status.</p>                      |
|   | <p>Wenn Sie einen weiteren Snapshot erstellen, basiert dieser auf dem Snapshot <i>mit SP2</i>, der dadurch auch zum übergeordneten Snapshot von <i>mit ie8</i> wird.</p>                                                                                                                |
|   | <p>Wenn Sie zu <i>Ausgangszustand</i> wechseln, wird <i>Ausgangszustand</i> der übergeordnete Snapshot des <i>Sie befinden sich hier</i>-Status. Erstellen Sie hier einen neuen Snapshot, basiert er genau wie <i>mit SP2</i> auf <i>Ausgangszustand</i>.</p>                           |
|  | <p>Sie können zu jederzeit zu jedem Snapshot wechseln und einen neuen erstellen.<br/>Wenn Sie wie in diesem Beispiel im Snapshot-Manager auf die Schaltfläche <i>Alle löschen</i> klicken, verlieren Sie <i>mit SP2</i>, übernehmen aber <i>mit ie8</i> und <i>mit FoxitReader</i>.</p> |

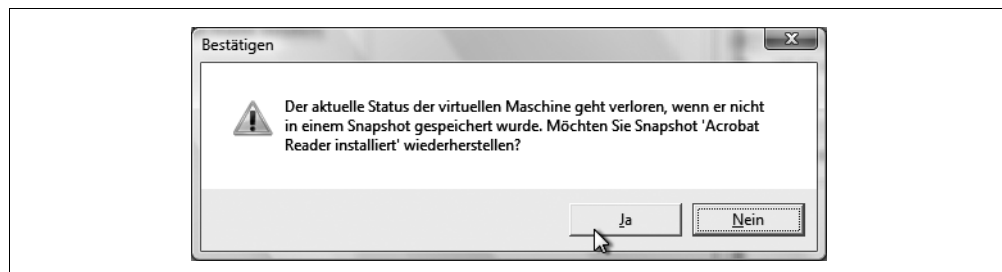


Abbildung 8-3: Meldung des Snapshot-Managers

- Wählen Sie BESTANDSLISTE → VIRTUELLE MASCHINE → SNAPSHOT → SNAPSHOT WIEDERHERSTELLEN aus.

Beachten Sie die Meldungen des Snapshot-Managers, bevor Sie eine Entscheidung treffen. Es gibt hier keinen Rückgängig-Befehl (siehe Abbildung 8-3).

Sie können insgesamt bis zu 32 Snapshots pro virtueller Maschine erstellen. Bedenken Sie dabei aber bitte den enormen Speicherbedarf, der über die gewählte Festplattengröße hinaus immer weiter anwächst.

## Fehlerbehebung bei Snapshots

Überprüfen Sie in regelmäßigen Abständen, ob Ihre Umgebung noch ungewollte Snapshots einzelner VMs enthält. Wie bereits oben erwähnt, muss ein Snapshot nicht manuell von einem Benutzer erstellt worden sein – auch Datensicherungsprogramme nutzen diese Möglichkeit, um die virtuelle Festplatte kopieren zu können. Leider hat die Praxis gezeigt, dass das Entfernen der Snapshots nicht bei jeder Software zuverlässig funktioniert.

Sollte es einer Datensicherungssoftware nicht möglich sein, einen Snapshot zu kreieren oder zu übernehmen, liegt das häufig an den VMware Tools in Verbindung mit betriebssystemeigenen Diensten. Unter Windows-Betriebssystemen ab Vista erhalten Sie bei den VMware Tools zusätzlich einen Treiber für die VSS-Unterstützung. Dieser verursacht manchmal Probleme. Deinstallieren Sie ihn aber nur bei Maschinen, bei denen Sie auf Probleme stoßen. Gehen Sie dazu wie folgt vor:

- Wählen Sie bei der eingeschalteten virtuellen Maschine aus dem Menü VMWARE TOOLS INSTALLIEREN / AKTUALISIEREN.
- Nehmen Sie dafür das interaktive Update und klicken Sie auf OK.
- Bestätigen Sie, dass Sie etwas ändern wollen, und nehmen Sie im nächsten Fenster das Häkchen bei VSS-UNTERSTÜTZUNG weg.
- Starten Sie nach Abschluss der Änderungen den Rechner neu.

## Snapshot-Dateien

Wie bereits erwähnt, werden im Verzeichnis der virtuellen Maschine Dateien für die Snapshots angelegt. Auch wenn Ihre VM noch nie einen Snapshot hatte, existiert bereits eine Datei mit der Endung *.vmsd*, und zwar mit der Größe 0. Wurden schon einmal Snapshots erstellt und ggf. wieder gelöscht, ist die Datei größer als 0. Wenn Sie diese Datei löschen und Ihre VM anschließend hochfahren, wird die Datei mit der Größe 0 neu angelegt.

Solange Sie aber Snapshots der Maschine haben, sollten Sie diese auf keinen Fall löschen, sonst können Sie die gemachten Snapshots nicht mehr löschen oder übernehmen. Haben Sie aus Versehen diese Datei gelöscht oder ist sie defekt, können Sie im Snapshot-Mana-

ger nur noch WECHSELN ZU anklicken – dann sind aber die Snapshot-Dateien immer noch aktiv und es wird nicht in die eigentliche Festplatte geschrieben.

Um diesen Missstand zu beheben, fahren Sie die VM herunter und schalten Sie sie aus. Gehen Sie anschließend in ihre Eigenschaften und wählen dort die Festplatte aus. Im rechten Teil des Fensters sehen sie die Festplattendatei mit der Bezeichnung *00001.vmdk* (oder so ähnlich) am Ende. Löschen Sie diese Datei – aber nicht von der Festplatte, sondern trennen Sie sie nur von der VM, sonst wird auch die tatsächliche Festplatte gelöscht. Als Nächstes fügen Sie der VM eine vorhandene Festplatte hinzu. Navigieren Sie zum Verzeichnis der VM und wählen Sie die Datei ohne die Endung *00001.vmdk* (oder so ähnlich).

Anschließend können Sie über den Datastore-Browser alle Dateien mit den Endungen

- *00001.vmdk* (oder so ähnlich),
- *SnapshotX.vmsn* (X ist der x-te Snapshot) und
- *.vmsd*

löschen.

Tabelle 8-3 enthält eine Auflistung aller zu einem Snapshot gehörenden Dateien samt kurzer Erklärungen.

*Tabelle 8-3: Zu einem Snapshot gehörende Dateien*

| Datei                | Bedeutung                                                                                                                                                    |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VM1-Snapshot1.vmsn   | Hauptspeichereinhalt der VM zum Zeitpunkt des Snapshots. Zu jedem Snapshot gibt es eine eigene Datei.                                                        |
| VM1.vmsd             | Informationen zu Snapshots. Ohne Snapshot: Größe 0.                                                                                                          |
| VM1-00001-delta.vmdk | Neue Festplatte des Snapshots. Darin werden die Änderungen zur tatsächlichen <i>.vmdk</i> -Datei aufgezeichnet. Zu jedem Snapshot gibt es eine eigene Datei. |
| VM1-00001.vmdk       | Festplattenbeschreibungsdatei zur Snapshot-Festplatte ( <i>delta.vmdk</i> ). Zu jedem Snapshot gibt es eine eigene Datei.                                    |

Abschließend betrachtet, ist ein Snapshot schon eine tolle Sache. Er lässt einen ohne großartige Umwege mal eben den gesamten Status einer VM einfrieren, und man kann ohne Schweißperlen auf der Stirn Updates und Servicepacks einspielen und ausprobieren.

Beachten Sie aber unbedingt die oben erwähnten Vorsichtsmaßnahmen, damit Sie nicht das ein oder andere Problem bekommen.

---

# Arbeiten auf der Kommandozeile

Egal, ob man sich direkt an den Server setzt und dort Alt+F1 drückt, um auf der Kommandozeile zu arbeiten, oder ob man sich mit einer Remote-Software wie putty verbindet: Einiges lässt sich nur hier erledigen. Gerade wenn Probleme mit dem Zugriff auf den ESXi Server bestehen, muss man häufig den einen oder anderen Befehl dort ausführen.

Die Möglichkeiten, die man dabei auf der direkten Konsole hat, sind sehr eingeschränkt, da sich kein Betriebssystem unter der Virtualisierungsschicht befindet. Über die BusyBox können allerdings einige Befehle eingegeben werden, die manchmal die letzte Möglichkeit bieten, den Host wieder ans Laufen zu bringen, eine andere Konfiguration zu erzwingen, einen Port in der Firewall frei zu bekommen oder auch eine hängende VM abzuschießen.

Für viele Arbeiten in den Konfigurationsdateien des Hosts braucht man einen Editor. Beim ESXi gibt es dafür über die direkte Konsole nur den vi. Alternativ kann man aber auch per Remote-Software über die grafische Oberfläche des Betriebssystems mit integrierten Editoren arbeiten, z.B. unter Windows mit WinSCP.

Möchten Sie beim ESXi direkt auf der Kommandozeile arbeiten, müssen Sie diese Funktion meist erst freischalten:

1. Drücken Sie am Host die Funktionstaste F2 (Customize System) und melden Sie sich als *root* dort an.
2. Gehen Sie mit den Pfeiltasten zu dem Text Troubleshooting Options und drücken Sie Enter.
3. Wenn der erste Eintrag DISABLE ESXi SHELL heißt, können Sie sich bereits auf der Kommandozeile anmelden. Heißt der erste Eintrag aber ENABLE ESXi SHELL, dann wählen Sie ihn aus und drücken Enter, um umzuschalten.
4. Drücken Sie zweimal Esc, um zum Ausgangsbildschirm zurückzugelangen.

Jetzt können Sie sich per Remote mit einem Tool oder über die Tastenfunktion Alt+F1 mit der Shell (Kommandozeileninterpreter) verbinden. Für alle Linux-Fans: Eine echte Shell gibt es hier nicht – die eingetragene Shell */bin/sh* ist in Wirklichkeit die BusyBox (*/bin/busybox*).

# Der Standardeditor vi

Der Editor *vi* ist klein und sehr schwer zu bedienen; dennoch erfreut er sich großer Beliebtheit, da er auf nahezu jedem Unix- und Linux-System zu finden ist und in jedem Terminal läuft (ähnlich wie früher EDLIN von DOS). Meist ist der *vi* über die Umgebungsvariable `$EDITOR` als Default-Editor eingetragen. Daher begegnet man ihm immer wieder, zumal es im Allgemeinen heißt: »Wenn nichts mehr geht – *vi* geht immer.« Der *vi* wird von Linux-Distributionen aus lizenzrechtlichen Gründen nicht sehr häufig verwendet, stattdessen nutzt man *vim* (*Vi IMproved*), der alle Eigenschaften des *vi* besitzt und ihn unter anderem durch wertvolle Verbesserungen wie Tabbing erweitert.

*vi* ist ein Texteditor, der unter anderem folgende Optionen bietet: mehrfaches Rückgängigmachen von Eingaben, mehrere Fenster und Buffer, automatische Vervollständigung von Dateinamen, Onlinehilfen, visuelle Hervorhebung von markierten Texten, Speicherung und Abruf eingegebener Befehle und Kommandos, Editieren von binären Dateien usw. Für weitere Informationen empfehle ich Ihnen das Buch »*vi*-Editor – kurz & gut« von Arnold Robbins, ISBN 978-3-89721-213-8, ebenfalls erschienen im O'Reilly Verlag.

Der bei unserem System eingesetzte Editor ist allerdings nicht der echte *vi*, sondern auch nur wieder ein Verweis auf `/bin/busybox`. Deshalb funktioniert hier auch nicht alles so, wie man es eventuell gewohnt ist. Ich bleibe der Einfachheit halber trotzdem bei der Bezeichnung *vi*.

## Befehle von vi

Dieser Editor lässt sich nicht intuitiv bedienen – wenn man die Tastenkürzel nicht kennt, ist man hoffnungslos verloren. Zunächst muss man wissen, dass der normale *vi* drei verschiedene Modi besitzt:

1. Im Befehlsmodus (*command mode*) wird jede Eingabe als Befehl bzw. Kommando interpretiert. Das ist der Standardmodus beim Starten. Durch den Befehl `c` (wie »command«) gelangt man in diesen Modus.
2. Der Einfügemodus (*insert mode*) lässt Texteingaben zu.
3. Der Komplexbefehlsmodus (*last line mode*) stellt den Befehlsmodus zur Verfügung, damit in der letzten Zeile die Befehle editiert werden können

Die wichtigsten Tastenkürzel sind in Tabelle 9-1 dargestellt:

Tabelle 9-1: Nützliche Kurzbefehle des *vi*-Editors

| Taste    | Funktion                              |
|----------|---------------------------------------|
| i, Einfg | wechselt in den Einfügemodus (insert) |
| Esc      | beendet den Einfügemodus              |
| h        | Cursorbewegung nach links             |
| l (L)    | Cursorbewegung nach rechts            |



Tabelle 9-1: Nützliche Kurzbefehle des vi-Editors (Fortsetzung)

| Taste | Funktion                                               |
|-------|--------------------------------------------------------|
| j     | Cursorbewegung nach unten                              |
| k     | Cursorbewegung nach oben                               |
| x     | löscht ein Zeichen                                     |
| dd    | löscht die aktuelle Zeile                              |
| p     | gelöschte Zeile an der Cursorposition einfügen (paste) |
| u     | Rückgängig machen (undo)                               |
| :     | wechselt in den Komplexbefehlsmodus                    |

Im Komplexbefehlsmodus hat man wiederum u. a. die in Tabelle 9-2 zusammengefassten Tasten zur Auswahl:

Tabelle 9-2: Wichtige Befehle, um zum Beispiel den vi wieder zu verlassen

|         |                                                 |
|---------|-------------------------------------------------|
| :w Name | speichert die Datei unter dem Namen <i>Name</i> |
| :wq     | speichert die Änderungen und beendet den vi     |
| :q!     | beendet den vi, ohne zu speichern               |
| :help   | startet eine Onlinehilfe                        |

Im vi kann man auch die normalen Cursortasten sowie Pos1, Ende und Tab benutzen. Mit der Taste Einfg kann man – wie bei DOS-Editoren auch – zwischen dem Einfüge- und dem Überschreibmodus wechseln. Der aktuelle Modus wird dabei in der letzten Zeile vor dem Dateinamen angezeigt: I = Einfügemodus, R = Überschreibmodus. Die Entf-Taste können Sie nicht benutzen, Sie müssen also mit der Pfeiltaste nach rechts gehen und dann die Backspace-Taste nehmen. Bild nach oben und Bild nach unten funktionieren nicht wie unter anderen Editoren.

Aus der Hilfestellung und dem Editor kommt man übrigens mit folgender Tastenkombination wieder heraus: Esc, :, q, !, Enter.

## Dienste und Konfigurationsdateien

Auf der Kommandozeile des Hosts kann man Einfluss auf einige Dienste nehmen, die üblicherweise durch Konfigurationsdateien festgelegt sind. Dazu gehören

1. Namensauflösung,
2. Login-Konfigurationen,
3. VMkernel-Konfigurationen,
4. Logdatei-Einstellungen und
5. Zeiteinstellungen, z.B. für NTP.

Da die Konfigurationen der Dienste jeweils aus Dateien nur beim Start des Diensts abgerufen werden, muss der jeweilige Daemon hinterher neu gestartet werden, damit die Änderungen übernommen und in der grafischen Oberfläche angezeigt werden. Auch das lässt sich einfach auf der Kommandozeile mit dem Befehl `<Dienst> restart` bewerkstelligen. Manchmal ist dafür die gesamte Pfadangabe zum Dienst notwendig.

## Namensauflösung

Viele Einstellungen im vCenter Server funktionieren nur, wenn sich die ESXi Server untereinander finden und der VCS ebenfalls darauf Zugriff hat. Eines der wichtigsten Dinge für DRS, HA und vMotion ist die Namensauflösung, die nur bei korrekt eingestelltem DNS oder konfigurierter Hosts-Datei funktioniert. Auf DNS kann man sich hier leider nicht immer verlassen, da es sich bei den Hosts ja nicht um Windows-Maschinen handelt!

Die Datei `/etc/nsswitch.conf` ist unter anderem für die IP- und Namensauflösung verantwortlich. Dort finden Sie als Standardeintrag die Zeile `hosts: files dns`. Das bedeutet, dass zunächst in einer lokalen Datei namens `/etc/hosts` nach Einträgen gesucht werden soll. Wird dort nichts gefunden, versucht der ESXi Server als Nächstes, in DNS eine Auflösung zu machen. Die Konfigurationsdatei für DNS wiederum ist `/etc/resolv.conf`, die bei der Installation nach Ihren Angaben erstellt wird. Darin steht z. B. die Arbeitsgruppe oder Domäne als Suchsuffix und die Information darüber, welcher DNS-Server für diesen Bereich zuständig ist:

```
[root@esx1]# less /etc/
nameserver 192.168.50.50
nameserver resolv.conf192.168.50.10
search cssv.dom
```

Die Datei `/etc/hosts` sollte Namen und IP-Adressen der beteiligten ESXi Server und des vCenter Servers enthalten, um sicherzugehen, dass DNS-Probleme nicht zu einer Fehlermeldung oder dem Abbruch von DRS, HA und VMotion führt:

```
[root@esx1]# less /etc/hosts
127.0.0.1 localhost
::1
192.168.50.51 esx1.cssv.dom esx1
192.168.50.52 esx2.cssv.dom esx2
192.168.50.53 esx3.cssv.dom esx3
192.168.50.54 esx4.cssv.dom esx4
192.168.50.50 vcs.cssv.dom vcs
```

Gegebenenfalls kann über VMware HA noch ein Eintrag hinzugefügt werden, falls die bestehenden Einträge nicht ausreichen.



Laut Konvention sollten die Namen kleingeschrieben werden. Beachten Sie, dass unter Unix und Linux zwischen Klein- und Großschreibung unterschieden wird! Allerdings ist es in der Datei `hosts` tatsächlich egal.

## Userlogin

Es gibt viele Möglichkeiten, sich auf einem ESXi Server anzumelden: über den vSphere Client, über die direkte Konsole und über einen SSH-Client wie putty oder WinSCP.

Der direkte Zugriff über den vSphere Client wird über einen *TCP Wrapper* zur Verfügung gestellt, SSH benutzt den *sshd*-Daemon, der wiederum über die Datei */etc/ssh/sshd\_config* konfiguriert ist. Dort sind allerdings einige Zeilen auskommentiert. Das ist ein Hinweis darauf, dass die Standardeinstellungen verwendet werden. Beispielsweise ist der Port, über den auf ssh gelauscht wird, üblicherweise Port 22. In der Datei ist die Zeile aber nicht aktiv: *#Port 22*. Nur wenn man sich über einen anderen Port verbinden möchte, muss man hier die Einstellung z.B. auf Port 23 ändern.

Möchte man sich nicht immer mit einem Usernamen anmelden und anschließend dann su – und erneut das Passwort eintippen müssen, kann man das *no* in der Zeile *PermitRootLogin no* in ein *yes* ändern und den *sshd*-Dienst neu starten.

```
[root@esx1]# /etc/init.d/SSH restart
SSH login disabled
SSH login enabled
```

Die User-Accounts findet man in der Datei */etc/passwd*, deren Passwörter verschlüsselt in */etc/shadow* abgelegt sind. Die Einstellungen für das notwendige Passwort befinden sich in der Datei *passwd* im Verzeichnis */etc/pam.d*. In der dritten Zeile steht am Ende u.a. der Eintrag *min=8,8,8,7,6*. Dabei bedeutet der erste Eintrag die Minimallänge des Passworts, wenn nur eine Zeichenart verwendet wird. Die zweite Zahl ist die minimale Länge bei Verwendung von zwei der Möglichkeiten, wobei der erste Großbuchstabe nicht zählt (Passwort weist also nur eine Zeichenart auf, PassWort zwei). Der dritte Wert gibt die Minimallänge einer Passphrase aus mindestens drei Wörtern an; der vierte und der fünfte Eintrag beschreiben die Mindestlänge bei drei bzw. vier verwendeten Zeichencodes. Die angegeben fünf Werte müssen absteigend oder gleich sein.

Um die Passwortlänge zu reduzieren, kann man also z.B. den Eintrag auf *min=6,6,6,6,6* ändern. Zum Ausschalten der Komplexität können Sie zusätzlich noch den Eintrag *enforce=none* anhängen. Die Änderungen können mit dem *vi* vorgenommen werden. Ein anderer Editor wird auf der i-Version nicht angeboten.

*Vorgehensweise:*

1. Um sich auf der Konsole anmelden zu können, müssen Sie zunächst bei der Konfiguration die »Troubleshooting Mode Options« ändern. Wollen Sie sich direkt am ESXi Server anmelden, wählen Sie mit den Pfeiltasten den Eintrag *ENABLE ESXI SHELL* aus und drücken Return.
2. Drücken Sie die Tastenkombination *Alt+F1*, um auf die erste Konsole zu kommen.
3. Geben Sie das Passwort des Users *root* ein und drücken erneut Enter.
4. Da es hier ja nur den *vi* gibt, geben Sie an der Position, an der Sie sich befinden, *vi /etc/pam.d/passwd* ein und drücken Sie Enter.

5. Gehen Sie mit den Pfeiltasten in die dritte Zeile und dann nach rechts, bis Sie den Eintrag ... `retry=3 min=` ... sehen. Drücken Sie `Einf`g und ergänzen Sie den Eintrag wie oben beschrieben oder ändern ihn entsprechend ab.
6. Drücken Sie `Esc` und anschließend `:wq` zum Speichern und Verlassen des Editors.
7. Sie brauchen weiter nichts zu veranlassen, denn diese Änderung wirkt bei der nächsten Anmeldung auf der Konsole sofort.

## Die Kernel-Konfigurationsdatei

Die Hauptkonfiguration für den VMware Kernel findet sich in der Datei `/etc/vmware/esx.conf`. Mit einem normalen Texteditor können Sie sich diese Datei ansehen und bearbeiten. Auch die Geräte, auf die der Kernel zugreift, sind dort aufgelistet. Die Datei enthält also Einstellungen für die Hardware, die zu ladenden Module (ähnlich wie die DLLs für Windows) und die Boot-, Laufwerk- und Netzwerkkonfiguration. In Version 2.x gab es dazu noch mehrere einzelne Dateien, die ab Version 3 hier zusammengefasst sind. Über den vSphere Client können Einstellungen zu dieser Datei auch indirekt verändert werden.

Da hier das Herzstück des ESXi Kernels liegt, ist es sicher eine gute Idee, diese Datei vor Änderungen woanders abzuspeichern.

Für Änderungen über die Kommandozeile empfiehlt sich das Tool `esxcfg-advcfg`. Die wichtigsten Schalter dieser Anwendung sind `-g` für »get« und `-s` für »set«.

```
[root@esx35-1]# esxcfg-advcfg -g Wert
Beispiel: esxcfg-advcfg -g /Misc/HostName
Ausgabe: Value of HostName is esx5.cssv.de
[root@esx35-1]# esxcfg-advcfg -s Wert
```

Änderungen, die Sie über den vSphere Client in den erweiterten Einstellungen des Hosts machen, werden typischerweise am Anfang dieser Datei aufgelistet. Sie brauchen diese Zeilen nur komplett zu löschen und den Host neu zu starten, dann haben Sie wieder die Standardeinstellungen geladen.

## Logdatei-Protokollierung

Zuständig für die Protokollierung ist der Daemon `vm syslogd`, über den auch Speicherort und Größe der Dateien eingestellt werden und festgelegt wird, wie viele aufgehoben werden sollen. Das können Sie über den vSphere Client unter KONFIGURATION → ERWEITERTE EINSTELLUNGEN → SYSLOG einrichten. Die Änderungen, die Sie hier vornehmen, landen in der Datei `/etc/vmsyslog.conf.d/vpxa.conf`.

Nachdem der Host zum vCenter Server hinzugefügt wurde, werden zusätzliche Dateien für die Fehlersuche angelegt. Diese finden Sie z.B. unter `/scratch/log/`, was wiederum (meistens) ein Link auf ein VMFS-Volume ist. Die dortigen Logdateien entsprechen dem obigen Beispiel. Die Datei `/var/log/vpxa.log`, die auch schon vorher existiert, zeigt als Link immer auf die aktuelle Logdatei im Ordner `/scratch/log/`, diese entspricht auf der Win-

dows-Seite ungefähr der Datei *vpv-index*. Die Logdateien heißen auf dem ESXi Server *vpv-n.log*, wobei *n* wieder fortlaufende Zahlen sein können.

Weiterhin existieren auf dem ESXi Server im selben Ordner wie die Datei */etc/vmsyslog.conf*, *d/vpv.conf*, in der man die Einstellungen für das Protokollieren vornehmen kann, auch einige weitere *.conf*-Dateien für die Protokollierung, die ähnlich aufgebaut sind, z.B. *des VMkernels*.

Eine HTML-basierte Datei finden Sie unter */etc/vmware/vpv/* – sehen Sie sich ihren Inhalt an: Dort ist z.B. festgelegt, welche Informationen (Level) abgespeichert werden. Der Standardwert *verbose* kann auch folgende Werte annehmen: *trivia*, *info*, *warning*, *error* oder *none*.

Der Wert *maxFileSize* liegt üblicherweise bei 1.048.576, was einem MByte entspricht, der Wert für *maxFileNum* liegt normalerweise bei 10. Das muss aber nicht unbedingt in der Datei stehen, da es sich dabei um Standardwerte handelt.

Die Informationen zum Host werden in verschiedenen Logdateien auf dem System selbst im Verzeichnis */var/log* abgespeichert. Sehen Sie sich die Dateien *vmkeventd*, *vmkernel*, *vmkwarning* und *hostd.log* z.B. mit dem Programm *less* an:

```
less /var/log/vmkernel
```

## Der NTP-Client

Wie bereits erwähnt, sollten Sie die Zeit und das Datum auf den ESXi Servern aktuell halten. Ansonsten haben die VMs beim Starten eine falsche Zeit oder ein falsches Datum, und die Informationen in den Logdateien lassen sich nur schwer einordnen. Eine gute Möglichkeit zur korrekten Einstellung der Zeit ist die Konfiguration des *Network Time Protocol* (NTP), die über den vSphere Client (siehe Abbildung 9-1) oder die Kommandozeile erfolgen kann.



Abbildung 9-1: NTP-Zeiteinstellungen

Den aktuellen Status sehen Sie auf der ESXi-Registerkarte KONFIGURATION. Klicken Sie im Abschnitt SOFTWARE auf UHRZEITKONFIGURATION. Abbildung 9-2 zeigt, woran Sie erkennen können, wenn der Dienst nicht eingerichtet oder fehlerhaft ist.

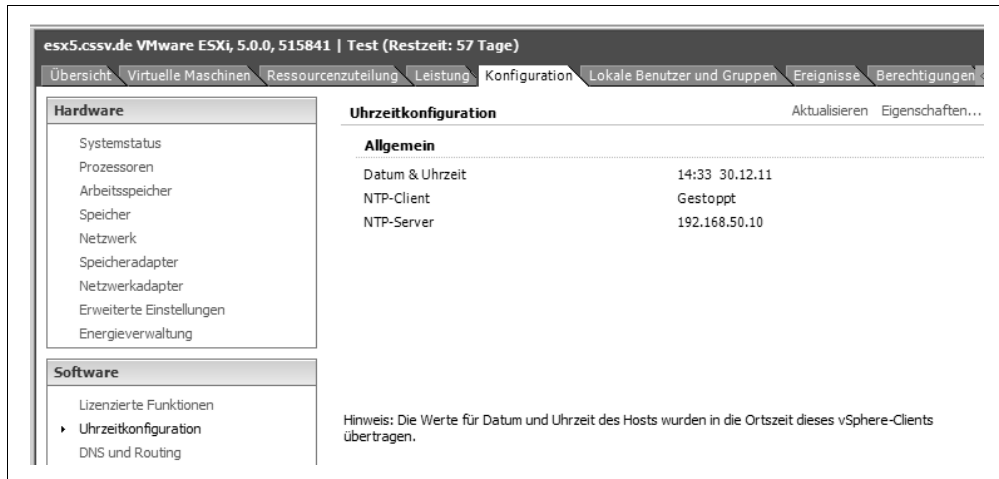


Abbildung 9-2: NTP-Konfiguration

Beachten Sie dabei, dass die Firewall den UDP-Port 123 geöffnet haben muss, was normalerweise automatisch abläuft. Falls nicht, öffnen Sie den Port, und üblicherweise wird der NTP-Client automatisch gestartet (ab Version 3.5).

Über die Eingabeaufforderung können Firewall-Einstellungen in der Datei `/etc/vmware/firewall/service.xml` konfiguriert werden. Dabei können vordefinierte Dienste wie `ntpClient` verändert oder auch beliebige andere definiert werden. Die Einstellungen zu diesem Dienst finden Sie bei der ID 0007. Folgende Zeilen sind dort standardmäßig enthalten:

```
<service id='0007'>
 <id>ntpClient</id>
 <rule>
 <direction>outbound</direction>
 <protocol>udp</protocol>
 <porttype>dst</porttype>
 <port>123</port>
 </rule>
 <enabled>false</enabled>
 <required>false</required>
</service>
```

Sind Sie mit den Änderungen fertig, müssen Sie noch die Firewall aktualisieren. Das können Sie auf der Kommandozeile mit folgendem Befehl tun:

```
esxcli network firewall refresh
```

Über den vSphere Client sehen Sie die Änderungen anschließend erst, nachdem Sie auch hier auf AKTUALISIEREN geklickt haben.

Sollte der NTP-Dienst nicht automatisch starten, erreichen Sie das mit folgender Eingabe:

```
/etc/init.d/ntpd start
```

Die eigentliche Konfiguration des NTP-Clients befindet sich in der Datei */etc/ntp.conf*. Diese können Sie mit dem vi ganz normal editieren und den Dienst anschließend neu starten über

```
/etc/init.d/ntpd restart
```

Die Änderungen sehen Sie hinterher auch über den vSphere Client.

## Ansichten der GUI aktualisieren

Bei Änderungen auf der Kommandozeile eines ESXi-Hosts spiegelt sich die Aktualisierung im vCenter Server nicht (bzw. nicht immer sofort) wider. Man kann in der grafischen Oberfläche den REFRESH-Button anklicken oder sich neu mit dem vSC (vSphere Client) anmelden. Helfen beide Vorgehensweisen nicht, muss man den Servicedienst neu starten:

```
[root@esx1]# /etc/init.d/vpxa restart
watchdog-vpxa: Terminating watchdog process with PID 3041
vpxa stopped.
vpxa is running
```

und

```
[root@esx1]# /etc/init.d/hostd restart
watchdog-vpxa: Terminating watchdog process with PID 2848
hostd stopped.
hostd started.
```

Der erste Befehl startet den vCenter Server-Agenten, der zweite den VMware Daemon *hostd* neu. Anschließend werden die jeweiligen aktuellen Daten angezeigt. Dabei ist es normal, dass der vSphere Client kurzfristig den Server verliert.

## Updates und Patches manuell einspielen

VMware stellt auf seiner Internetseite in unregelmäßigen Abständen Patches und Updates für die Aktualisierung seiner Produkte bereit. Die Vorgehensweisen zum Einspielen dieser Aktualisierungen sind jedoch unterschiedlich.

Sie können sich bei VMware über die Internetseite per Mail auch benachrichtigen lassen, wenn neue Patches und Updates zur Verfügung stehen:

<http://support.vmware.com/selfsupport/subscription/>

## Patches

Die zum Download angebotenen Patches vom selben Datum werden nach ihrer Art und Verwendung nochmals unterschieden in Patches für den ESXi Server (*Critical*, *Security* und *General*) sowie für den vCenter Server.

Auf der Internetseite <http://www.vmware.com/patchmgr/download.portal/> können Sie die Dateien für Ihr System heraussuchen, herunterladen und anschließend einspielen.

Für das vCenter werden nach dem Anklicken des blauen Links weitere Informationen (auf Englisch) angezeigt. Dabei ist zu beachten, dass gegebenenfalls vor der Installierung noch einige vorbereitende Schritte nötig sein können, z.B. für den Anschluss an eine Datenbank.

Für den ESXi Server werden Patches als *.zip*-Dateien angeboten. Nach dem Herunterladen von einem Windows-PC aus müssen diese zunächst entpackt und dem ESXi Server zur Verfügung gestellt werden. Das kann man z.B. mit dem Datastore-Browser oder WinSCP machen. Es wird empfohlen, die Patches und Updates zentral in einem Unterverzeichnis *updates* in dem Verzeichnis */var* abzulegen, mit *md5sum* zu überprüfen und von dort aus auszupacken und zu installieren.

Im folgenden Beispiel nehme ich ein neues Verzeichnis auf dem VMFS-Datastore und portiere die Dateien dort hin. Ich wähle extra diesen Weg, weil auf dem Volume meist mehr Platz ist als im Verzeichnis */var* und weil dieses einfacher von einem anderen Rechner aus zu steuern ist. Anschließend muss auf der Kommandozeile folgender Befehl ausgeführt werden:

```
esxcli software vib update -d <Pfad zur index.xml Datei>
```

Also zum Beispiel

```
esxcli software vib update -d /vmfs/volumes/esx5-datastore1/Updates/
```

Anschließend sollten Sie diese Meldung bekommen:

Message:

```
The update completed successfully, but the system needs to be rebooted for the changes to be effective.
```

Starten Sie den Host neu, indem Sie auf der Kommandozeile *reboot* eingeben. Anschließend werden noch einige Linux- und VMware-Befehle einschließlich Handhabung und Beispielen aufgeführt.



Seien Sie auf der Kommandozeile mit den *root*-Rechten besonders vorsichtig. Teilweise wird ohne Warnung der (vielleicht falsch) eingegebene Befehl ausgeführt!

## Die Kommandozeile, wichtige Dateien und Befehle

Da der ESXi Server auf der sogenannten BusyBox aufbaut, sind hier einige wenige Linux-Kommandos möglich. Die für die Arbeit wichtigen habe ich im Folgenden zusammengestellt.



## Kommandozeilenbefehle der ESXi Shell

Die folgenden Befehle sind direkt auf der Kommandozeile ausführbar. Ihr Ergebnis spiegelt nur die Standardbefehle wider. Im nächsten Abschnitt finden Sie die Befehle für den VMkernel, den eigentlichen Kern von VMware ESXi.

Beachten Sie bitte, dass viele Befehle nur vom *root*-Benutzer ausgeführt werden können und außerdem bei Linux-Systemen zwischen Klein- und Großbuchstaben unterschieden wird. Die Liste ist alphabetisch sortiert.

### *alias*

Zeigt alle Aliase an. Beispielsweise kann *cls* in *clear* umgewandelt werden: *alias cls=clear*. Anschließend können Sie die kürzere Schreibweise *cls* verwenden. Ein anderes Beispiel wäre *cdd="cd /vmfs/volumes/esx5-datastore1"*: Damit brauchen Sie nur noch *cdd* einzugeben und landen anschließend im VMFS-Volume des Rechners.

### *cat Datei*

Zeigt den Inhalt einer Datei an, ähnlich wie *type* in der DOS-Welt.

### *cd Verzeichnis*

Wechselt zum Verzeichnis. *cd /* wechselt zum *root*-Mountpoint, *cd ..* wechselt in das nächsthöhere Verzeichnis (achten Sie auf das Leerzeichen).

### *chgrp Gruppe Datei*

Ändert die Eigentümergruppe der Datei. Verzeichnisse werden wie bei *chown* abgeändert.

### *chmod Benutzer +-Berechtigung Datei*

Ändert die Berechtigung an einer Datei oder einem Verzeichnis. Mit *chmod -R* kann man wiederum ein Verzeichnis mit allen Unterverzeichnissen und Dateien ändern. Die Berechtigung wird entweder oktal (1 = ausführen, 2 = schreiben, 4 = lesen) oder als Buchstabe (*r* = lesen, *w* = schreiben, *x* = ausführen) angegeben. Diese Berechtigung ist dreigeteilt in Eigner, Eignergruppe und andere. *chmod +rwxrxx Datei* bedeutet beispielsweise Folgendes: Eigner darf alles, Eignergruppe darf lesen und ausführen, und andere dürfen nur ausführen. Oktal lautet der Befehl *chmod 751 Datei*.

### *chown Benutzer : Gruppe Datei*

Ändert den Eigentümer der Datei. *chown -r root /root/vmware* ändert alle Dateien im Verzeichnis auf den Eigner *root*.

### *clear*

Dieser Befehl löscht den gerade sichtbaren Bildschirminhalt.

### *cp Quelle Ziel*

Kopiert eine oder mehrere Dateien. Dieser Befehl kann nicht zum Kopieren auf eine oder von einer VMFS-Partition genutzt werden. Dafür ist *vmkfstools* zuständig (siehe unten).

### *date -u MMDDhhmmYY*

Datum des Rechners einstellen. *-u* bedeutet UTC (koordinierte Weltzeit), *MM* Monat, *DD* Tag, *hh* Stunde, *mm* Minute, *YY* Jahr. Denken Sie daran, alle Zeitangaben zweistellig anzugeben, also für Januar z.B. 01.

`dd if=/dev/cdrom of=/Verzeichnis/Datei.iso bs=32k`

Dieser Befehl erstellt ein ISO-CD-Image aus der eingelegten CD und speichert es im angegebenen Verzeichnis unter dem angegebenen Dateinamen. Das ist besonders nützlich, da Sie mit ISO-Images besser arbeiten können als mit physischen CDs. Allerdings sollten Sie dabei beachten, dass keine Überprüfung des Image auf Richtigkeit stattfindet.

`df`

Zeigt die Speicherbelegung der Partitionen an. Mit `df -h` werden MBytes und GBytes statt Bytes angezeigt, um die Lesbarkeit zu verbessern.

`du Verzeichnis`

Zeigt die Plattenbelegung des aktuellen Verzeichnisses an.

`find Pfadname Dateiname`

Sucht im Pfad nach Dateien mit dem angegebenen Dateinamen. `-size` als Parameter sucht nach Dateien mit bestimmter Größe, `-mtime` nach Dateien mit einem bestimmten Erstellungsdatum.

`grep String`

Durchsucht einen Text nach einem Muster (String). Beispielsweise zeigt der Befehl `cat /etc/vmware/pcitable | grep Dell` die unterstützten PCI-Geräte von Dell an. Im Beispiel wird der Inhalt der Datei `pcitable` an `grep` weitergegeben und `grep` durchsucht diesen Inhalt nach `Dell` und gibt dann die gefundenen Zeilen aus.

`groupadd Gruppe`

Legt eine neue Gruppe an. Dieser Befehl ist veraltet, es sollte lieber `vim-cmd` dafür genutzt werden.

`gunzip Datei`

Entpackt die angegebene Datei.

`gzip Datei -best`

Packt eine Datei mit dem `gzip`-Verfahren. Nach dem Packen wird die Endung `.gz` an den Dateinamen angehängt.

`halt`

Dieser Befehl fährt das System herunter.

`head Datei`

Zeigt Ihnen die ersten zehn Zeilen einer Datei an. Mit `head -20 Datei` werden die ersten 20 Zeilen angezeigt.

`hostname`

Zeigt den Rechnernamen an. `hostname neuer_Rechnername` ändert den Rechnernamen des Systems, allerdings nur zur Laufzeit. Nach einem Reboot ist der alte Name wieder eingetragen.

`kill Prozess ID`

Beendet einen Prozess. `kill -9` beendet auch hartnäckigste Prozesse.

### *less Datei*

Zeigt den Inhalt einer Datei an und verbleibt an deren Ende. Man kann mit `Bild` nach oben und `q` nach unten die Seiten wechseln.

### *ls -la Pfad*

Dieser Befehl listet alle Dateien im Pfad auf. Wenn keine Pfadangabe gemacht wird, gilt das aktuelle Verzeichnis. Der Parameter `l` zeigt die Dateien mit Details an, `a` zeigt auch die versteckten Dateien an. `ls -la | more` oder `ls -la | less` führt dazu, dass die Dateien seitenweise angezeigt werden. `ls -ltr` zeigt Dateien und Verzeichnisse nach Datum und Uhrzeit sortiert an.

### *lsof*

Listet alle durch Prozesse geöffneten Dateien auf. `lsof -i` listet nur alle aktiven IP-Prozesse auf. Mit `lsof -i | grep vm1.vmx` bekommt man die Prozess-ID der VM `vm1` heraus. Mit `kill <ID>` kann man die VM hart abschalten, wenn es über die grafische Oberfläche mit dem vSphere Client nicht mehr möglich ist.

### *lspci*

Zeigt die PCI-Geräte des Hosts an.

### *md5sum*

Erstellt einen Hash-Wert mithilfe des md5-Algorithmus. Dieser Wert ist einmalig für eine Datei, jede Veränderung der Datei selbst hat also eine Änderung des Hash-Werts zur Folge. Bei jedem Download und beim Kopieren von sensiblen Dateien von oder zu einem Rechner sollten Sie die Hash-Werte beider Dateien überprüfen, um sich vor Veränderungen zu schützen. Veränderungen können durch einen fehlerhaften Kopierprozess oder durch absichtliche Manipulation entstehen.

### *mkdir Verzeichnis*

Erstellt ein Verzeichnis.

### *mv Quelle Ziel*

Verschiebt eine Datei oder ein Verzeichnis.

### *passwd Benutzer*

Ändert das Passwort des angegebenen Benutzers. Wird kein Benutzer angegeben, wird das Passwort des aktuellen Benutzers geändert.

### *ps*

Zeigt die Prozesse eines Systems mit ihrem Aufruf und der Prozess-ID an. `ps -t` listet alle Prozesse mit zugehörigem Typ auf. `ps -c` zeigt alle Prozesse detailliert an.

### *pwd*

Dieser Befehl zeigt das aktuelle Verzeichnis an. Mit `export PS1='[\u@\h \w]\$ '` bekommt man auch den ganzen Pfad angezeigt. Diese Einstellung gilt nur für die aktuelle Sitzung. Möchten Sie den Pfad immer haben, muss er in die »Konfigurationsanmeldedatei« `profile` im Verzeichnis `/etc/` eingetragen werden (achten Sie auf die Kleinschreibung des Buchstaben »w«). Hier können Sie auch Aliase eintragen, die dann beim nächsten Anmelden wieder gültig sind.

## reboot

Neustart des Systems. Unter VMware ESX 2.5 werden standardmäßig alle laufenden virtuellen Maschinen automatisch durch die VMware Tools heruntergefahren; ab Version 3 geschieht das nur, wenn Sie es explizit eingestellt haben.

## rm *Datei*

Löscht eine Datei. `rm -r Verzeichnis` löscht ein Verzeichnis mit allen darin enthaltenen Dateien. Da bei VMware ESX `rm` ein Alias auf `rm -i` ist, wird bei jeder Datei nachgefragt, ob Sie sie wirklich löschen wollen. Bei Verzeichnissen mit vielen Dateien oder Unterverzeichnissen kann das lästig sein. In diesem Fall können Sie einfach `/bin/rm -r Verzeichnis` eingeben, und Sie werden nicht mehr gefragt. Verwenden Sie diesen Befehl bitte nur, wenn Sie sich über Ihr Tun im Klaren sind, da man gelöschte Dateien nicht mehr so ohne Weiteres wieder herbeizaubern kann.

## rmdir *Verzeichnis*

Löscht ein leeres Verzeichnis.

## scp *Quelle Benutzer@Host:Pfad*

Kopiert eine oder mehrere Dateien über *ssh* auf einen anderen Server. Das wird benötigt, wenn die ESX Server auf höchste Sicherheit eingestellt sind. Hier ein Beispiel: `scp /etc/inittab root@esxserver.testnetz.local:/root/` kopiert die Datei */etc/inittab* auf den ESX Server *esxserver.testnetz.local* ins Verzeichnis */root* unter Verwendung des *root*-Benutzers zum Verbindungsaufbau über das Netzwerk.

## set

Zeigt alle Systemvariablen an.

## su

Umschalten zum *root*-Benutzer. Es ist gängige Praxis, sich als normaler Benutzer ohne besondere Rechte anzumelden und mit *su* in die Root-Shell zu wechseln. Diese Shell wird mit *exit* verlassen. Mit `su -c Befehl` kann ein beliebiger Befehl mit Root-Rechten ausgeführt werden. Um als Benutzer *root* zu einer Shell mit normalen Benutzerrechten zu gelangen, muss einfach `su Benutzername` eingegeben werden. Möchte man sich z.B. über *ssh* (putty) direkt anmelden, ohne den Umweg über einen anderen User zu gehen, muss man die Datei */etc/ssh/sshd\_config* editieren, indem man in der Zeile mit *PermitRootLogin* *yes* einträgt und abspeichert. Das ist allerdings ein Sicherheitsrisiko! Um die Änderungen wirksam zu machen, muss der *ssh*-Dienst neu gestartet werden: `service sshd restart`.

## tail *Datei*

Zeigt Ihnen die letzten zehn Zeilen einer Datei an. Mit `tail -20 Datei` werden die letzten 20 Zeilen angezeigt.

## tar -czvf *Zieldatei Quelle*

Fasst die Quelldatei oder das Quellverzeichnis zu einer *.tar*-Datei zusammen und packt sie anschließend mit *gzip* *c* = create (erstellen), *z* = mit *gzip* packen, *v* = verbose (detaillierte Ausgabe), *f* = file.

`tar -xvzf Quelldatei`

Entpackt die Datei in das aktuelle Verzeichnis, x = extract (entpacken).

`touch Datei`

Verändert das Zugriffsdatum einer Datei, ohne den Inhalt zu verändern. Falls die Datei nicht existiert, wird sie neu erstellt.

`useradd Benutzer (-g Gruppe -d Heimatverzeichnis)`

Legt einen neuen Benutzer an. Wenn keine Gruppe und kein Heimatverzeichnis angegeben werden, wird eine neue Gruppe mit dem Benutzernamen erstellt, in der er Mitglied wird, und ein Heimatverzeichnis mit dem Benutzernamen unter */home*. Dieser Befehl ist veraltet, es sollte lieber `vim-cmd` dafür genutzt werden.

`userdel Benutzer`

Löscht den Benutzer vom System. Das Heimatverzeichnis wird allerdings nur gelöscht, wenn der Parameter `-r` mitgegeben wird. Dieser Befehl ist veraltet, es sollte lieber `vim-cmd` dafür genutzt werden.

`usermod Optionen Benutzer`

Ändert das Benutzerkonto. `-l` sperrt den Benutzer; `-g` ändert die primäre Gruppenzugehörigkeit und `-d` das Heimatverzeichnis. Dieser Befehl ist veraltet, es sollte lieber `vim-cmd` dafür genutzt werden.

`which Befehl`

Zeigt den Speicherort des angegebenen Befehls an.

`who`

Zeigt alle aktuell angemeldeten Benutzer des Systems an.

`whoami`

Zeigt den angemeldeten Benutzer an.

## Kommandozeilenbefehle des VMkernels

Diese Befehle werden auf der direkten Konsole ausgeführt, betreffen aber nur den VMware Kernel. Wieder folgen die Befehle in alphabetischer Reihenfolge:

`esxtop`

Wie `top`, allerdings mit allen Informationen zum VMkernel.

`vdf`

Wie `df`, zeigt allerdings auch die VMFS-Partitionen an. `vdf -h` macht das Ganze übersichtlicher. Sie sehen allerdings die wirklichen physischen Pfade zu den SCSI- oder Fibre-Channel-Platten und nicht den Friendly Name.

`vmkload_mod`

Verwaltet die geladenen Module des VMkernels. `vmkload_mod -l` zeigt die geladenen Kernel-Module an. `vmkload_mod -u Modulname` entlädt das Modul. `vmkload_mod Modulname pfad /Modulname.o` lädt das entsprechende Kernel-Modul.

## vm-support

Bei Problemen mit dem VMware ESXi Server kann man mit diesem Befehl die Datei *esx-<Datum>.id.tgz* erstellen, um sie anschließend dem VMware-Support zur Verfügung zu stellen. In dieser Datei stehen alle wichtigen Informationen des VMware ESXi Servers. Unter Umständen ist es empfehlenswert, diesen Befehl monatlich auszuführen und die ausgegebene Datei zu sichern.

## vmware-cmd

Mit dem folgenden Programm können Sie nur über die RCLI arbeiten. Dieser Befehl ist auf der direkten Konsole nicht vorhanden. Ein Ersatz, der hier verfügbar ist, ist das Tool *esxcli*, das weiter unten behandelt wird.

Mit *vmware-cmd* können Sie über die RemoteCLI sämtliche virtuellen Maschinen steuern! Ich gehe hier auf alle wichtigen Parameter ein. Einer der Parameter ist fast immer die Konfigurationsdatei, also die VMware-.*vmx*-Datei, z.B. */vmfs/volumes/storage1/Server1/server1.vmx*.

*vmware-cmd -l*

Gibt eine Liste aller registrierten virtuellen Maschinen aus.

*vmware-cmd -s register Konfig-Pfad/.vmx Datei*

Registriert eine virtuelle Maschine.

*vmware-cmd -s unregister Konfig-Pfad/.vmx Datei*

Löscht die Registrierung der virtuellen Maschine.

*vmware-cmd Konfig-Pfad/.vmx Datei getstate*

Zeigt den Status der virtuellen Maschine an.

*vmware-cmd Konfig-Pfad/.vmx Datei getpid*

Zeigt die Prozess-ID der virtuellen Maschine an.

*vmware-cmd Konfig-Pfad/.vmx Datei getid*

Zeigt die World-ID der virtuellen Maschine an.

*vmware-cmd Konfig-Pfad/.vmx Datei getuptime*

Zeigt die Laufzeit der virtuellen Maschine an. In diesem Zeitraum wurde diese virtuelle Maschine nicht abgeschaltet.

*vmware-cmd Konfig-Pfad/.vmx Datei getheartbeat*

Wenn Sie diesen Befehl zweimal hintereinander ausführen und das Ergebnis gleich ist, können Sie davon ausgehen, dass die virtuelle Maschine nicht mehr läuft.

*vmware-cmd Konfig-Pfad/.vmx Datei getremoteconnections*

Zeigt die Anzahl aller derzeitigen Remote-Console-Verbindungen an.

*vmware-cmd Konfig-Pfad/.vmx Datei answer*

Falls unbeantwortete Fragen anstehen, können sie mit diesem Befehl beantwortet werden. Wenn Sie beispielsweise eine virtuelle Maschine mit einer Festplatte im

nicht dauerhaften Modus haben, und beim Abschalten dieser Maschine (wie immer) gefragt werden, ob alle Änderungen zurückgeschrieben werden sollen – diese Frage könnten Sie dann mit dem Befehl beantworten.

```
vmware-cmd Konfig-Pfad/.vmx Datei [start | stop | reset | suspend] {soft | trysoft | hard }
```

Damit wird die virtuelle Maschine gestartet, beendet, neu gestartet oder vorübergehend stillgelegt. Der zweite Parameter gibt an, ob versucht wird, die Maschine über die VMware Tools normal herunterzufahren, oder ob sie einfach hart abgeschaltet werden soll. Der Mittelweg ist trysoft, womit erst versucht wird, die Maschine normal herunterzufahren. Sollte das innerhalb einer gewissen Zeit nicht funktionieren, wird einfach ausgeschaltet.

```
vmware-cmd Konfig-Pfad/.vmx Datei addredo Festplatte
```

Schaltet die Festplatte in den nicht dauerhaften Modus, alle Änderungen werden also nicht direkt auf die Festplatte, sondern in eine andere Datei geschrieben, das REDO-Log. Diese Festplatte muss mit ihrem physischen Namen und nicht mit dem Dateinamen der Festplattendatei angegeben werden. Dieser Name steht in der Konfigurationsdatei bzw. kann über die MUI ausgelesen werden.

Beispiel: `vmware-cmd /home/vmware/Server1/server1.vmx addredo scsi0:0.`

```
vmware-cmd Konfig-Pfad/.vmx Datei commit Festplatte
```

Schreibt alle Änderungen aus dem REDO-Log auf die Festplatte zurück und schaltet die Festplatte wieder in den ursprünglichen Modus. Darüber hinaus werden diese Änderungen beim Ausschalten der virtuellen Maschine zurückgeschrieben.

## vmkfstools

Dieser Befehl dient der Verwaltung der Festplattendateien virtueller Maschinen.

```
vmkfstools -c #[gGmMkK] Festplattendatei
```

Es wird eine neue Festplattendatei angelegt, die Sie in einer virtuellen Maschine nutzen können. `vmkfstools -c 10G /vmfs/local/server1.vmdk` legt eine Festplatte mit einer Größe von 10 GByte an. Denken Sie daran, dass diese Datei nur vom *root*-Benutzer eingerichtet werden kann. Soll der Zugriff auf diese Festplattendatei für andere freigegeben werden, müssen Sie später die Berechtigung mit `chown` abändern.

```
vmkfstools -C [vmfs3|vmfs5] -n ## vmhbaC:T:L:P
```

Formatiert eine Partition mit dem VMFS3-Dateisystem (mit VMFS kann auch noch das alte Dateisystemformat genutzt werden). *vmhba* steht für den SCSI-/Fibre-Channel-Adapter des VMkernels, C = Controller, T = SCSI Target, L = LUN Number, P = Partition. Beispiel: `vmkfstools -C vmfs3 vmhba0:0:0:1`. Mit dem Parameter `-n` kann zusätzlich die maximale Anzahl der möglichen Dateien festgelegt werden. Statt maximal 256 Dateien (Maximum über die MUI) kann die Formatierung hier mit bis zu 1.024 Dateien konfiguriert werden. Der letzte Wert ist vor allem in Verbindung mit

der Template-Ablage des vCenter Servers sinnvoll. Auch kann die Größe der Blöcke mit `-b` angegeben werden: `vmkfstools -C vmfs3 -b 2m vmhba1:3:0:1`.

`vmkfstools -e Ziel Quelle`

Exportiert eine VMware ESX-Festplattendatei in ein für VMware Server und VMware Workstation lesbares Format. Die Quelldatei muss auch im VMFS-Dateisystem liegen. Zudem wird die Quelldatei wieder in kleinere Dateien aufgesplittet.

`vmkfstools -E oldName newName`

Eine Virtual Disk wird mit diesem Befehl umbenannt.

`vmkfstools -g Festplattendatei`

Zeigt die Festplattengeometrie an, die unter Umständen für den Export wichtig sein kann.

`vmkfstools -i Quelle Ziel`

Importiert eine Festplattendatei von VMware Server oder VMware Workstation in eine VMware ESX-Festplattendatei. *Ziel* ist eine VMFS-Partition: `vmkfstools -i /vmimages/server1.vmdk /vmfs/local/server1.dsk`. Da die Quellfestplattendateien meist aus mehreren GByte Dateien bestehen, müssen Sie daran denken, nur die erste *.vmdk*-Datei anzugeben. Der Importvorgang fasst alle Dateien zu einer *.dsk*-Datei zusammen. Dieser Befehl kann auch zum Vervielfältigen von Festplattendateien (jeweils auf VMFS) genommen werden. Beachten Sie, dass heute standardmäßig die *.vmdk*-Datei und nicht die *.dsk*-Datei genutzt wird.

`vmkfstools -L reserve | release | targetreset | lunreset | busreset vmhbaC:T:L:P`

Dieser Befehl gilt hauptsächlich für Clusterszenarien. Angenommen, einer der Clustermitglieder stürzt ab und sperrt die LUN, können Sie mit `vmkfstools -L release vmhba0:0:0:1` die Sperre wieder aufheben.

`vmkfstools -P vmhbaC:T:L:P`

Zeigt detaillierte Informationen über die angegebene Partition an.

`vmkfstools -B Festplattendatei`

Sollte eine virtuelle Maschine abstürzen, kann es passieren, dass die Festplattendatei gesperrt ist. Mit diesem Befehl können Sie die Sperre aufheben.

`vmkfstools -S Label vmhbaC:T:L:P`

Um nicht immer mit den physischen Namen der Festplatten arbeiten zu müssen, können Sie mit diesem Befehl einen sogenannten »Friendly Name« vergeben. Beispiel: `vmkfstools -S VMFS-1 vmhba0:0:0:1`.

`vmkfstools -U /vmfs/local/server1.dsk`

Löscht die Dateien mit dem Namen der virtuellen Festplatte.

`vmkfstools -X #[gGmMkk] Festplattendatei`

Vergrößert eine Festplattendatei auf die angegebene (nicht zusätzliche) Größe. Danach wäre Ihre Festplattendatei mit hoher Wahrscheinlichkeit unbrauchbar. `vmkfstools -X 20G /vmfs/local/server1.vmdk` würde die Festplatte von Server1 auf 20 GByte vergrößern. Diese Vergrößerung hilft allerdings dem Betriebssystem erst ein-



mal überhaupt nicht. Sie müssen trotzdem mit einem Partitionstool an die Festplatte herangehen, um dieses Mehr an Speicherplatz nutzen zu können. Wird eine geringere Größe angegeben als die wirkliche Festplattengröße, kann sie durch die Angabe des Parameters `-force` auch verkleinert werden. Achten Sie darauf, dass Sie Snapshots der VM hinterher nicht mehr nutzen können! Eine bessere Möglichkeit zum Vergrößern und Verkleinern der Platten bietet der VMware Converter (siehe Kapitel 13, *VMware Update Manager und Converter*).

`vmkfstools -Z Erweiterungsgesetz existierendes_VMFS-Volumen`

Hiermit kann man ein Volumen vergrößern. Die Daten auf dem hinzuzufügenden Volumen werden dabei gelöscht, das bereits bestehende bleibt erhalten. Beispiel:  
`vmkfstools -Z /vmfs/devices/disks/vmhba0:1:2:1 /vmfs/devices/disk /vmhba1:3:0:1.`

## esxcfg-tools

Wenn Sie `esxcfg-` eingeben und anschließend zweimal die Tab-Taste drücken, können Sie noch weitere Konfigurationstools anzeigen lassen. Diese können meist mit dem Parameter `-h` oder `--help` aufgerufen werden.



Wenn die `esxcfg-*`-Befehle verwendet werden, sollten anschließend die Befehle `/etc/init.d/vpxa restart` und `/etc/init.d/hostd restart` ausgeführt werden, um den *vmware-hostd*-Prozess neu zu starten und Management-Tools wie dem vSphere Client mitzuteilen, dass sich die Konfiguration geändert hat.

### *esxcfg-advcfg*

Konfiguriert erweiterte Optionen für ESXi Server.

Um die erweiterten Optionen im vSphere Client zu konfigurieren, klicken Sie auf ERWEITERTE EINSTELLUNGEN. Wenn das Dialogfeld ERWEITERTE EINSTELLUNGEN geöffnet wird, verwenden Sie die Liste auf der linken Seite, um den Gerätetyp oder die Aktivität auszuwählen, mit dem/der Sie arbeiten möchten, und nehmen die entsprechenden Einstellungen vor.

### *esxcfg-dumppart*

Konfiguriert eine Diagnosepartition oder sucht nach bestehenden Diagnosepartitionen.

Bei der Installation von ESXi Server wird eine Diagnosepartition zur Speicherung von Informationen zur Fehlersuche erstellt, für den Fall dass ein Systemfehler auftritt. Sie müssen diese Partition nicht manuell anlegen, es sei denn, Sie stellen fest, dass es keine Diagnosepartition für den Host gibt. Für Diagnosepartitionen stehen im vSphere Client folgende Verwaltungsvorgänge zur Verfügung:

- *Überprüfung des Vorhandenseins einer Diagnosepartition* – Klicken Sie auf STORAGE (SPEICHER) → HINZUFÜGEN und sehen auf der ersten Seite des Assistenten zum Hinzufügen von Speicher nach, ob die Option DIAGNOSE aufgeführt wird.

Wenn DIAGNOSE nicht zu den Optionen zählt, verfügt ESXi Server bereits über eine Diagnosepartition.

- *Konfiguration einer Diagnosepartition* – Klicken Sie auf SPEICHER → HINZUFÜGEN → DIAGNOSE und folgen Sie den Anweisungen des Assistenten.

#### *esxcfg-info*

Druckt Informationen zum Status der Servicekonsole, des VMkernels, verschiedener Untersysteme im virtuellen Netzwerk und der Speicherressourcenhardware aus.

Mit dem vSphere Client können diese Informationen nicht ausgedruckt werden, die meisten davon können jedoch über verschiedene Registerkarten und Funktionen in der Benutzeroberfläche eingesehen werden. So können Sie zum Beispiel den Status der virtuellen Maschinen auf der Registerkarte VIRTUELLE MASCHINEN überprüfen.

#### *esxcfg-init*

Führt interne Initialisierungsroutinen aus.

Dieser Befehl wird für den Bootstrap-Prozess verwendet, und Sie sollten ihn unter keinen Umständen ausführen. Dieser Befehl kann zu Problemen mit dem ESX Server-Host führen. Es gibt keine vSphere Client-Entsprechung für diesen Befehl.

#### *esxcfg-module*

Legt die Treiberparameter fest und stellt ein, welche Treiber während des Hochfahrens geladen werden.

Dieser Befehl wird für den Bootstrap-Prozess verwendet und ist nur für die technische Unterstützung von VMware vorgesehen. Geben Sie diesen Befehl nur auf ausdrückliche Anweisung eines Vertreters des technischen Supports von VMware ein. Es gibt keine vSphere Client-Entsprechung für diesen Befehl.

#### *esxcfg-mpath*

Konfiguriert die Multipath-Einstellungen für Fibre Channel- oder iSCSI-Festplatten.

Klicken Sie zur Konfiguration der Multipath-Einstellungen für den Speicher im vSphere Client auf SPEICHER. Wählen Sie einen Datastore oder eine zugeordnete LUN aus und klicken Sie auf EIGENSCHAFTEN. Wählen Sie gegebenenfalls im Dialogfeld EIGENSCHAFTEN die gewünschte Erweiterung aus. Klicken Sie dann auf BEREICHSGERÄT → PFADE VERWALTEN und konfigurieren Sie die Pfade über das Dialogfeld PFAD VERWALTEN.

#### *esxcfg-nas*

Verwaltet die NAS-Einbindung.

Mit diesem Befehl können Sie NAS-Geräte hinzufügen, löschen und auflisten sowie ihre Attribute ändern. Klicken Sie zur Anzeige der NAS-Geräte im vSphere Client auf SPEICHER und blättern Sie durch das Speicherverzeichnis. In der SPEICHER-Ansicht können Sie außerdem folgende Vorgänge ausführen:

- *Attribute eines NAS-Geräts anzeigen* – Markieren Sie das Gerät. Sie erhalten die Daten unter DETAILS.
- *Hinzufügen eines NAS-Geräts* – Klicken Sie auf SPEICHER HINZUFÜGEN.
- *Löschen eines NAS-Geräts* – Klicken Sie auf ENTFERNEN.
- *Änderung der Attribute eines NAS-Geräts* – Klicken Sie auf das Gerät und dann auf DETAILS → EIGENSCHAFTEN.

#### *esxcfg-nics*

Druckt ein Verzeichnis der physischen Netzwerkadapter sowie Informationen zum Treiber, dem PCI-Gerät und dem Verbindungsstatus jeder NIC.

Sie können diesen Befehl auch verwenden, um die Geschwindigkeit und den Duplexmodus eines physischen Netzwerkadapters zu steuern. Die Informationen zu den physischen Netzwerkadapters des Hosts können Sie im vSphere Client anzeigen, indem Sie auf NETWORK ADAPTERS (NETZWERKADAPTER) klicken. Klicken Sie zur Änderung der Geschwindigkeit und des Duplexmodus für einen physischen Netzwerkadapter im vSphere Client bei einem virtuellen Switch, der dem physischen Netzwerkadapter zugeordnet wurde, auf NETZWERK → EIGENSCHAFTEN. Klicken Sie dann im Dialogfeld EIGENSCHAFTEN auf NETWORK ADAPTERS (NETZWERKADAPTER) → BEARBEITEN und wählen Sie GESCHWINDIGKEIT/DUPLEX aus.

#### *esxcfg-resgrp*

Stellt die Ressourcengruppeneinstellungen wieder her und ermöglicht die Ausführung grundlegender Verwaltungsaufgaben für Ressourcengruppen.

Wählen Sie einen Ressourcenpool aus dem Inventarfenster aus und klicken Sie in der ÜBERSICHT-Registerkarte auf EINSTELLUNGEN BEARBEITEN, um die Einstellungen der Ressourcengruppe zu ändern.

#### *esxcfg-route*

Legt die Standardgateway-Route des VMkernels fest oder ändert sie.

Um die Standardgateway-Route des VMkernels im vSphere Client festzulegen, klicken Sie auf DNS UND ROUTING. Wenn Sie die Standardroute ändern möchten, klicken Sie auf EIGENSCHAFTEN und aktualisieren die Daten auf beiden Registerkarten im Dialogfeld DNS- UND ROUTING-KONFIGURATION.

#### *esxcfg-swiscsi*

Konfiguriert den iSCSI-Softwareadapter.

Klicken Sie zur Konfiguration des Software-iSCSI-Systems im vSphere Client auf SPEICHERADAPTER, markieren Sie den iSCSI-Adapter, den Sie konfigurieren möchten, und klicken Sie auf EIGENSCHAFTEN. Konfigurieren Sie den Adapter über das Dialogfeld EIGENSCHAFTEN DES iSCSI-INITIATORS.

#### *esxcfg-vmknics*

Erstellt und aktualisiert VMkernel-TCP/IP-Einstellungen für VMotion, NAS und iSCSI.

Klicken Sie zur Einrichtung von Netzwerkverbindungen von VMotion, NFS oder iSCSI im vSphere Client auf NETZWERK → VERWALTEN. Wählen Sie VMKERNEL aus und folgen Sie den Anweisungen des Assistenten zum Hinzufügen von Netzwerken. Definieren Sie IP-Adresse, Subnetzmaske und das VMkernel-Standardgateway im Schritt VERBINDUNGSEINSTELLUNGEN.

Wenn Sie die Einstellungen überprüfen möchten, klicken Sie auf das blaue Symbol links neben dem VMotion-, iSCSI- oder NFS-Port. Möchten Sie eine der Einstellungen bearbeiten, klicken Sie für den entsprechenden Switch auf EIGENSCHAFTEN. Wählen Sie den Port aus dem Verzeichnis im Dialogfeld EIGENSCHAFTEN aus und klicken Sie auf EIGENSCHAFTEN, um das EIGENSCHAFTEN-Dialogfeld zum Port zu öffnen und die Einstellungen für den Port zu ändern.

#### *esxcfg-vswitch*

Erstellt und aktualisiert die Netzwerkeinstellungen für virtuelle Maschinen.

Klicken Sie zur Einrichtung von Netzwerkverbindungen für eine virtuelle Maschine im vSphere Client auf NETZWERK → VERWALTEN. Wählen Sie VIRTUELLE MASCHINE aus und folgen Sie den Anweisungen des Assistenten zum Hinzufügen von Netzwerken. Wenn Sie die Einstellungen überprüfen möchten, klicken Sie auf das Sprechblasensymbol links von der gewünschten Portgruppe der virtuellen Maschine. Möchten Sie eine der Einstellungen bearbeiten, klicken Sie für den entsprechenden Switch auf EIGENSCHAFTEN. Wählen Sie den Port der virtuellen Maschine aus dem Verzeichnis im Dialogfeld EIGENSCHAFTEN aus und klicken Sie auf BEARBEITEN, um das Dialogfeld PORT EIGENSCHAFTEN zu öffnen und dessen Einstellungen zu ändern.

Folgende weitere *esxcfg*- Befehle gibt es auf der Kommandozeile:

#### *esxcfg-fcoe*

Mit diesem Befehl kann Fibre Channel over Ethernet konfiguriert werden.

#### *esxcfg-hwiscsi*

Mit diesem Befehl können Hardware-iSCSI-Karten konfiguriert werden.

#### *esxcfg-ipsec*

Hiermit wird IPSec inklusive eventueller Zertifikate eingerichtet.

#### *esxcfg-rescan*

Um Hostbusadapter nach neuen Storages zu überprüfen, kann dieser Befehl genutzt werden.

#### *esxcfg-scsidevs*

Dieser Befehl kann für Listen der Beziehungen zwischen HBAs und Storages benutzt werden.

#### *esxcfg-volume*

Hiermit können eine VMFS3- in eine VMFS5-Partition aktualisiert sowie Snapshots und Replicas bearbeitet werden.

# Skripten

Die folgenden Skripten liegen alle im Verzeichnis */etc/init.d*. Die meisten davon kennen als Parameter *start*, *stop*, *restart*, *status* und *reload*. Die ersten vier Parameter bedürfen keiner Erklärung; *reload* bewirkt, dass der Prozess die Konfigurationsdateien neu einliest und mit den geänderten Parametern weiterläuft. Sie werden diese Skripten sehr selten benötigen, aber falls Sie versehentlich einmal einen Prozess beenden oder einer der Prozesse abstürzt, können Sie an dieser Stelle nachsehen, wie das Skript heißt, das Sie dann mit dem Parameter *start* einfach neu aufrufen müssen.

Ich habe hier nicht alle vorhandenen Skripten aufgeführt, weil einige auch im Buch besprochen werden oder nicht so wichtig sind.

## *ESXShell*

Dieses Skript steuert die Anzeige des Login-Screens.

## *cdp*

Dieses Skript aktiviert/deaktiviert das Cisco Discovery-Protokoll.

## *dcbd*

Gehört ebenfalls zum Cisco Discovery-Protokoll.

## *iked*

Startet/stoppt den Internet Key Exchange-Dienst.

## *lbt*

Startet/stoppt ein netzwerkbasierendes Debugging-Tool (Load-Based Teaming Feature).

## *lsassd*, *lwiod*, *netlogond*

Skripten von Likewise für das Netzwerk: Likewise Identity and Authentication Service, IO Manager Service und Site Affinity Service.

## */sbin/services.sh*

Ein Skript, das alle Dienste des ESXi Servers neu startet (Ausnahme: Firewall wird nur aktualisiert).

## Wichtige Dateien und Verzeichnisse

Für den direkten Eingriff in das Verhalten des ESXi Servers gibt es einige wichtige Dateien in unterschiedlichen Ordnern. Hier werden nur die wichtigsten behandelt.

## */etc/inittab*

Diese Datei kann zum Ausführen von Programmen beim Systemstart benutzt werden, beispielsweise Backup-Clients.

## */var/log/*

Hier werden standardmäßig alle Protokolldateien abgelegt. VMware-Protokolldateien starten mit der Zeichenfolge *vm*. Die Hauptprotokolldatei liegt ebenfalls in die-

sem Verzeichnis und heißt *messages*. Beachten Sie auch die Hinweise in diesem Kapitel unter Logdateien.

#### */etc/ntp.conf*

Diese Datei dient der Konfiguration des NTP-Daemons, man könnte also manuell Zeitserver zur Zeitsynchronisation angeben.

### **VMware ESXi-Konfiguration**

Fast die gesamte Konfiguration des ESXi Host befindet sich in der Datei *esx.conf* im Verzeichnis */etc/vmware*. Diese Datei wurde im Laufe des Buches schon häufiger angesprochen, deshalb erwähne ich sie nur der Vollständigkeit halber.

## **Konfigurationsdatei der virtuellen Maschinen**

Wie Sie sicher noch wissen, finden Sie diese Konfigurationsdatei namens *Servername.vmx* im Heimatverzeichnis der virtuellen Maschine. Ich gehe im Folgenden alphabetisch auf die wichtigsten Parameter innerhalb dieser Datei ein.

#### *checkpoint.cptconfigname*

Name der Suspend-Datei, falls die virtuelle Maschine vorübergehend angehalten wird.

#### *displayName*

Es erscheint der Anzeigename der virtuellen Maschine.

#### *ethernet0.generatedaddress*

Die MAC-Adresse des ersten Netzwerkkadapters. Die ID wird bei mehreren Adaptern hochgezählt. Es kann durchaus nützlich sein, sich diese Adresse zu notieren, falls man bei Neuanlage der virtuellen Maschine wieder dieselbe MAC-Adresse verwenden will.

#### *ethernet0.networkname*

Name des virtuellen Switch, mit dem der entsprechende virtuelle Netzwerkkadapter verbunden ist.

#### *ethernet0.present = "TRUE"*

Angabe, ob ein Netzwerkkadapter vorhanden ist. Bei mehreren Adaptern wird die ID hochgezählt.

#### *ethernet0.virtualDev*

Art der Netzwerkkarte: *e1000*, *vmxnet* oder andere.

#### *floppy0.filename*

Name des Disketten-Image oder des physischen Pfads zum Laufwerk.

#### *floppy0.present*

Angabe, ob ein Diskettenlaufwerk vorhanden ist. Bei mehreren Laufwerken wird die ID hochgezählt.

#### *floppy0.startconnected*

Angabe, ob das Diskettenlaufwerk beim Starten angeschlossen sein soll.

*guestOS*

Betriebssystem innerhalb der virtuellen Maschine.

*ide0:0.deviceType*

Art des IDE-Geräts. Da von VMware ESX ab Version 4 nicht nur die CD-ROM-Laufwerke unterstützt werden, können die Werte sich auf CD-ROM-Image, physisches CD-Laufwerk oder Festplatten beziehen.

*ide0:0.fileName*

Name der CD-ROM-Imagedatei oder des physischen Pfads zum Laufwerk

*ide0:0.present*

Angabe, ob ein IDE-Controller vorhanden ist

*ide0:0.startConnected*

Angabe, ob das CD-Laufwerk beim Starten »angeschlossen« sein soll

*memSize*

Zugewiesener Hauptspeicher in MByte

*sched.cpu.shares*

Zugeweilte Shares (Anteile) für den Prozessor

*sched.mem.shares*

Zugeweilte Shares (Anteile) für den Arbeitsspeicher

*scsi0.present*

Angabe, ob ein SCSI-Controller in der virtuelle Maschine steckt. Bei mehreren Controllern wird die SCSI-ID hochgezählt.

*scsi0.virtualDev*

Art des SCSI-Bus-Adapters. Werte sind Bus Logic, LSI Logic, Paravirtuell oder SAS.

*tools.syncTime*

Angabe, ob die VMware Tools die Zeit mit dem Wirt abgleichen

*usb.present*

Angabe, ob USB-Anschlüsse innerhalb der virtuellen Maschine vorhanden sind

*virtualhw.version*

Angabe, welche virtuelle Hardwareversion in der virtuellen Maschine vorhanden ist

## Weitere Tools

Zusätzlich zu den bisher vorgestellten Kommandozeilenbefehlen gibt es noch weitere, wobei ich hier nur die wichtigsten detaillierter beschreibe. Dazu gehören *localcli*, *esxcli*, *vmkvsitools* und *vim-cmd*, wobei *localcli* und *esxcli* fast identisch sind. Die weiteren vorhandenen Befehle und Kommandos – auch die, die bisher nicht in diesem Kapitel aufgeführt wurden – finden Sie unten zusammenfassend aufgelistet.

Folgende alphabetisch geordnete Befehle sind auf das Kommando */bin/busybox* (Busy-Box) umgeleitet, haben aber fast immer die gleiche Bedeutung wie unter einem normalen Linux:

---

|          |          |          |        |
|----------|----------|----------|--------|
| ash      | fdisk    | mktemp   | su     |
| awk      | fgrep    | more     | sum    |
| basename | find     | mv       | sync   |
| cat      | getty    | nohup    | tail   |
| chgrp    | grep     | nslookup | tar    |
| chmod    | gunzip   | od       | tee    |
| chown    | gzip     | passwd   | test   |
| chvt     | halt     | poweroff | time   |
| cksum    | head     | printf   | touch  |
| clear    | hexdump  | readlink | true   |
| cp       | hostname | reboot   | uname  |
| cron     | id       | reset    | uniq   |
| cut      | inetd    | resize   | unzip  |
| date     | init     | rm       | usleep |
| dd       | kill     | rmdir    | vi     |
| diff     | ln       | sed      | watch  |
| dirname  | lockfile | seq      | wc     |
| du       | logger   | setsid   | wget   |
| echo     | login    | sh       | which  |
| egrep    | ls       | sha1sum  | who    |
| eject    | md5sum   | sleep    | whoami |
| env      | mkdir    | sort     | xargs  |
| expr     | mkfifo   | stat     | zcat   |
| false    | mknod    | stty     |        |

---

Folgende Befehle sind auf das Kommando */sbin/vmksitools* umgeleitet:

---

|            |        |       |        |
|------------|--------|-------|--------|
| amldump    | hwinfo | pidof | vdf    |
| bootOption | lsOf   | pkill | vdu    |
| hwclock    | lspci  | ps    | vmware |

---

Folgende Befehle für Benutzer und Gruppen sind »deprecated« (also veraltet), funktionieren aber noch:

---

|          |          |         |
|----------|----------|---------|
| adduser  | groupadd | useradd |
| delgroup | groupdel | userdel |
| deluser  | groups   | usermod |

---



*addgroup* Folgende Befehle gibt es tatsächlich – also ohne Umleitungen –, im Verzeichnis */usr/bin*:

---

|                   |                  |                   |                |
|-------------------|------------------|-------------------|----------------|
| busybox           | host_shutdown.sh | openssl           | ticket         |
| cim_host_powerops | kdestroy         | prop_of_instances | vmware-vmidump |
| cim-diagnostic.sh | kinit            | python            | vmx            |
| cimslp            | klist            | sfcg-config.py    | vmx-buildtype  |
| enum_instances    | less             | strace            | vmx-debug      |
| gdbserver         | lw-lsa           | tcpdump-uw        | vmx-stats      |
| host_reboot.sh    | nc               |                   |                |

---

Folgende Befehle gibt es tatsächlich – also ohne Umleitungen –, im Verzeichnis */usr/sbin* (Link auf */sbin*):

---

|                     |                       |                     |                      |
|---------------------|-----------------------|---------------------|----------------------|
| BootModuleConfig.sh | generate-certificates | openwsmand          | vmkbacktrace         |
| Formatters.py       | grabCIMData           | partedUtil          | vmkchdev             |
| InstallHelper.sh    | hbrfilterctl          | powerOffVms         | vmkdevmgr            |
| Session.py          | host-ind              | randomSeed          | vmkdump_extract      |
| apply-host-profiles | hostd                 | remoteDeviceConnect | vmkerrcode           |
| applyHostProfile    | iked                  | scantools           | vmkeventd            |
| authd               | init-launcher         | secpolicytools      | vmkfstools           |
| auto-backup.sh      | initterm.sh           | sensord             | vmkiscsi-tool        |
| backup.sh           | jumpstart             | services.sh         | vmkiscsid            |
| ls                  | localcli              | sfcgd               | vmkload_mod          |
| chkconfig           | logchannellogger      | shutdown.sh         | vmkmicrocode         |
| dcgd                | lsassd                | slpd                | vmkmkdev             |
| dcui                | lsusb                 | smbiosDump          | vmkperf              |
| dcuiweasel          | lwiod                 | spmd                | vmkping              |
| df                  | memstats              | spmdctl             | vmkramdisk           |
| dhclient-uw         | net-cdp               | statedumper         | vmkvsitools          |
| dmesg               | net-dvs               | storageRM           | vmtar                |
| doat                | net-fence             | summarize-dvfilter  | vmware-autostart.sh  |
| dosfsck             | net-lbt               | techsupport.sh      | vmware-usbarbitrator |
| emmett              | netlogond             | tmpwatch.py         | vprobe               |
| esxcli.py           | nologin               | traceroute          | vprobed              |
| esxtop              | ntp-keygen            | uptime              | vscsiStats           |
| esxupdate           | ntpd                  | vmcp                | vsi_traverse         |
| ethtool             | ntpdg                 | vmdumper            | vsish                |
| firmwareConfig.sh   | ntpq                  | vmfs-support        | watchdog.sh          |
| ft-stats            |                       |                     |                      |

---

Die Befehle *ping* und *ping6* sind auf */sbin/vmkiping* umgeleitet.

Der Befehl *vim-cmd* löst den Befehl */sbin/hostd* aus.

Die Befehle *scp* und *ssh* verweisen auf die gleichnamigen Programme unter */usr/lib/vmware/openssh/bin/*.

Eine Umleitung auf */sbin/vmkvstools* existiert für folgende Kommandos:

*amldump*, *bootOption*, *hwclock*, *hwinfo*, *lsof*, *lspci*, *pidof* und *vmkswap*.

## Das Tool *localcli*

Das Kommando *localcli* ist wie das Tool *esxcli* neu in der Version 5 von VMware vSphere. Diese beiden Utilities sind fast identisch, mit der Ausnahme, dass *localcli* die Befehle an den lokalen *hostd*-Prozess weiterleitet. Damit kann man es noch benutzen, wenn der *hostd*-Daemon nicht mehr reagiert. Dieses Tool greift also ziemlich tief in das Geschehen ein und sollte nur in Notfällen verwendet werden, oder wenn der VMware-Support Sie dazu auffordert.

## Das Tool *esxcli*

Das Werkzeug *esxcli* kann für sehr verschiedene Einsatzzwecke verwendet werden: FibreChannel over Ethernet, Hardware, iSCSI, Netzwerk, Software, Storage, System und Prozesse von virtuellen Maschinen. Eine ausführliche Übersicht über alle Möglichkeiten erhalten Sie, indem Sie an der Eingabeaufforderung folgenden Befehl angeben (zweimal hintereinander »esxcli« ist richtig!):

*esxcli esxcli command list*

In der Spalte *Command* sehen Sie die Möglichkeiten, die Sie mit diesem Befehl haben. Darunter sind das Hinzufügen (*add*), das Auslesen und Setzen (*get/set*), das De-/Aktivieren (*Disable*, *Enable*), das Auflisten (*list*), das Entfernen (*remove*) und andere.

Einiges, was in den Vorgängerversionen noch über *esxcfg*-Befehle erreicht werden konnte, wird jetzt mit diesem Tool erledigt. So können Sie zwar weiterhin z. B. *esxcfg-vswitch* benutzen, erreichen aber mit *esxcli* das Gleiche. Um z. B. einem vSwitch eine Portgruppe hinzuzufügen, können Sie den Befehl

*esxcfg-vswitch -A <Portgruppenname> <vSwitchname>*

angeben. Bei *esxcli* würden Sie das Gleiche mit folgendem Befehl erreichen:

*esxcli network vswitch standard portgroup add --portgroup-name="Goepel" --vswitch-name="vSwitch0"*

Es wird bei VMware angedacht, die noch vorhandenen *esxcfg*-Befehle (siehe oben) in Zukunft gänzlich durch *esxcli* zu ersetzen.

## Das Tool vmkvsitools

Auch bei diesem Befehl sollten Sie vorsichtig sein – benutzen Sie ihn nur in Zusammenarbeit mit dem VMware Support. Wie bereits oben erwähnt, sind einige der »normalen« Befehle auf dieses Tool umgeleitet.

## Das Tool vim-cmd

Über dieses Werkzeug können einige Befehle für die virtuellen Maschinen eingegeben werden. Dabei ist die Syntax etwas gewöhnungsbedürftig, da die Hilfestellung auf der Kommandozeile etwas anderes aussagt, als die tatsächliche Syntax ist. Möchten Sie sich z. B. alle auf dem Host registrierten VMs in Listenform ansehen, nehmen Sie folgenden Befehl:

*vim-cmd vmsvc/getallvms*

Auch Befehle für den ESXi Host können hiermit angegeben werden. Dazu gehören z. B. die Aktivierung des Wartungsmodus mit

*vim-cmd hostsvc/maintenance\_mode\_enter*

und sein Verlassen mit

*vim-cmd hostsvc/maintenance\_mode\_exit*

Weitere Möglichkeiten des Befehls bekommen Sie angezeigt, indem Sie nur seinen Namen auf der Shell angeben. Hilfe zu einem Untermenü bekommen Sie über die Angabe des Befehls, des gewünschten Untermenüs und help:

*vim-cmd vmsvc help*

Nach den obigen Beispielen können Sie sich dann das Gewünschte heraussuchen.

## Eigene Skripten schreiben

Dieser Abschnitt versucht nicht, Ihnen die Skriptsprache von Linux beizubringen. Er zeigt Ihnen lediglich ein paar Beispiele dafür, wie man die eine oder andere Aufgabe skriptgesteuert erledigen kann. Mehr Informationen über das Erstellen von Shell-Skripten finden Sie unter <http://tldp.org/guides.html>.



Wenn Sie das *Remote Command Line Interface* (RCLI) für den ESXi einsetzen, sind die Befehle ein wenig anders. VMware hat darüber eine sehr ausführliche Dokumentation herausgebracht, die Sie sich auch von der Website zum Buch herunterladen können. Beachten Sie aber, dass seit der Version 3.5 U3 die kostenlose i-Version nur einen schreibgeschützten Zugriff gestattet.

### Ein einfaches Beispiel

Erstellen Sie eine Textdatei mit dem Namen *Test* mithilfe des vi:

```
#!/bin/sh # %ber die sh-Shell ausf%hren
Das ist ein Testskript # nur eine Bemerkung
```

```
cd /vmfs/volumes # gehe zum Verzeichnis
ls ñal # listet den Inhalt auf
```

Speichern Sie die Datei unter dem Namen *Test* und führen Sie den Befehl

```
chmod +x Test
```

aus, um die Textdatei in ein ausführbares Skript zu ändern. Anschließend können Sie das Skript ausprobieren, indem Sie es wie folgt aufrufen:

```
./Test
```

Es sollte Ihnen jetzt den Inhalt des Verzeichnisses */vmfs/volumes* anzeigen, also üblicherweise die Verzeichnisse der virtuellen Maschinen.

## Variablen in Skripten benutzen

Variablen, die in Skripten verwendet werden, nennt man *lokale Variablen*, weil sie und ihr Inhalt nach der Ausführung verloren gehen. Variablen können in Groß- und Kleinbuchstaben angegeben und mit dem Befehl `echo` ausgegeben werden, also z. B. so:

```
echo $VARIABLE
echo $variable
```

Das Setzen des Werts einer Variablen kann auf zwei verschiedenen Wegen erfolgen:

```
set VARIABLE=wert
VARIABLE=wert
export VARIABLE
```

Eine Variable zu exportieren, heißt in diesem Zusammenhang, dass sie nach der Beendigung des Skripts weiterhin als Umgebungsvariable deklariert ist.

## Nützliche Skriptbefehle

Die folgende Liste ist nicht ausführlich, sondern soll Ihnen lediglich eine Anregung für Ihre Skripten geben, die Sie auf dem ESXi Server benutzen können. Beachten Sie auch den Anfang dieses Kapitels, der viele mögliche Befehle für die Kommandozeile und somit auch für Ihre Skripten enthält.

---

|                                       |                                                                                  |
|---------------------------------------|----------------------------------------------------------------------------------|
| <code>esxcfg-vswitch</code>           | Hinzufügen, entfernen und modifizieren von virtuellen Switches und Einstellungen |
| <code>esxcfg-nics</code>              | Informationen über physische Netzwerkkarten                                      |
| <code>esxcfg-info</code>              | Informationen über das System                                                    |
| <code>esxcli software vib list</code> | Alle VIB-Pakete auf dem Server anzeigen                                          |
| <code>vmware -v</code>                | ESX Server-Versionshinweise anzeigen                                             |
| <code>who</code>                      | Anzeigen, wer angemeldet ist                                                     |
| <code>date</code>                     | Datum und Uhrzeit anzeigen                                                       |

---

### Beispiel

```
#!/bin/sh
Dieses Skript zeigt einige Beispiele und Informationen auf
PATH=/bin:/usr/bin:/usr/sbin
LOGFILE=/tmp/esx-report.txt
date > $LOGFILE
echo "ESXi Server Version: " >> $LOGFILE
vmware nv >> $LOGFILE
echo "Virtual Switch-Konfiguration: " >> $LOGFILE
esxcfg-vswitch nl >> $LOGFILE
echo "Verfuegbare Pakete: ">> $LOGFILE
esxcli software vib list >> $LOGFILE
who >> $LOGFILE
EOF
```

In diesem Skript werden zwei Variablen definiert: eine namens PATH, die dem Skript anzeigt, wo es welche Befehle findet, und eine namens LOGFILE. Dieses Skript erstellt also eine kleine Datei, die Folgendes beinhaltet:

- Datum und Uhrzeit der Ausführung dieses Skripts
- die Version des ESXi Servers, auf dem es ausgeführt wird
- eine Liste der virtuellen Switches
- eine Liste der verfügbaren ESXi-Pakete
- welche User gerade angemeldet sind

### Umgang mit Leerzeichen im Pfad

Werden Leerzeichen im Verzeichnis- oder Dateinamen verwendet, kommt es bei der Ausführung von Linux-Befehlen und -Skripten oft zu Problemen, da nach dem Leerzeichen abgebrochen wird.

Will man eine virtuelle Maschine mit Leerzeichen im Namen einschalten, muss man entweder den Pfad mit Hochkommata versehen oder vor dem Leerzeichen einen Backslash (\) platzieren, um die Leerzeichen nutzen zu können, also

```
vim-cmd vmsvc/power.on /vmfs/volumes/datastore/VM\ Name/VM\ Name.vmx
```

oder

```
vim-cmd vmsvc/power.on "/vmfs/volumes/datastore/VM Name/VM Name.vmx"
```

Nun haben Sie das Handwerkszeug parat, um weitere eigene Skripten zu erstellen. Beachten Sie aber dabei, dass Dateien auf dem ESXi Server in fast allen Verzeichnissen beim Neustart gelöscht werden – mit Ausnahme der Dateien auf dem VMFS-Volume.

Ich möchte abschließend nochmals betonen, was ich schon am Anfang geschrieben habe: Für fast alles, was Sie am ESXi Server machen müssen, gibt es die Möglichkeit, es über den vSphere Client über die grafische Oberfläche zu tun. In Verbindung mit dem vCenter Server können Sie noch mehr erledigen und Vieles sogar über die geplanten Tasks.



# Der vCenter Server

Wir haben unsere Umgebung mit mehreren ESXi Servern jetzt aufgebaut und einen gemeinsamen Speicherplatz eingerichtet. Unsere virtuellen Maschinen laufen auf den Hosts ohne Probleme. Was nun noch fehlt, ist eine zentrale Instanz, die wir dazu nutzen wollen, alle Server und Gäste in einem Fenster zu überblicken, sie von dort aus zu konfigurieren und viele weitere Funktionen einzusetzen. Dafür gibt es, wie bereits in Kapitel 2 beschrieben und schon oft erwähnt, den vCenter Server.

Ein vCenter Server ist eine Anwendung, die üblicherweise auf einem 64-Bit-Windows-Server installiert wird und anschließend als Dienst im Hintergrund läuft. Eine Installation auf einer Workstation-Version ist nicht mehr möglich. Im vCenter Server werden die Hosts mit dem *vpxuser*-Account angeschlossen, so dass über den Windows-Rechner die Zugriffe an die ESXi Hosts durchgereicht werden. Weiterhin wird eine Datenbank auf diesem Computer installiert oder ein Zugriff auf eine bereits bestehende Datenbank abgefragt, damit z.B. die Performancedaten der Hosts und VMs dort abgelegt werden können.

Noch einfacher und ohne Windows kann man die vorgefertigte vCenter Server Appliance importieren. Diese basiert auf SuSE Linux 11 und ist von VMware auf die Aufgaben speziell vorbereitet.

Der Benutzer kann weiterhin mit dem vSphere Client arbeiten und verbindet sich jetzt mit dem Management-Server. Auch WebAccess ist über den vCenter Server möglich.

## Funktionen des vCenter Servers

Was bietet dieser Server uns alles als zusätzliche Funktionen, die wir beim allein stehenden ESXi Server nicht haben? Hier zunächst eine grobe Übersicht der Möglichkeiten, die natürlich abhängig von der eingesetzten Lizenz sind:

- *vMotion*: Virtuelle Maschinen im laufenden Betrieb von einem ESXi Server auf einen anderen verschieben
- *Storage vMotion*: Dateien der virtuellen Maschinen von einem Storage auf einen anderen verschieben, ohne die VM herunterzufahren

- *Distributed Resource Scheduler (DRS)*: Automatisches Load-Balancing zwischen den Hosts bezüglich RAM und CPU-Last
- *High Availability (HA)*: Automatischer Neustart ausgefallener VMs auf den verbliebenen Hosts
- *Fault Tolerance (FT)*: Gespiegelte virtuelle Maschinen für die Ausfallsicherheit
- *Hostprofile*: Vergleichen der ESXi Server in ihrer Konfiguration
- *Importer/Converter*: Import physikalischer Rechner und virtueller Maschinen aus anderen Programmen und Erstellung neuer VMs aus Backups und Images
- *Data Recovery*: Zeitgesteuertes Backup der VM Dateien
- *Distributed vSwitches*: ESXi-übergreifende Netzwerk-Switches mit mehr Funktionen als Standard-vSwitches
- *Alarme*: Senden von Informationen auf die Oberfläche per E-Mail, SNMP o. Ä.
- *vApp*: Zusammenfassung von VMs zu Gruppen mit leichterer Bedienbarkeit
- *Distributed Power Management (DPM)*: Power-Management für ESXi Hosts zum Stromsparen
- *Geplante Tasks*: Zeitgesteuertes Ausführen von Aktionen
- *Sitzungen*: Überwachen und Beenden von Zugriffen einzelner User
- *Ordner*: Erstellen von Ordnern für das Zusammenfassen oder Gliedern von Objekten
- *Update Manager*: Automatisches, zeitgesteuertes Aktualisieren der Host- und Gast-systeme
- *Lizenzen*: Vereinfachtes Management aller erworbenen Lizenzen
- *Leistung*: Ressourcendiagramme über Tage, Monate und Jahre
- *Zuordnungen*: Grafische Zusammenhänge zwischen VMs, Hosts, Storages und Netzwerken
- *Vorlagen*: Erstellen von Templates
- *Klonen*: Duplizieren von VMs
- *Zugriffsrechte*: Rechtevergabe über Windows-(Domänen-)User und -Gruppen.
- *vSphere Web Client*: Zugriff über einen Browser anstelle des vSphere Clients
- *vSphere Auto Deploy*: Automatisiertes Bereitstellen mehrerer ESXi Hosts
- *vSphere Storage Appliance (VSA)*: Gemeinsamer Storage über lokale ESXi-Platten

Die einzelnen Funktionen werden im Laufe des Buchs noch detaillierter besprochen.

Um Funktionen wie das Verschieben von VMs zur Laufzeit (vMotion), das Load-Balancing über die Auslastung von Prozessor und Arbeitsspeicher der Hosts (DRS) oder den automatischen Neustart der VMs beim Ausfall einer Hosthardware (HA) zu erreichen, ist ein gemeinsamer Storage (VSA-, NFS-, iSCSI-SAN- oder FC-SAN-Speicher) notwendig (siehe Abbildung 10-1).



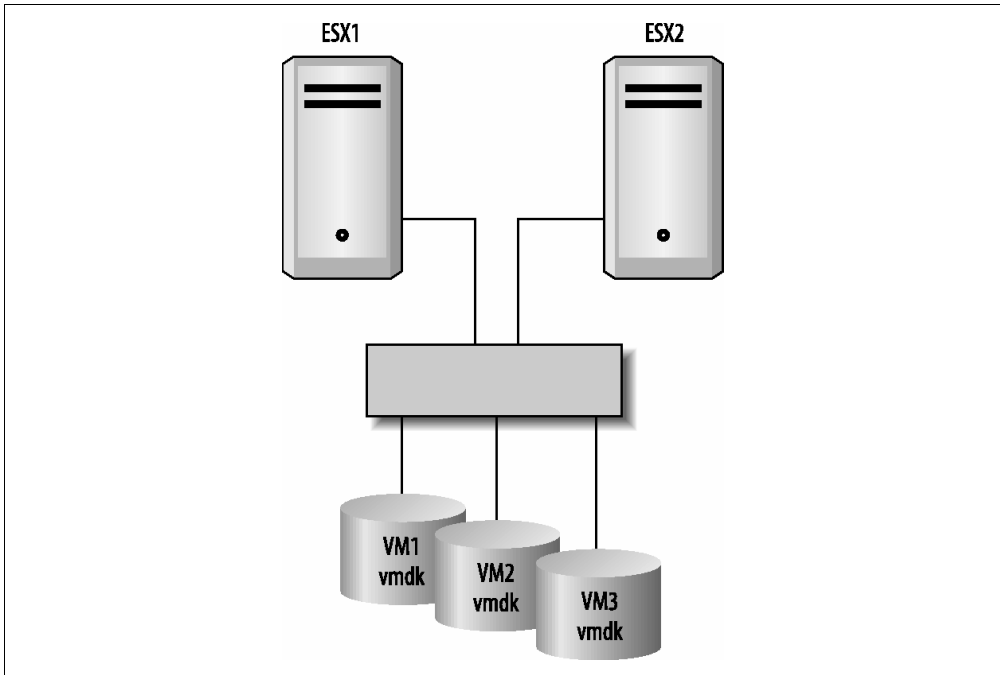


Abbildung 10-1: vSphere-Umgebung mit SAN

Nur wenn auf dem gemeinsamen Speicher alle Dateien der virtuellen Maschine abgelegt und von allen beteiligten ESXi Servern erreichbar sind, lassen sich diese Funktionen einsetzen.

Die angesprochenen Komponenten werden im weiteren Verlauf noch ausführlich besprochen.

Die schematische Darstellung der Kernkomponenten einer vSphere5-Umgebung, die Sie in Abbildung 10-2 sehen, stammt aus der deutschen Dokumentation von VMware zu diesem Thema.

## Maximalwerte für die vSphere5-Umgebung

Die maximal möglichen Werte für den ESXi Host und die virtuelle Maschine habe ich in den jeweiligen Kapiteln schon angesprochen. Die mögliche Ausbaustufe mit dem vCenter Server unterscheidet sich dabei, und es werden zusätzliche Komponenten zur Verfügung gestellt. Auf der Internetseite von VMware können Sie sich die deutschsprachige PDF-Datei *vsp\_50\_config\_max\_de.pdf* ansehen und herunterladen. Sie wird immer aktuell gehalten, denn manchmal ändern sich z.B. durch Updates ein paar Details. Die in den folgenden Tabellen angegebenen Werte sind besagter PDF-Datei entnommen.

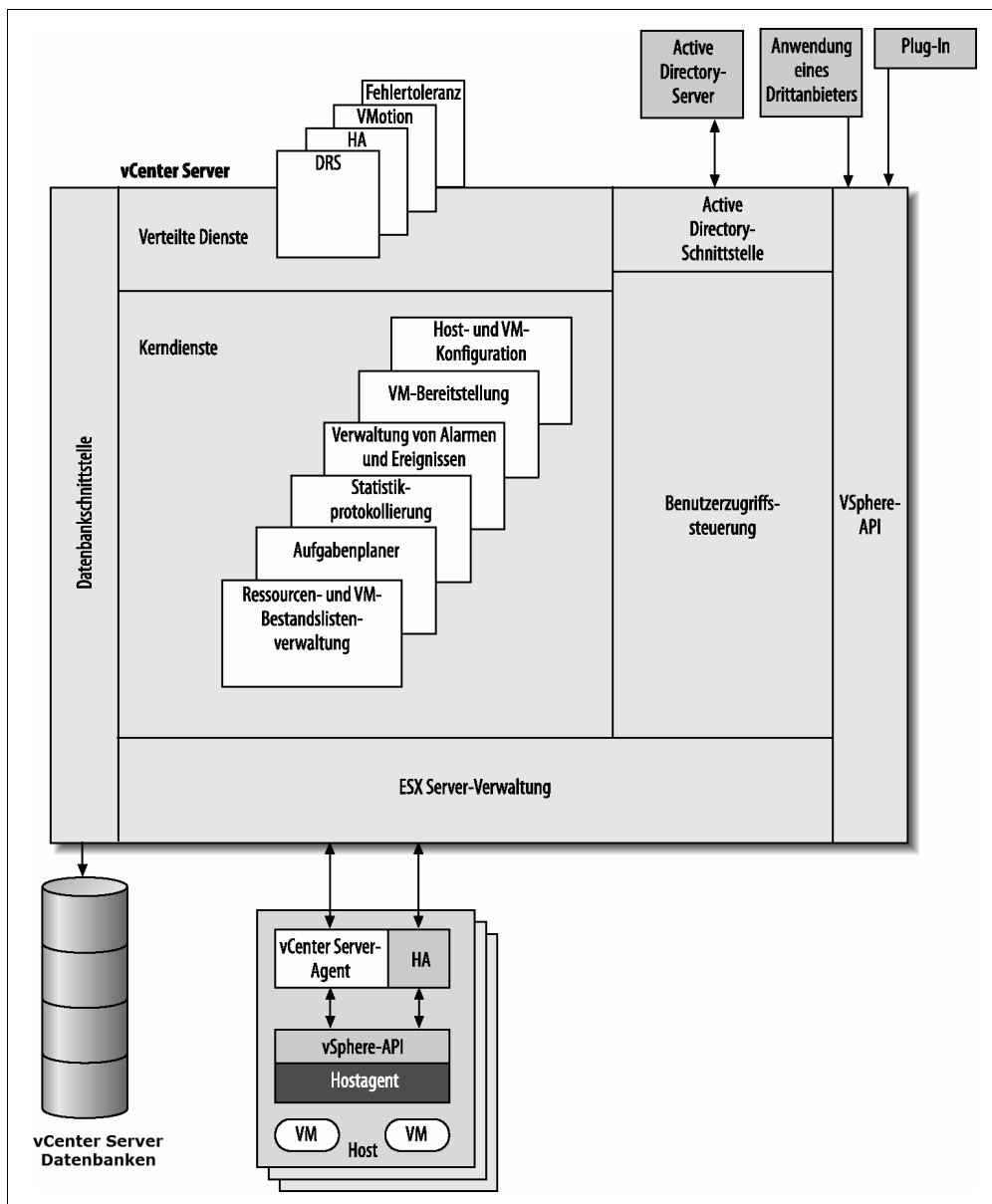


Abbildung 10-2: Komponenten einer vSphere-Umgebung

## Maximalwerte für virtuelle Maschinen

In der Tabelle 10-1 sind die maximal möglichen Ressourcen für die virtuellen Maschinen unter vSphere5 aufgelistet.

Tabelle 10-1: Maximalwerte für VMs

| Element                                                                | Maximalwert             |
|------------------------------------------------------------------------|-------------------------|
| <b>Rechenressourcen</b>                                                |                         |
| Virtuelle CPUs je virtuelle Maschine (Virtual SMP)                     | 32                      |
| <b>Arbeitsspeicher</b>                                                 |                         |
| RAM je virtuelle Maschine                                              | 1 TByte (1.011 MByte)   |
| Größe der Auslagerungsdatei für die virtuelle Maschine                 | 1 TByte (1.011 MByte)   |
| <b>Virtuelle Speicheradapter und -geräte</b>                           |                         |
| Virtuelle SCSI-Adapter je virtuelle Maschine                           | 4                       |
| Virtuelle SCSI-Ziele je virtueller SCSI-Adapter                        | 15                      |
| Virtuelle SCSI-Ziele je virtuelle Maschine                             | 60                      |
| Festplattengröße                                                       | 2 TByte minus 512 Byte  |
| IDE-Controller je virtuelle Maschine                                   | 1 (Primary + Secondary) |
| IDE-Geräte je virtuelle Maschine                                       | 4                       |
| Diskettencontroller je virtuelle Maschine                              | 1                       |
| Diskettenlaufwerke je virtuelle Maschine                               | 2                       |
| <b>Virtuelle Netzwerkgeräte</b>                                        |                         |
| Virtuelle Netzwerkkarten je virtuelle Maschine                         | 10                      |
| <b>Virtuelle Peripherieschnittstellen</b>                              |                         |
| Parallele Schnittstellen je virtuelle Maschine                         | 3                       |
| Serielle Schnittstellen je virtuelle Maschine                          | 4                       |
| USB-Controller je virtuelle Maschine                                   | 1                       |
| USB 2.0-Geräte je virtuelle Maschine                                   | 20                      |
| USB 3.0-Geräte je virtuelle Maschine                                   | 1                       |
| <b>Grafikkarte</b>                                                     |                         |
| Videoarbeitsspeicher je virtuelle Maschine                             | 128 MByte               |
| <b>Verschiedenes</b>                                                   |                         |
| Gleichzeitige Remote-Console-Verbindungen zu einer virtuellen Maschine | 40                      |

## Maximalwerte für ESXi-Hosts

Die folgenden Tabellen enthalten die Maximalwerte für die Konfiguration von ESXi-Hosts.

Tabelle 10-2: Maximalwerte für den Speicher

| Element                       | Maximalwert |
|-------------------------------|-------------|
| <b>Virtuelle Festplatten</b>  |             |
| Virtuelle Festplatten je Host | 2.048       |
| iSCSI physisch                |             |

Tabelle 10-2: Maximalwerte für den Speicher (Fortsetzung)

| Element                                                                                                   | Maximalwert            |
|-----------------------------------------------------------------------------------------------------------|------------------------|
| LUNs pro Server                                                                                           | 256                    |
| Qlogic 1 GB iSCSI-HBA-Initiator-Ports je Server                                                           | 4                      |
| Broadcom 1 GB iSCSI-HBA-Initiator-Ports je Server                                                         | 4                      |
| Broadcom 10 GB iSCSI-HBA-Initiator-Ports je Server                                                        | 4                      |
| Netzwerkkarten, die dem Software-iSCSI-Stack je Server zugewiesen oder an den Port gebunden werden können | 8                      |
| Anzahl aller Pfade auf einem Server                                                                       | 1.024                  |
| Anzahl der Pfade zu einer LUN (Software-iSCSI und Hardware-iSCSI)                                         | 8                      |
| Qlogic-iSCSI: dynamische Ziele je Adapterport                                                             | 64                     |
| Qlogic-iSCSI: statische Ziele je Adapterport                                                              | 62                     |
| Broadcom 1 GB iSCSI-HBA-Ziele je Adapterport                                                              | 64                     |
| Broadcom 10 GB iSCSI-HBA-Ziele je Adapterport                                                             | 128                    |
| Software-iSCSI-Ziele                                                                                      | 256                    |
| <b>NAS</b>                                                                                                |                        |
| NFS-Mounts je Host                                                                                        | 256                    |
| <b>Fibre-Channel</b>                                                                                      |                        |
| LUNs pro Host                                                                                             | 256                    |
| LUN-Größe                                                                                                 | 64 TByte               |
| LUN-ID                                                                                                    | 255                    |
| Anzahl der Pfade zu einer LUN                                                                             | 32                     |
| Anzahl aller Pfade auf einem Server                                                                       | 1.024                  |
| Anzahl an HBAs beliebigen Typs                                                                            | 8                      |
| HBA-Ports                                                                                                 | 16                     |
| Ziele je HBA                                                                                              | 256                    |
| <b>FCoE</b>                                                                                               |                        |
| Software-FCoE-Adapter                                                                                     | 4                      |
| <b>VMFS</b>                                                                                               |                        |
| Volumes je Host                                                                                           | 256                    |
| Hosts je Volume                                                                                           | 64                     |
| Eingeschaltete virtuelle Maschinen je VMFS-Volume                                                         | 2.048                  |
| <b>VMFS3</b>                                                                                              |                        |
| Volumegröße                                                                                               | 64 TByte               |
| Größe der Raw-Gerätezuordnung (virtuelle Kompatibilität)                                                  | 2 TByte minus 512 Byte |
| Größe der Raw-Gerätezuordnung (physische Kompatibilität)                                                  | 2 TByte minus 512 Byte |
| Blockgröße                                                                                                | 8 MByte                |
| Dateigröße (1 MByte Blockgröße)                                                                           | 256 GByte              |
| Dateigröße (2 MByte Blockgröße)                                                                           | 512 GByte              |
| Dateigröße (4 MByte Blockgröße)                                                                           | 1 TByte                |

Tabelle 10-2: Maximalwerte für den Speicher (Fortsetzung)

| Element                                                  | Maximalwert            |
|----------------------------------------------------------|------------------------|
| Dateigröße (8 MByte Blockgröße)                          | 2 TByte minus 512 Byte |
| Dateien je Volume                                        | ca. 30.720             |
| VMFSS                                                    |                        |
| Volumegröße                                              | 64 TByte               |
| Größe der Raw-Gerätezuordnung (virtuelle Kompatibilität) | 2 TByte minus 512 Byte |
| Größe der Raw-Gerätezuordnung (physische Kompatibilität) | 64 TByte               |

Tabelle 10-3: Maximalwerte für Rechenressourcen

| Element                              | Maximalwert |
|--------------------------------------|-------------|
| Virtuelle CPUs je Host               | 2.048       |
| Virtuelle Maschinen je Host          | 512         |
| Logische Prozessoren je Host         | 160         |
| Virtuelle CPUs je physischer Kern    | 25          |
| Fehlertoleranz                       |             |
| Virtuelle Festplatten                | 16          |
| Virtuelle CPUs je virtuelle Maschine | 1           |
| RAM je FT VM                         | 64 GByte    |
| Virtuelle Maschinen je Host          | 4           |

Tabelle 10-4: Maximalwerte für den Arbeitsspeicher

| Element                     | Maximalwert                                                                |
|-----------------------------|----------------------------------------------------------------------------|
| Größe des RAM je Host       | 2 TByte                                                                    |
| Auslagerungsdateien         | 1 pro virtuelle Maschine                                                   |
| Größe der Auslagerungsdatei | entsprechend der maximalen Größe des RAM der virtuellen Maschine (1 TByte) |

## Maximalwerte für das Netzwerk

Die folgenden Grenzwerte stellen erreichbare maximale Grenzwerte für die Netzwerk-konfiguration in Umgebungen dar, in denen keine restriktiveren Grenzwerte gelten (z. B. vCenter Server-Grenzwerte, von Funktionen wie HA oder DRS auferlegte Grenzwerte sowie andere Konfigurationen, die beim Bereitstellen großer Systeme zu berücksichtigende Einschränkungen beinhalten).

Tabelle 10-5: Maximalwerte für das Netzwerk

| Element                                      | Maximalwert |
|----------------------------------------------|-------------|
| <b>Physische Netzwerkkarten</b>              |             |
| e1000 NICs Ethernet-Ports (Intel PCI-x NIC)  | 32          |
| e1000e NICs Ethernet-Ports (Intel PCI-e NIC) | 24          |

Tabelle 10-5: Maximalwerte für das Netzwerk (Fortsetzung)

| Element                                                                     | Maximalwert                     |
|-----------------------------------------------------------------------------|---------------------------------|
| igb 1 GB Ethernet-Ports (Intel)                                             | 16                              |
| tg3 1 GB Ethernet-Ports (Broadcom)                                          | 32                              |
| bnx2 1 GB Ethernet-Ports (Broadcom)                                         | 16                              |
| forcedeth 1 GB Ethernet-Ports (Nvidia)                                      | 2                               |
| nx_nic 10 GB Ethernet-Ports (NetXen)                                        | 8                               |
| ixgbe Oplink 10 GB Ethernet-Ports (Intel)                                   | 8                               |
| bnx2x 10 G Ethernet-Ports (Broadcom)                                        | 8                               |
| Kombination aus 10-GB- und 1-GB-Ethernet-Ports                              | 6 10-GByte- und 4 1-GByte-Ports |
| Infiniband-Ports (an VMware Community Support wenden)                       | nicht bekannt <sup>1</sup>      |
| <b>PCI VMDirectPath-Grenzwerte</b>                                          |                                 |
| PCI/PCIe VMDirectPath-Geräte je Host                                        | 8                               |
| PCI/PCIe VMDirectPath-Geräte je virtuelle Maschine                          | 4 <sup>2</sup>                  |
| <b>vSphere Standard und Distributed Switch</b>                              |                                 |
| Gesamtzahl der virtuellen Netzwerkswitch-Ports je Host (vDS- und vSS-Ports) | 4.096                           |
| Maximal aktive Ports je Host (vDS und VSS)                                  | 1.016                           |
| Virtuelle Netzwerkswitch-Ports je Standardswitch                            | 4.088                           |
| Portgruppen je Standardswitch                                               | 256                             |
| Verteilte virtuelle Netzwerk-Switch-Ports je vCenter                        | 30.000                          |
| Statische Portgruppen je vCenter                                            | 5.000                           |
| Flüchtige Portgruppen je vCenter                                            | 256                             |
| Hosts je verteilter Switch                                                  | 350                             |
| Verteilte Switches je vCenter                                               | 32                              |
| <b>Gleichzeitige Vorgänge</b>                                               |                                 |
| Gleichzeitige vMotion-Vorgänge je Host (1 GBit/s-Netzwerk)                  | 4                               |
| Gleichzeitige vMotion-Vorgänge je Host (10 GBit/s-Netzwerk)                 | 8                               |

1. Mellanox Technologies InfiniBand HCA-Gerätetreiber werden direkt von Mellanox Technologies zur Verfügung gestellt. Wenden Sie sich bitte an Mellanox, wenn Sie mehr über die Unterstützung von InfiniBand HCAs mit ESXi erfahren möchten (<http://www.mellanox.com>).
2. Eine virtuelle Maschine kann sechs Geräte unterstützen, wenn es sich bei zweien von ihnen um Teradici-Geräte handelt.

Tabelle 10-6: Maximalwerte für Ressourcenpools und Cluster

| Element                                | Maximalwert |
|----------------------------------------|-------------|
| <b>HA- und DRS-Cluster</b>             |             |
| Hosts je HA-Cluster                    | 32          |
| Virtuelle Maschinen je Cluster         | 3.000       |
| Virtuelle Maschinen je Host im Cluster | 512         |

Tabelle 10-6: Maximalwerte für Ressourcenpools und Cluster (Fortsetzung)

| Element                                         | Maximalwert    |
|-------------------------------------------------|----------------|
| Maximale Anzahl gleichzeitiger Host-HA-Failover | 32             |
| Failover als Prozentsatz an Clustern            | 100 %          |
| <b>Ressourcenpool</b>                           |                |
| Ressourcenpools je Cluster                      | 1.600          |
| Ressourcenpools je Host                         | 1.600          |
| Untergeordnete Elemente je Ressourcenpool       | 1.024          |
| Strukturtiefe Ressourcenpool                    | 8 <sup>1</sup> |

1. Vier zusätzliche Ressourcenpools werden von internen Systemkomponenten verwendet.

### Verwendung von Maximalwerten für mehrere Konfigurationsoptionen

Wenn eine der in den Tabellen oben aufgeführten Konfigurationsoptionen mit dem Maximalwert verwendet wird, sollten ESXi Host und vCenter Server diese Werte mit der jeweiligen Standardkonfiguration verarbeiten können.

Wenn mehrere Konfigurationsoptionen (z.B. Anzahl an virtuellen Maschinen, Anzahl an LUNs und Anzahl an vDS-Ports) mit dem Maximalwert verwendet werden, kann es passieren, dass der Arbeitsspeicher für einige der auf dem Host ausgeführten Prozesse nicht mehr ausreicht. Das kann dazu führen, dass der Host die Verbindung zum vCenter Server immer wieder trennt. In diesem Fall müssen Sie den verfügbaren Arbeitsspeicher für diese Hostprozesse erhöhen, so dass der Host der geplanten Arbeitslast standhalten kann. Sie müssen die Menge an Arbeitsspeicher in Relation zur Anzahl der mit dem Maximalwert verwendeten Konfigurationsoptionen erhöhen.

Tabelle 10-7: Maximalwerte für vCenter Server

| Element                                                 | Maximalwert |
|---------------------------------------------------------|-------------|
| <b>vCenter Server-Skalierbarkeit</b>                    |             |
| Hosts je vCenter Server                                 | 1.000       |
| Eingeschaltete virtuelle Maschinen je vCenter Server    | 10.000      |
| Registrierte virtuelle Maschinen je vCenter Server      | 15.000      |
| Verknüpfte vCenter Server-Systeme                       | 10          |
| Hosts im verknüpften Modus                              | 3000        |
| Eingeschaltete virtuelle Maschinen im verknüpften Modus | 30.000      |
| Registrierte virtuelle Maschinen im verknüpften Modus   | 50.000      |
| Gleichzeitige vSphere Client-Verbindungen               | 100         |
| Hosts je Datacenter                                     | 500         |
| MAC-Adressen je vCenter Server                          | 65.536      |
| <b>Benutzeroberfläche</b>                               |             |
| An den vSphere-Client angeschlossene USB-Geräte         | 20          |

## vCenter Server-Erweiterungen

Die Maximalwerte für die Erweiterungen zum vCenter Server folgen in den nächsten Tabellen, damit Sie sich vor der Installation der einzelnen Komponenten die notwendigen Informationen hier holen können. Beachten Sie, dass Sie z.B. den Update Manager nicht unbedingt auf demselben Server wie den vCenter Server installieren müssen. Gerade in großen Umgebungen kann es sinnvoll sein, diesen auf einem anderen Server zu positionieren.

*Tabelle 10-8: Maximalwerte für vCenter Update Manager*

| Element                                                          | Maximalwert |
|------------------------------------------------------------------|-------------|
| <b>vCenter Update Manager-Skalierbarkeit</b>                     |             |
| Hostprüfungen in einem einzelnen vCenter Server                  | 1.000       |
| Prüfungen virtueller Maschinen in einem einzelnen vCenter Server | 10.000      |
| Cisco VDS-Update und -Bereitstellung                             | 70          |
| <b>Gleichzeitige Vorgänge</b>                                    |             |
| Prüfungen der VMware Tools je ESXi-Host                          | 90          |
| Upgrade der VMware Tools je ESXi-Host                            | 24          |
| Hardwareprüfungen einer virtuellen Maschine je Host              | 90          |
| Hardware-Upgrades einer virtuellen Maschine je Host              | 24          |
| Prüfungen der VMware Tools je VUM-Server                         | 75          |
| Upgrades der VMware Tools je VUM-Server                          | 75          |
| Hardwareprüfungen einer virtuellen Maschine je VUM-Server        | 75          |
| Hardware-Upgrades einer virtuellen Maschine je VUM-Server        | 75          |
| ESXi-Host-Prüfung je VUM-Server                                  | 75          |
| ESXi-Host-Standardisierung je VUM-Server                         | 71          |
| ESXi-Host-Upgrade je VUM-Server                                  | 71          |
| ESXi-Host-Upgrade je Cluster                                     | 1           |

*Tabelle 10-9: Maximalwerte für vCenter Orchestrator*

| Element                            | Maximalwert |
|------------------------------------|-------------|
| Verbundene vCenter Server-Systeme  | 10          |
| Verbundene ESXi-Instanzen          | 100         |
| Verbundene virtuelle Maschinen     | 15.000      |
| Gleichzeitig ausgeführte Workflows | 150         |

*Tabelle 10-10: Maximalwerte für Speicher-DRS*

| Element                                        | Maximalwert |
|------------------------------------------------|-------------|
| Virtuelle Festplatten je Datenspeicher-Cluster | 9.000       |
| Datenspeicher je Datenspeicher-Cluster         | 32          |
| Datenspeicher-Cluster je vCenter               | 256         |



# Die technischen Voraussetzungen für einen vCenter Server

VMware gibt als minimale Hardwareanforderungen unter anderem zwei CPUs (mit 64 Bit, aber kein Itanium IA64) und 4 GByte Arbeitsspeicher an. Das reicht dann für bis zu 200 Hosts und 2.000 laufende VMs. Bei kleinen Umgebungen mit z.B. vier ESXi Servern und bis zu 30 virtuellen Maschinen kommt man aber auch mit weniger Ressourcen aus, also z.B. einem Prozessor und 3 GByte RAM aus.

Wichtig sind bei der Dimensionierung auch Überlegungen zu den Funktionen, die der vCenter Server unterstützen soll. So muss man bedenken, dass der Update Manager eine eigene Datenbank haben sollte, dass der Converter/Importer und viele gleichzeitige Verbindungen mit dem vSphere Client den Rechner belasten und dass jede weitere Funktion (etwa vSphere Webservices), die implementiert wird, dem Server auch zu schaffen macht. Kalkulieren Sie mit Augenmaß, wie die Hardware Ihres Servers beschaffen sein sollte.

Beachten Sie bitte, dass die Anforderungen für die vCenter Server Appliance andere Werte voraussetzen, weil dort alle Dienste auf nur einem Rechner laufen. Auf die genauen Details gehe ich auf der folgenden Seite ausführlich ein.

Auf der Festplatte müssen zunächst für die vCenter Server-Komponenten 4 GByte frei sein. Für die Datenbank des Servers und gegebenenfalls für den Update Manager müssen ebenfalls jeweils mindestens 2 GByte während der Installation zur Verfügung stehen, falls die mitgelieferte kostenlose SQL Server 2008 R2 Express-Version genutzt wird (die wiederum den MS Installer 4.5 bedingt und im Lieferumfang des DVD/ISO-Image enthalten ist). Sie können aber auch eine externe Datenbank verwenden – auch auf einem dedizierten Rechner. Eine Installation auf einem USB-Stick oder einer Netzwerkfreigabe wird übrigens nicht unterstützt.

Die Netzwerkkarten sollten GBit-Ethernet-Adapter sein. Wie viele Sie brauchen, hängt auch hier von Ihrer Umgebung ab – ob Sie z.B. getrennte Subnetze verwenden wollen –, sonst reicht meist eine, und Sie sollten eine statische IP-Adresse verwenden. Sie können natürlich auch hier IPv6 einsetzen, dann wird aber der vCenter Orchestrator (Workflow-Engine zur Automatisierung von Prozessen) nicht mehr unterstützt, sehr wohl aber bei einer gemischten IPv4- und IPv6-Umgebung.

Als Betriebssystem für den vCenter Server 5.0 brauchen Sie einen Windows-Rechner mit 64-Bit-OS. Das kann ein Microsoft Server 2003 SP2, 2003 R2, 2008 SP1/2 oder 2008 R2 sein.

Stellen Sie sicher, dass zwischen dem vCenter Server und den ESXi Hosts keine Netzwerk-adressübersetzung (NAT, *Network Address Translation*) stattfindet.

Wenn Berechtigungen für Domänenmitglieder gesetzt werden sollen, muss der vCenter Server Mitglied der Domäne sein. Die Verbindung muss dann vor der Installation hergestellt werden, und er darf selbst kein Domänencontroller sein.

Wenn Sie Active Directory nutzen wollen, müssen Sie Mitglied der Administratoren oder Domänen-Admins sein. Während der Installation wird automatisch *Anmelden als Dienst*

und *Teil des Betriebssystems* eingerichtet. Die Probleme, die bei der Vorgängerversion diesbezüglich noch auftraten, sind mittlerweile bereinigt.

Softwarevoraussetzung ist das Microsoft DotNet 3.5 SP1 Framework. Ist es noch nicht vorhanden, wird es während der Installation installiert – das dauert aber sehr lange und braucht eine Verbindung zur Microsoft-Website.



Wenn Sie ein Betriebssystem einsetzen, das nicht englischsprachig ist, sollten Sie nach der Installation des DotNet Frameworks ebenfalls das dazugehörige Language Pack installieren. Auf dem DVD /ISO-Image ist nur die englische Version enthalten.

## vCenter Server Appliance

Statt einen vCenter Server als Anwendung auf einem Windows-Server-Betriebssystem zu installieren, kann man auch eine vorgefertigte Appliance (fertige virtuelle Maschine) dafür nehmen. Gerade in kleinen Umgebungen wird man die Einschränkungen gegenüber der erstgenannten Variante kaum bemerken: keine Möglichkeit, den verknüpften vCenter Server-Modus zu verwenden, kein IPv6 für die Kommunikation, mindestens ein ESX oder ESXi Host der Version 4.0, mindestens 7 GByte auf dem ESX(i) Storage (oder SAN) verfügbar.

Die Bereitstellung der vCenter Server Appliance werde ich im Anschluss an die Standardinstallation der vSphere-Komponenten erklären.

## Erforderliche Ports

Der vCenter Server benötigt bestimmte Ports zum Senden und Empfangen von Daten zwischen den verwalteten Hosts und von jedem vSphere Client aus. Die Quell- und Zielhosts müssen Daten untereinander austauschen können, um Migrations- und Bereitstellungsaktivitäten zwischen verwalteten Hosts zu ermöglichen.

Für die Kommunikation aller beteiligten Komponenten verwendet VMware bestimmte Ports im TCP/IP-Protokoll. Die beteiligten Hosts überwachen mithilfe von Agenten und Daemons (Diensten) einige Ports, die darüber Daten vom vCenter Server empfangen sollen. Falls sich zwischen den Hosts oder zwischen den Hosts und dem vCenter Server eine zusätzliche Firewall befindet, müssen Sie dafür Sorge tragen, dass die in Tabelle 10-11 aufgelisteten Ports offen sind. Während der Installation auf dem vCenter Server öffnet das Installationsprogramm die Ports der Windows Firewall normalerweise automatisch. Für benutzerdefinierte Firewalls auf dem vCenter Server müssen Sie die erforderlichen Ports gegebenenfalls manuell öffnen.

Die folgende Tabelle und der Abschnitt zu Port 80 im Anschluss sind der deutschsprachigen PDF-Datei *vsphere-esxi-vcenter-server-50-installation-setup-guide.pdf* von VMware entnommen (ab Seite 37).

Tabelle 10-11: Für die Kommunikation zwischen vSphere-Komponenten erforderliche Ports

| Port  | Beschreibung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 80    | <p>Wenn Sie eine benutzerdefinierte Microsoft SQL-Datenbank verwenden (nicht im Lieferumfang der SQL Server 2008-Datenbank enthalten), die auf demselben Hostcomputer wie der vCenter Server gespeichert ist, wird Port 80 vom SQL Reporting Service verwendet. Bei der Installation von vCenter Server werden Sie vom Installationsprogramm aufgefordert, den HTTP-Port für vCenter Server zu ändern. Ändern Sie den HTTP-Port für vCenter Server HTTP in einen benutzerdefinierten Wert, um eine erfolgreiche Installation zu gewährleisten.</p> <p>Microsoft Internet Information Services (IIS) verwendet ebenfalls Port 80 (siehe »Konflikt zwischen vCenter Server und IIS für Port 80« am Ende der Tabelle).</p>                                                                       |
| 389   | <p>Sowohl auf der lokalen als auch auf allen Remote-Instanzen von vCenter Server muss dieser Port geöffnet sein. Dies ist die LDAP-Portnummer für die Verzeichnisdienste der vCenter Server-Gruppe. Das vCenter Server-System benötigt auch dann eine Bindung mit Port 389, wenn Sie diese vCenter Server-Instanz nicht mit einer Gruppe im verknüpften Modus verbinden. Wenn auf diesem Port ein anderer Dienst ausgeführt wird, ist es in manchen Fällen empfehlenswert, ihn zu löschen oder einen anderen Port zuzuweisen. Sie können den LDAP-Dienst auf jedem Port zwischen 1025 und 65535 ausführen.</p> <p>Sofern diese Instanz als das Microsoft Windows Active Directory dient, ändern Sie die Portnummer von 389 in die Nummer eines verfügbaren Ports zwischen 1025 und 65535.</p> |
| 443   | <p>Der Standardport, den das vCenter Server-System zum Überwachen von Verbindungen vom vSphere-Client verwendet. Öffnen Sie Port 443 in der Firewall, um dem vCenter Server-System den Empfang von Daten vom vSphere-Client zu ermöglichen.</p> <p>Das vCenter Server-System verwendet ebenfalls Port 443 zur Überwachung der Datenübertragung zwischen SDK-Clients.</p> <p>Wenn Sie eine andere Portnummer für HTTPS-Übertragungen verwenden, müssen Sie bei der Anmeldung an das vCenter Server-System das Format IP-Adresse:Port verwenden.</p>                                                                                                                                                                                                                                            |
| 636   | <p>Im Falle des verknüpften Modus von vCenter Server ist dies der SSL-Port der lokalen Instanz. Wenn auf diesem Port ein anderer Dienst ausgeführt wird, ist es in manchen Fällen empfehlenswert, ihn zu löschen oder einen anderen Port zuzuweisen. Sie können den SSL-Dienst auf jedem Port zwischen 1025 und 65535 ausführen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 902   | <p>Der Standardport, den das vCenter Server-System zum Senden von Daten an verwalteten Hosts verwendet. Verwaltete Hosts senden außerdem regelmäßig Taktsignale über den UDP-Port 902 an das vCenter Server-System. Dieser Port darf nicht durch Firewalls zwischen dem Server und den Hosts bzw. zwischen Hosts blockiert werden.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 902   | <p>Port 902 darf nicht zwischen dem vSphere-Client und den Hosts blockiert werden. Der vSphere-Client verwendet diesen Port zur Anzeige der Konsolen von virtuellen Maschinen.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| 8080  | Web Services HTTP. Für VMware VirtualCenter Management Webservices verwendet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 8443  | Web Services HTTPS. Für VMware VirtualCenter Management Webservices verwendet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 60099 | Webservice-Port für den Änderungsbenachrichtigungsdienst                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| 10443 | vCenter Inventory Service HTTPS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 10109 | vCenter Inventory Service-Verwaltung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| 10111 | vCenter Inventory Service-Kommunikation im verknüpften Modus                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

### Konflikt zwischen vCenter Server und IIS für Port 80

Sowohl vCenter Server als auch Microsoft Internet Information Service (IIS) verwenden Port 80 als Standardport für direkte HTTP-Verbindungen. Dieser Konflikt kann zur

Folge haben, dass vCenter Server nach der Installation von vSphere Authentication Proxy nicht neu gestartet werden kann.

#### Ursache

Wenn IIS bei der Installation von vSphere Authentication Proxy nicht installiert wurde, werden Sie aufgefordert, IIS zu installieren. Da IIS Port 80 verwendet, der auch als Standardport für die direkten HTTP-Verbindungen von vCenter Server dient, wird vCenter Server nach Abschluss der Installation von vSphere Authentication Proxy nicht neu gestartet.

#### Lösung

Um einen Konflikt zwischen IIS und vCenter Server hinsichtlich Port 80 zu beheben, führen Sie eine der folgenden Aktionen durch:

Wenn Sie IIS vor der Installation von vCenter Server installiert haben, ändern Sie den Port für direkte HTTP-Verbindungen von vCenter Server von 80 auf einen anderen Wert.

Wenn Sie vCenter Server vor der Installation von IIS installiert haben, ändern Sie vor dem Neustart von vCenter Server den Bindungsport der IIS-Standard-Website von 80 auf einen anderen Wert.

## Checkliste für die Installation des vCenter Servers

Damit Sie nicht ein neues System für die Installation des vCenter Servers nach seiner Installation aufsetzen müssen, habe ich hier eine Checkliste zusammengestellt, die Sie vorher berücksichtigen sollten:

- Mindesthardwareanforderungen erfüllt
- Mindestsoftwareanforderungen erfüllt
- Name im Betriebssystem schlüssig und max. 15 Zeichen
- Name über DNS vom vSphere Client und auch von den ESXi Hosts erreichbar (FQDN)
- Eintrag in DNS (Forward- und Reverse-Lookup-Zone) korrekt
- IP-Adresse statisch zugewiesen (möglichst)
- Installationsuser hat lokale administrative Berechtigungen
- Rechner ist kein Domänencontroller
- Rechner erreicht mindestens einen Domänencontroller
- Rechner ist Mitglied einer Domäne (optional, aber empfohlen)
- vorhandenes Datenbanksystem und Anmeldeinformationen dafür bekannt und DSN angelegt (optional, wenn SQL Express verwendet wird)
- kein NAT (Network Address Translation) zu den ESXi Servern
- ggf. Firewall-Ports offen

# Den vCenter Server installieren

Die Meinungen zu der Frage, ob der vCenter Server als eigenständige physische oder als virtuelle Maschine installiert werden soll, gehen ziemlich weit auseinander.

Was spricht dagegen, ihn virtuell zu betreiben? Sind die Daten auf einem Storage, auf den alle beteiligten ESXi Server zugreifen können, kann der vCenter Server schnell wieder reaktiviert werden, falls es zu einem Ausfall kommt. Über HA (*High Availability*) würde dieser beim Ausfall eines ESXi Servers auf einem anderen Host automatisch neu starten und seine Funktionen wieder aufnehmen. Bei einem Hardwareserver ist das nicht so einfach. Dann wäre es wohl leichter, ihn neu auf einer anderen Maschine zu erstellen (falls man noch eine übrig hat).

Alle Vorteile, die die Virtualisierung mit sich bringt, sind hier ebenfalls vorhanden! Sie können Snapshots der Maschine erstellen und mit vMotion verschieben und auch jeden anderen Vorteil einer VM nutzen. Legen Sie einfach ein Backup des Servers (oder nur die \*.vmx-, die \*.vmxf- und beide \*.vmdk-Dateien) auf einen weiteren Datenträger, z.B. Software-iSCSI. Dann können Sie ihn direkt neu starten und mit Storage vMotion wieder auf einen schnelleren Datenträger überspielen. Warum also ein erhöhtes Risiko eingehen?

Selbst über Data Recovery gibt es die Möglichkeit, den vCenter Server wiederherzustellen, falls er nicht mehr läuft (siehe Kapitel 16).

Übrigens gibt es in der VMware-Community eine heiße Diskussion darüber, ob der vCenter Server nun virtuell oder physisch laufen sollte. VMware äußert sich dazu in seinen Dokumenten dahingehend, dass man auf die Vorteile einer VM nicht verzichten sollte.

Legen Sie die DVD in das Laufwerk oder binden Sie das ISO-Image an die VM, um mit der Installation zu beginnen. Falls das in Abbildung 10-3 gezeigte Fenster nicht durch den Autostart erscheint, klicken Sie auf Ihr DVD-Laufwerk und starten die Datei *autorun.exe*.



Abbildung 10-3: Startbild zur Installation

Überlegen Sie sich, ob Sie den vSphere Client auf dem vCenter Server benötigen. Wenn Sie per Remote über RDP zugreifen, ist das sinnvoll, ansonsten können Sie natürlich über ihren lokalen vSphere Client oder über Web Access auf den Server zugreifen.

1. Klicken Sie auf den Link **VCENTER SERVER**.
2. Wählen Sie für die Installation eine Sprache aus. Der Server wird anschließend nicht unbedingt in dieser Sprache angezeigt, das hängt von den Ländereinstellungen in Ihrem System ab. Es gibt aber, wie schon in Kapitel 4 erwähnt, die Möglichkeit, den vSphere Client mit definierter Sprache (-locale) aufzurufen.
3. Akzeptieren Sie die Patent- und Lizenzvereinbarung und klicken Sie auf **WEITER**.
4. Entscheiden Sie sich jetzt für den 60-Tage-Testmodus oder geben Sie hier schon Ihre Lizenzdaten ein. Das können Sie aber auch später in der grafischen Oberfläche nachholen.
5. Im nächsten Fenster müssen Sie eine Entscheidung bezüglich der Datenbank treffen. Für kleine Umgebungen mit bis zu fünf ESXi Servern und ca. 50 VMs reicht die freie SQL-Version von Microsoft aus. Sie können aber auch einen bereits vorhandenen SQL-, DB2- oder Oracle-Datenbankserver dafür nehmen.



Sollten Sie eine Fehlermeldung bekommen, dass der Name (FQDN) nicht aufgelöst werden kann, brechen Sie die Installation ab und beseitigen Sie zuerst diesen Fehler, sonst kann es anschließend zu gravierenden Problemen kommen. Überprüfen Sie z. B. mit *nslookup*, ob der DNS-Server antwortet.

6. Wählen Sie die Authentifizierungsmethode für den Zugriff auf Ihre Datenbank. Die Windows-Konto-Methode verlangt nach administrativen Berechtigungen möglichst im Format *Domäne\Username*. Am einfachsten belassen Sie es beim Systemkonto. Klicken Sie auf **WEITER**.
7. Suchen Sie sich einen Speicherort für die Programme und die Datenbank aus. Meist wird dieser wohl in *C:\Programme\* oder *C:\Program Files\* liegen.



Wenn Sie die vCenter Server-Programme auf einem anderen Laufwerk als *C:\* installieren möchten, achten Sie darauf, dass der Ordner *C:\WINDOWS\Installer* über genügend Speicherplatz verfügt, um die Installationsdatei (.msi) von Windows Installer zu installieren. Ist nicht genügend Speicherplatz verfügbar, scheitert die Installation.

8. Wählen Sie **INSTANZ FÜR EIGENSTÄNDIGES VMWARE VCENTER SERVER-PRODUKT ERSTELLEN** oder **GRUPPE BEITRETEN** aus (siehe Abbildung 10-4) und klicken Sie auf **WEITER**. Wenn Sie das Beitreten zu einer Gruppe für den verknüpften Modus wählen, können Sie im vSphere Client Daten über mehrere vCenter Server-Systeme hinweg anzeigen lassen, suchen und verwalten. Das lässt sich auch noch später erledigen.

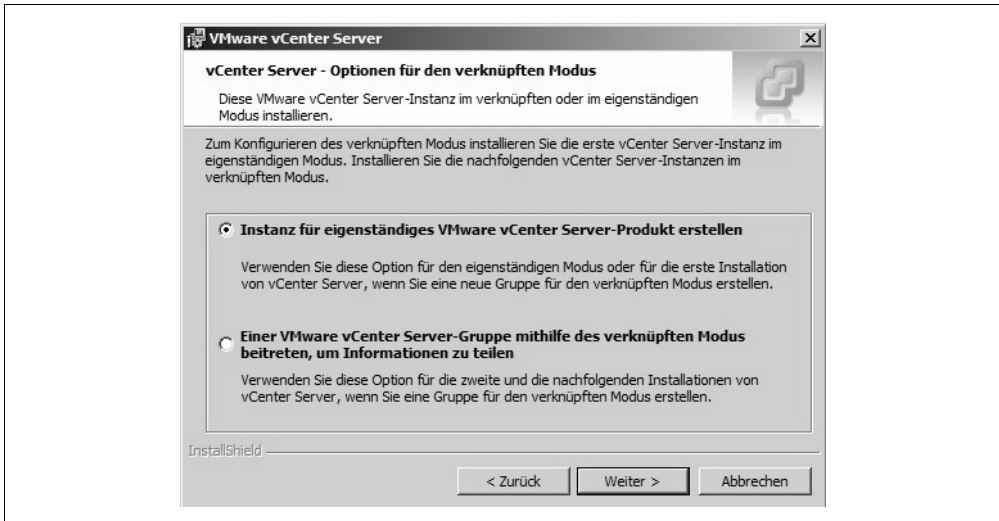


Abbildung 10-4: vCenter Server: verknüpfter Modus



Diese Option wird nicht angezeigt, wenn Sie ein Upgrade des VirtualCenter- oder vCenter-Datenbankschemas durchführen. Wird sie nicht angezeigt, können Sie nach Abschluss der Installation einer Gruppe im verknüpften Modus beitreten. Wenn Sie einer Gruppe von vCenter Servern beitreten wollen, können Sie den voll qualifizierten Domännennamen oder die IP-Adresse und die LDAP-Portnummer eines Remote-vCenter Server-Systems eingeben.



Sollten Sie eine Fehlermeldung beim verknüpften Modus für einen Windows Server 2008 64-Bit bekommen, schalten Sie das User Account Control (UAC) kurzfristig unter CONTROL PANEL → USER ACCOUNTS (Systemsteuerung) aus, verknüpfen Sie Ihre vCenter Server und schalten es wieder an.

9. Im nächsten Fenster (siehe Abbildung 10-5) werden einige der in Tabelle 10-11 beschriebenen Portnummern abgefragt. Ziehen Sie die Tabelle zurate, wenn Probleme wie Doppelbelegungen mit einem Port genannt werden. Die Ports für den Inventory Service werden im nächsten Fenster separat abgefragt.
10. In dem Fenster für den JVM-Arbeitsspeicher (u. a. für den Webservice *Tomcat*) wählen Sie eine der drei Möglichkeiten aus. Eine kleine Umgebung umfasst hier weniger als 100 ESXi Server und maximal 1.000 VMs.
11. Nachdem Sie auf WEITER geklickt haben, können Sie noch ein Häkchen bei den flüchtigen (temporären) Ports setzen. Das ist aber nur notwendig, wenn Sie mehr als 2.000 VMs gleichzeitig einschalten wollen, z.B. über einen View Manager. Ein

erneutes Klicken auf INSTALLIEREN startet die Installation, wobei einige Laufbalken angezeigt werden. Je nachdem, was Sie vorher schon auf Ihrem System installiert hatten und welche Datenbank Sie nehmen, kann sicher der eine oder andere Kaffee getrunken werden.

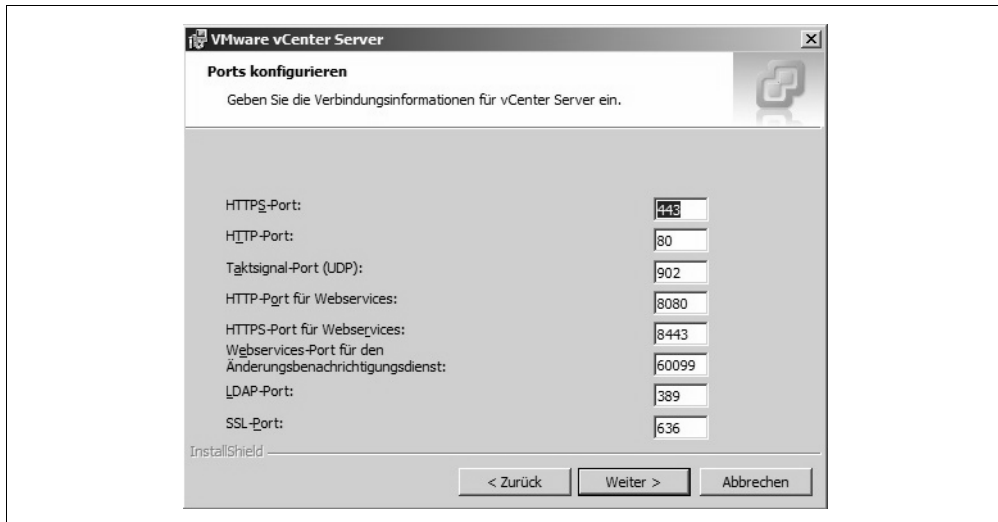


Abbildung 10-5: Auswahl der Ports



Wenn die Installation beendet ist, lesen Sie den Text im sich öffnenden Fenster genau durch. Achten Sie darauf, ob dort *erfolgreich installiert* oder *nicht erfolgreich installiert* steht.

## Installation des vCenter Orchestrator

Die Installation von vCenter Orchestrator geschieht gänzlich unbemerkt im Hintergrund. Lediglich nach der Installation des vCenter Servers sieht man einen zusätzlichen Dienst mit Namen *VMware vCenter Orchestrator Configuration* und im Startmenü unter PROGRAMME drei neue Einträge hierzu. Der Orchestrator ist eine Workflow-Engine (Automatisierung von Prozessen), also ein Modul mit einem umfangreichen Satz von Tools zur Verwaltung der virtuellen IT-Umgebung, die noch durch Plugins erweitert werden können. Einige Drittanbieter haben weitere Applikationen für den Orchestrator im Angebot. VMware Orchestrator koordiniert nicht nur Automatisierungsaufgaben über mehrere VMware-Produkte, sondern auch einige Management- und Verwaltungslösungen von anderen Anbietern. Weiterhin bietet er eine Bibliothek von Tools für den Zugriff auf die vCenter Server-API (*Application Programming Interface*).

Die im ersten Fenster (bei *autorun.exe* in Abbildung 10-3) angezeigten Komponenten, die Sie jetzt ebenfalls installieren können, werden nachfolgend besprochen und dann installiert.



## Installation des vSphere Client

Die Installation und Konfiguration des vSphere Clients wurde bereits in Kapitel 4 ausführlich behandelt, weshalb ich sie hier nicht noch einmal besprechen werde. Überlegen Sie sich, ob es nicht sinnvoll wäre, den Client auch auf dem vCenter Server zu installieren, damit Sie z.B. mit Remote Desktop von überall aus (lokales LAN, VPN-Verbindung von zu Hause etc.) die Umgebung bearbeiten können.

## Installation des vSphere Web Client (Server)

Der vCenter Web Client ist eine 64-Bit-Erweiterung für den vCenter Server. Mit ihm können Sie auf die über den vCenter Server verwalteten Hosts und VMs per Browser zugreifen.

Bevor Sie den Web Client installieren können, muss .NET Framework 3.5 SP1 und der Adobe Flash Player (10.1 oder höher) installiert sein. Als Browser werden Internet Explorer 7 und 8 sowie Firefox Version 3.6 unterstützt. Dafür sind die HTTP- und HTTPS-Ports 9090 und 9443 notwendig.

Die weitere Installation läuft ähnlich wie beim vCenter Server ab und wird hier nicht extra detailliert wiedergegeben.

Nach der Installation wird der Standardbrowser automatisch gestartet und die Webseite *<https://localhost:9443/admin-app/>* aufgerufen. Haben Sie den Adobe Flash Player noch nicht installiert, kommt eine Seite mit dem entsprechenden Hinweis.

Zunächst erhalten Sie eine fast leere Seite, da der (lokale) vCenter Server erst noch registriert werden muss. Dafür und für den Web Client Server können Sie den Namen, den FQDN oder die IP-Adresse verwenden. Anschließend müssen Sie noch das Zertifikat abnicken (ignorieren). War die Registrierung erfolgreich, können Sie in der Zeile der URL statt */admin-app/* die Seite mit dem vSphere-Client abrufen, also z.B. *<https://localhost:9443/vsphere-client/>*, und sich dort mit den Anmeldeinformationen Zugang zum vCenter Manager verschaffen. Die Abmeldung befindet sich übrigens etwas versteckt unter Ihrem Namen in der obigen blauen Leiste.

Wenn unsere Umgebung fertig ist, alle ESXi Server in einem Cluster stecken und die virtuellen Maschinen laufen, kommen wir zu diesem Punkt nochmals zurück.

## Den Update Manager installieren

Der vCenter Update Manager ist für Umgebungen mit dem vCenter Server gedacht. Mit ihm können Sie die einzelnen Hosts, Appliances und virtuellen Maschinen auf eine neuere Version bringen oder die z.B. bei VMware, Linux und Microsoft regelmäßig erscheinenden Updates und Patches einspielen.

Der Update Manager darf erst nach der Installation des vCenter Servers installiert werden, weil während seiner Installation die Zugangsdaten zum vCenter Server überprüft

werden. Installieren Sie das Paket auf der Maschine des vCenter Servers oder auf einer Maschine, die ihn über das Netzwerk erreicht. Sie müssen sich für die Konfiguration und Bedienung des Update Managers anschließend noch das Plugin für Clientkomponenten herunterladen und installieren.

Der Update Manager braucht eine Datenbank für die Informationen, die er über das Internet bezieht. Die Datenbankanforderungen sind nicht mit denen des vCenter Servers identisch, da dieser ein 64-Bit-DSN nutzt und nicht wie der Update Manager ein 32-Bit-DSN. Sie können wie vorher beim vCenter Server eine vorhandene Datenbank verwenden oder eine neue Microsoft SQL 2008 Express-Datenbank installieren, die mit dem Paket mitgeliefert wird. Nehmen Sie aus Performancegründen nicht die gleiche Datenbank wie für den vCenter Server.

Die Installation unterscheidet sich kaum von den bereits beschriebenen, weshalb hier nur die Besonderheiten behandelt werden.

Die Verbindungsinformationen für das vCenter Server-System müssen eingegeben werden, weil der Update Manager hier als Erweiterung hinzugefügt wird (siehe Abbildung 10-6).

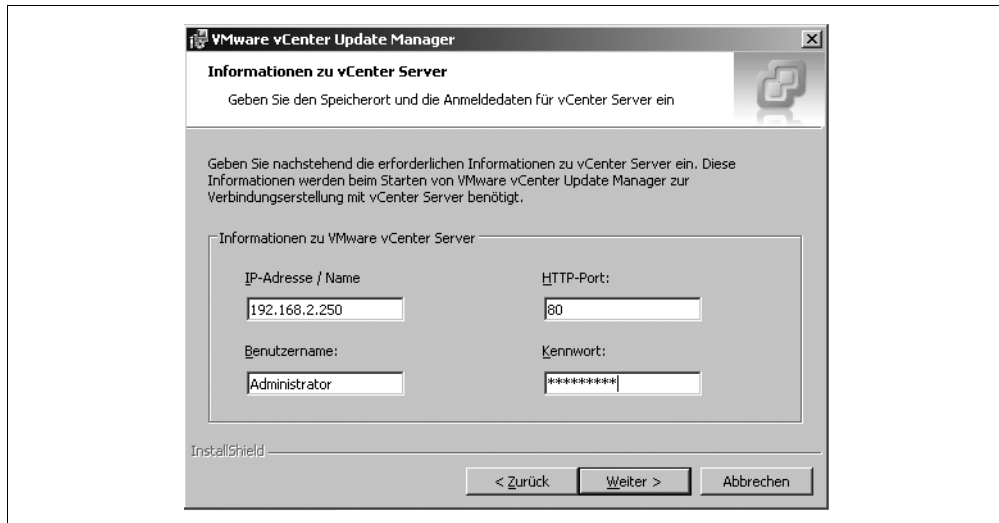


Abbildung 10-6: Informationen für den Update Manager

Sie können die Option JA, ICH VERFÜGE ÜBER EINE INTERNETVERBINDUNG UND MÖCHTE DIE PROXY-EINSTELLUNGEN JETZT KONFIGURIEREN auswählen oder die Informationen später über den vCenter Server eingeben, wenn Sie sich das Plugin auf Ihrem Rechner installiert haben.

Sie brauchen dafür den Namen des Proxy-Servers und seine Portnummer. Wenn auf der lokalen Maschine Proxy-Einstellungen konfiguriert sind, verwendet das Installationsprogramm standardmäßig diese. Gegebenenfalls können Sie PROXY ANHAND DER NACHFOL-

GENDEN ANMELDEDATEN AUTHENTIFIZIEREN auswählen und den Benutzernamen und das Kennwort für die Authentifizierung eingeben. Diese Informationen benötigt der Update Manager, um Definitionen, Patches und Updates von VMware und Microsoft herunterladen zu können.

Der Standardspeicherort für die Patch-Downloads ist meistens ungünstig gewählt, speichern Sie sie lieber an einem anderen Ort, an dem mindestens 20 GByte freier Platz vorhanden sind. Die ansonsten folgende Warnmeldung bekommen Sie nicht, wenn ihr Laufwerk mehr als 120 GByte freien Speicher hat. Wenn Sie später im Update Manager die sogenannten *Baselines* (Grundeinstellungen für Updates) bearbeiten, können Sie sich z.B. dafür entscheiden, alle ESX(i)-Updates und -Patches herunterzuladen und die VM-Updates und -Patches über einen anderen Weg zu verteilen (WSUS-Server) – dann reichen die oben angegebenen 20 GByte für lange Zeit aus.

## vCenter Support-Tools

Insgesamt vier weitere Tools stehen für die Installation über die DVD oder das ISO-Image zur Verfügung. Einiges davon ist durch neue Funktionen in der Version 5 notwendig geworden und dadurch, dass der bisherige ESX Server auf Linux-Basis nicht mehr vorhanden ist.

### VMware ESXi Dump Collector

Zum Sammeln von Arbeitsspeicher-Informationen auf einem Netzwerklaufwerk bei einem möglichen Absturz wird dieses Tool gegebenenfalls benötigt. Hat der ESXi Server nicht genügend eigenen freien lokalen Storage zur Verfügung oder wurde ein Auto Deployment genutzt, sollte man den Dump Collector einsetzen. Dieser muss zwar nicht auf dem vCenter Server installiert werden, aber über das Netzwerk Zugriff auf diesen haben. Auch dieser Dienst bietet keine Unterstützung von IPv6, muss also über IPv4 auf den vCenter Server zugreifen können.

Während der Installation wird man aufgefordert, eine Portadresse und den Speicherort im Netzwerk anzugeben, an dem sich die Informationen der beteiligten Hosts befinden.

### VMware Syslog Collector

Mit dem Syslog Collector können Sie System- und Netzwerkprotokolle mehrerer ESXi Server an einen beliebigen Netzwerkspeicherort (Repository) umleiten. Dieser muss ebenfalls nicht auf dem vCenter Server installiert werden, aber Zugriff über das Netzwerk auf diesen haben. Auch dieser Dienst bietet keine Unterstützung von IPv6, muss also über IPv4 auf den vCenter Server zugreifen können.

Während der Installation werden der Port, das Protokoll (TCP oder UDP) und die Anzahl der beizubehaltenden Austauschprotokolle abgefragt. Beachten Sie dabei den dafür notwendigen Speicherplatz auf der Netzwerkfreigabe.

## VMware vSphere Auto Deploy

Mit dem vSphere Auto Deploy haben Sie die Möglichkeit, ESXi Server in Ihrer Netzwerkumgebung zu installieren und anzupassen. Dafür benötigen Sie das Image des ESXi Servers, das direkt in den Arbeitsspeicher geladen wird. In großen Umgebungen kann diese Anwendung binnen kurzer Zeit etliche neue ESXi Server bereitstellen. Dieser Dienst unterstützt – im Gegensatz zu den zwei erstgenannten – sowohl IPv4 als auch IPv6.

Während der Installation müssen Sie wiederum eine Portnummer und das Auto Deploy Repository angeben. Dieses muss mindestens 350 MByte freien Platz haben und darf nicht auf einer Netzwerkreigabe liegen.

## VMware vSphere Authentication Proxy

Der Authentication Proxy erlaubt den ESXi Servern den Beitritt zu einer Active Directory-Domäne, ohne die Anmeldeinformationen des AD zu kennen. Das ist ein Sicherheitsfeature, das zum Beispiel für Hosts genutzt werden kann, die über Auto Deploy installiert werden. Damit müssen die Anmeldeinformationen in keinem Installationskript auftauchen. Dieser Dienst bietet ebenfalls keine Unterstützung für IPv6, muss also über IPv4 auf den vCenter Server zugreifen können.

Als Voraussetzung muss vorher das vSphere Auto Deploy installiert sein, aber nicht notwendigerweise auf derselben Maschine, wohl aber in der gleichen Domäne. Wollen Sie diesen Dienst unter Windows Server 2008 R2 installieren, sollten Sie vorher den KB-Artikel 981506 beachten und den dort erwähnten Hotfix installieren (falls noch nicht geschehen).

Während der Installation wird ein zusätzliches Domänenkonto für den Dienst erstellt. Der Name beginnt mit CAM-, und es wird ein 32-stelliges zufälliges Kennwort erstellt, das nie abläuft. Ändern Sie das Kennwort und die Einstellungen nicht manuell.

## Nach der Installation

Der vCenter Server ist ein Dienst. Um zu überprüfen, ob er korrekt läuft, rufen Sie die Liste der Windows-Dienste auf und überprüfen, ob der Dienst gestartet wurde. Im Hintergrund ist noch die alte Bezeichnung »VirtualCenter Server« zu sehen. Auch bei anderen Gelegenheiten sieht man noch Begriffe von VMware Infrastructure 3.

Folgende Dienste werden bei der vollständigen Installation aller Komponenten des vSphere auf dem vCenter Server bereitgestellt (siehe Abbildung 10-7):

- *vCenter Inventory Service*: Java Service Wrapper. Von diesem Dienst ist der vSphere Profile-Driven Storage Service abhängig.
- *VMware USB Arbitration Service*: Ermöglicht einer VM, USB Geräte über den vSphere Client anzuschließen.
- *VMware vCenter Orchestrator Configuration*: Webzugriff für den Orchestrator.

| Name                                          | Beschreibung      | Status    | Starttyp   | Anmelden als   |
|-----------------------------------------------|-------------------|-----------|------------|----------------|
| vCenter Inventory Service                     | vCenter Inve...   | Gestartet | Automat... | Lokales System |
| VMware Snapshot Provider                      | VMware Snap...    |           | Manuell    | Lokales System |
| VMware Syslog Collector                       | Unterstützt d...  | Gestartet | Automat... | Lokales System |
| VMware Tools Service                          | Bietet Unters...  | Gestartet | Automat... | Lokales System |
| VMware USB Arbitration Service                |                   | Gestartet | Automat... | Lokales System |
| VMware vCenter Orchestrator Configuration     | VMware vCe...     |           | Manuell    | Lokales System |
| VMware VirtualCenter Management Webservices   | Allows config...  | Gestartet | Automat... | Lokales System |
| VMware VirtualCenter Server                   | Ermöglicht di...  | Gestartet | Automat... | Lokales System |
| VMware vSphere Auto Deploy Waiter             | Bietet Startk...  | Gestartet | Automat... | Lokales System |
| VMware vSphere Profile-Driven Storage Service | VMware vSph...    | Gestartet | Automat... | Lokales System |
| VMware vSphere Update Manager UFA-Dienst      | Der VMware ...    |           | Manuell    | Lokales System |
| VMware vSphere Update Manager-Dienst          | VMware vSph...    | Gestartet | Automat... | Lokales System |
| VMwareVCMSDS                                  | Bietet VMwar...   | Gestartet | Automat... | Netzwerkdienst |
| Volumeschattenkopie                           | Verwaltet un...   |           | Manuell    | Lokales System |
| vSphere ESXi Dump Collector                   | Unterstützt d...  | Gestartet | Automat... | Lokales System |
| vSphere ESXi Dump Collector Web Server        | Stellt die Kon... | Gestartet | Automat... | Lokales System |
| vSphere Web Client                            | VMware vSph...    | Gestartet | Automat... | Lokales System |

Abbildung 10-7: Liste der Dienste auf dem vCenter Server

- *VMware VirtualCenter Management Webservice*: WebAccess auf VMs und Hosts über den vCenter Server (Tomcat).
- *VMware VirtualCenter Server*: Zentrale Verwaltung der gesamten Umgebung.
- *VMware vSphere Profile-Driven Storage Service*: Dienst, der das VM-Speicherprofil ermöglicht.
- *VMware vCenter Update Manager UFA-Dienst*: Wird für das Anschließen von VM-Festplatten zur Überprüfung benötigt.
- *VMware vCenter Update Manager Dienst*: Wird für Updates von VMs und Hosts benötigt.
- *VMware VCMSDS*: Ermöglicht Zugriff über LDAP auf Active Directory.
- *VMware Mount Service for VirtualCenter*: Dient zum Anbinden von Festplatten der VMs als Ordner im Explorer (z.B. bei Data Recovery).
- *vSphere Web Client*: Web Access über den vCenter Server auf die ESXi Hosts.

Wenn Sie den vCenter Server als virtuelle Maschine aufgesetzt haben, laufen folgende Dienste von VMware zusätzlich auf dem Rechner:

- *VMware Snapshot Provider*: Unterstützt Snapshots der VM, z.B. zur Datensicherung.
- *VMware Tools Dienst*: Service für die VMware Tools, u.a. Unterstützung von Maus, Tastatur, Heartbeat usw.
- *VMware-Upgrade-Hilfsprogramm*: Notwendiger Dienst für das Upgraden der virtuellen Hardware, z.B. von Version 7 auf 8.

Sollten Sie die vCenter Support-Tools ebenfalls installiert haben, kommen folgende Dienste von VMware dazu:

- *vSphere ESXi Dump Collector*: Unterstützt das Erfassen von Core-Dumps von Remote-Hosts.
- *vSphere ESXi Dump Collector Web Server*: Stellt die Konfiguration und die Dateninformation für vSphere ESXi Dump Collector Server bereit.
- *VMware Syslog Collector*: Unterstützt das Erfassen von Systemprotokollen von Remote-Hosts.
- *VMware vSphere Auto Deploy Waiter*: Komponente für das Installieren von ESXi Hosts über PXE und ihre Startkonfiguration.
- *VMware vSphere Authentication Proxy (bedingt IIS)*: Dienst für Auto Deploy und den Zutritt der Hosts zur AD-Domäne.

Anschließend können Sie über den vSphere Client auf den Server zugreifen. Wenn z.B. auf Ihrem Rechner mit der IP 192.168.50.100 der Server installiert wurde, lautet der Aufruf lokal wie in Abbildung 10-8:



Abbildung 10-8: vSphere Client-Aufruf

Sie können hierüber alle ESXi Server konfigurieren. Natürlich ist es mit dem vSphere Client auch möglich, einen einzelnen Server aufzurufen und nur diesen zu konfigurieren oder neue virtuelle Maschinen zu erstellen.

## vCenter Server Appliance bereitstellen

Wie bereits erwähnt, gibt es von VMware eine auf SuSE Linux 11 basierende fertige virtuelle Maschine, die man sich von deren Webseite als OVF-Datei herunterladen kann. Sie kann anstatt des auf einem 64-Bit-Windows-Server zu installierende Applikation genutzt werden, hat allerdings ein paar Einschränkungen gegenüber der Windows-Variante:

- keine Unterstützung von Datenbanken von Microsoft (SQL) und IBM (DB2)
- keine Unterstützung von reinem IPv6 (IPv4 ist immer möglich)
- keine Unterstützung des verknüpften Modus für den vCenter Server
- kein integrierter Update Manager
- VSA Storage wird nicht unterstützt

Diese virtuelle Maschine wurde von VMware für den Gebrauch als vCenter Server optimiert. Sie können sich als Standardbenutzer *root* mit dem Passwort *vmware* (alles kleingeschrieben) an diesem Rechner anmelden oder sich über den vSphere Client nach der Bereitstellung auf einem ESXi oder ESXi Host mit der Version 4.x oder 5.0 damit verbinden. Als freien Festplattenspeicher benötigt diese Appliance mindestens 7 GByte freien Platz. Nehmen Sie das Thick-Format, sind es für die beiden Festplatten (22 und 60 GByte) und den Arbeitsspeicher beim Einschalten (.vswp-Datei von 8 GByte) insgesamt also 80 GByte benötigter Speicher.

Achten Sie beim Herunterladen darauf, dass die Appliance mit zwei Festplatten geliefert wird. Die OVF-Datei und die beiden VMDK-Dateien müssen sich im selben Ordner befinden, damit sie bei der Bereitstellung gefunden werden.

Auf dem Host können Sie über das Menü DATEI → OFV-VORLAGE BEREITSTELLEN anschließend nach dem Speicherort browsen und die OVF-Datei auswählen. Bestätigen Sie im Assistenten die einzelnen Seiten, bis die neue virtuelle Maschine in Ihrer Bestandsliste auftaucht.

Konfigurieren Sie die Appliance vor dem ersten Einschalten:

- Als Arbeitsspeicher reichen 4 GByte aus, wenn Sie nicht mehr als 10 ESXi Server und 100 VMs in die Bestandsliste aufnehmen möchten. 8 GByte reichen für 100 Hosts und 1.000 VMs, 13 GByte für 400 ESXi Server und 4.000 VMs und 17 GByte oder mehr für alles darüber.
- Die Grafikkarteneinstellung sollten Sie auf automatisch setzen.
- Überprüfen Sie die Einstellungen bei CD/DVD-Laufwerk und Netzwerkkarte.

Nach dem Einschalten sucht sich das System eine DHCP-Adresse. Überlegen Sie sich, ob Sie diese behalten (169.254.x.y, APIPA wird nicht empfohlen) oder doch lieber eine statische vergeben möchten. Das geht ganz einfach über das Menü CONFIGURE NETWORK, das nach dem Start angezeigt wird. Wenn Sie mit den Vorgaben des Assistenten einverstanden sind, können Sie sie direkt mit Return bestätigen. Bedenken Sie dabei, dass das Tastaturlayout englisch ist, Sie also auf der Tastatur »z« drücken müssen, wenn Sie »y« meinen.

Haben Sie die IP-Informationen gesetzt oder die per DHCP bekommenen akzeptiert, sollten Sie noch die Zeitzone auf den korrekten Wert einstellen – das geht aber auch hinterher über die Webseite. Anschließend müssen Sie sich über einen Webbrowser verbinden, um noch einige Einstellungen zu machen. Eine Anmeldung mit dem vSphere Client ist vorher nicht möglich. Beachten Sie dabei, dass die Webseite nur angezeigt wird, wenn Sie den vollständigen Kontext, also <https://<IP-Adresse>:5480> angeben. Ohne das »s« bei https und die Portnummer 5480 funktioniert es nicht.

Weitere Vorgehensweise:

- Loggen Sie sich als User *root* mit dem Passwort *vmware* an.

- Akzeptieren Sie die EULA, indem Sie auf die Schaltfläche ACCEPT EULA klicken. Haben Sie Geduld, bis der Status auf ACCEPTED springt. Falls es bei Ihnen nicht funktioniert, rollen Sie mit dem Laufbalken ganz nach unten und klicken Sie nochmals auf die Schaltfläche.
- Klicken Sie anschließend auf das Kästchen mit dem Wort DATABASE. Als Typ können Sie beim Drop-down-Feld ORACLE oder EMBEDDED auswählen. Haben Sie EMBEDDED gewählt, lassen sich die Felder darunter nicht ausfüllen. Diese Version der Datenbank reicht für 100 ESXi Server und ca. 1.000 VMs.
- Klicken Sie anschließend unter ACTIONS auf den Button TEST SETTINGS. Kurze Zeit später sollte im linken Feld in grüner Schrift OPERATION WAS SUCCESSFUL erscheinen. Vergessen Sie nicht, SAVE SETTINGS anzuwählen, sonst ist die Auswahl verloren. Über RESET DB CONTENTS wird der Inhalt der Datenbank gelöscht.
- Wählen Sie als Nächstes den Punkt SETTINGS und suchen Sie aus dem dortigen Drop-down-Feld die Größe Ihrer Umgebung aus. Die Ports brauchen üblicherweise nicht geändert zu werden. Wie vorher können Sie die Einstellungen testen und abspeichern.
- Unter ADMINISTRATION lassen sich ein neues Passwort für den User *root* festlegen (empfohlen) und der Remote-Zugriff über ssh ein- und ausschalten. Als Standard darf sich der Administrator (User *root*) schon über ssh anmelden.

Weitere Einstellungen sind erst einmal nicht notwendig. Jetzt können Sie unter dem Eintrag VCENTER SERVER die zweite Schaltfläche anklicken, den vCenter Server Dienst starten und sich anschließend über den vSphere Client anmelden.

Da der Update Manager nicht enthalten ist, können Sie diesen nach der Bereitstellung und Konfiguration der Appliance auf einer Windows-Maschine installieren. Während seiner Installation brauchen Sie die Zugangsdaten zum vCenter Server, deshalb geht es nicht umgekehrt. Installieren Sie das Paket auf einer beliebigen Maschine, die über das Netzwerk den vCenter Server erreicht. Sie müssen sich für die Konfiguration und Bedienung des Update Managers anschließend noch das Plugin für Clientkomponenten herunterladen und installieren.

Der Update Manager braucht ebenfalls eine Datenbank für die Informationen, die er über das Internet bezieht. Die Datenbankanforderungen sind nicht mit denen des vCenter Servers identisch, da dieser ein 64-Bit-System-DSN nutzt und nicht wie der Update Manager ein 32-Bit-DSN. Sie können eine vorhandene Datenbank verwenden oder eine neue Microsoft SQL 2008 Express-Datenbank installieren, die mit dem Paket mitgeliefert wird.

## vCenter Server-Lizenzen

In der Vorgängerversion gab es noch Lizenzdateien und den Lizenzmanager eines Drittherstellers (LMTools), der damals mit Infrastructure ausgeliefert wurde. Das hat



sich seit vSphere4 geändert: Im vCenter und auch beim ESXi Server werden 25 Zeichen umfassende Lizenzschlüssel eingetragen, in denen alle gekauften Funktionen enthalten sind (siehe Abbildung 10-9). Sollten Sie auf eine andere Version aufrüsten, wird der alte Schlüssel durch einen neuen ersetzt. Dies und das Zusammenfassen mehrerer einzelner Schlüssel geschieht gegebenenfalls über das Lizenzportal von VMware.

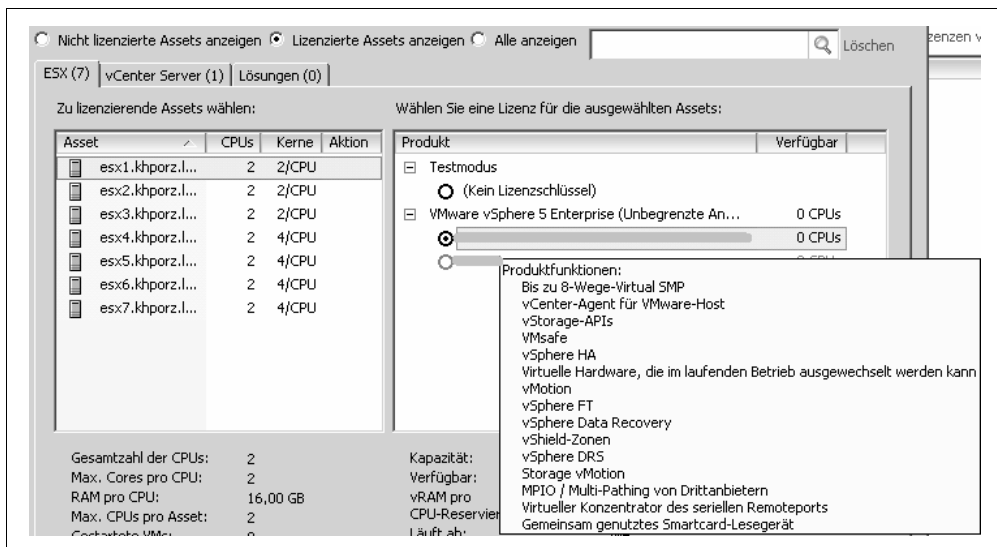
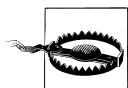


Abbildung 10-9: Lizenzen auf dem vCenter Server



Achten Sie unbedingt vor dem Kauf der Lizenzen auf Ihre Erfordernisse. Es werden sogenannte Bundles oder Kits angeboten, die nicht erweiterbar sind. Diese sind meist auf maximal sechs CPU-Sockel und drei Hosts beschränkt. Eine Erweiterung dazu gibt es nicht – Sie können aber (gegen Geld) zum nächsthöheren Produkt aufstocken. Das lohnt sich jedoch gegenüber einer normal erweiterbaren Struktur meistens finanziell nicht.

Informieren Sie sich vorher über die möglichen Funktionen (die z.B. am Anfang dieses Buchs behandelt wurden) und welche Sie davon brauchen. Gehen Sie dabei am besten die einzelnen zu virtualisierenden Rechner anhand von Worst-Case-Szenarien durch. Fragen Sie sich, für welchen Rechner Sie HA, DRS, vMotion, Storage vMotion, Fault Tolerance, verteilte vSwitches und Ähnliches einsetzen würden. Dann erst suchen Sie sich das passende Produkt heraus.



Schauen Sie sich vor dem Kauf neuer Lizenzen Ihre jetzigen an. Wenn Sie einen noch laufenden Supportvertrag haben, können Sie meist kostenlos auf eine neuere Version updaten.

## Grundlegendes zur Kapazität von Lizenzschlüsseln

Lizenzschlüssel besitzen eine bestimmte Kapazität. Diese basiert auf der Anzahl der Prozessorsockel im Host oder der Anzahl der Instanzen des Software-Assets (Softwarekomponenten wie vCenter Server) und den an die VMs zu verteilenden RAM (vRAM). Für eine Softwarekomponente – Asset-Instanz genannt – brauchen Sie nur eine Lizenz pro beteiligtem ESXi Host, unabhängig von seiner CPU-Sockelanzahl.

Für die meisten vSphere-Produkte müssen Sie beim Erwerb der vSphere-Lizenzen die gesamte Anzahl der Prozessoren berücksichtigen, nicht die Anzahl der Hosts, auf denen die Produkte ausgeführt werden. Sie können die Prozessorkapazität einer beliebigen Kombination von Hosts zuweisen. Angenommen, Sie kaufen einen vSphere-Lizenzschlüssel für zwölf Prozessoren, können Sie ihn einer beliebigen der folgenden Hostkombinationen zuweisen:

- 6 Hosts mit je 2 Prozessoren
- 4 Hosts mit 2 Prozessoren und 1 Host mit 4 Prozessoren
- 2 Hosts mit 4 Prozessoren und 2 Hosts mit 2 Prozessoren
- 1 Host mit 8 Prozessoren und 2 Hosts mit 2 Prozessoren

Beachten Sie dabei Folgendes:

- Prozessoren mit zwei oder mehr Kernen, z.B. Intel-Prozessoren, die zwei oder mehr unabhängige CPUs auf einem einzigen Chip kombinieren, gelten als ein Prozessor.
- Ein Host mit mehreren Prozessoren kann nicht teilweise lizenziert werden. Beispielsweise benötigt ein Host mit vier CPUs auch vier Prozessorlizenzen.



Aus Sicht der ESXi Lizenz ist eine CPU ein Prozessor, der auf einem Prozessorsockel steckt. Und: Jede Lizenz unterstützt beliebig viele Kerne pro CPU!

Die neue Lizenzierungsart mit dem vRAM hat einiges an Gegenwind für VMware ausgelöst. Nach dem Sturm der Entrüstung wurde dann ein wenig nachgebessert. Jetzt sieht es so aus, dass eine VM so viel Speicher bekommen kann, wie sie braucht. Es ist ein Maximum bei 96 GByte gesetzt: Wenn eine virtuelle Maschine 136 GByte RAM zugewiesen bekommen hat, zieht sie also aus dem gemeinsamen Pool nur 96 GByte heraus. So ein Pool besteht aus allen Lizenzen, die man gekauft hat. Nimmt man beispielsweise das Essentials Plus Kit, hat jede CPU-Lizenz gleichzeitig 32 GByte vRAM. Bauen wir einen Cluster mit drei Hosts und jeweils zwei CPU-Sockeln, kommen wir auf insgesamt  $6 \cdot 32 \text{ GByte} = 192 \text{ GByte}$  für den Cluster. Wie viel physischen Speicher Ihre ESXi Server haben, ist dabei unbedeutend.

Alle Lizenzen bis einschließlich vSphere Standard haben 32 GByte vRAM, Enterprise hat 64 GByte und Enterprise Plus 96 GByte pro CPU-Lizenz. Im vCenter Server befindet sich

ein zusätzliches Tool, das den jeweils genutzten vRAM der eingeschalteten Systeme zählt. Wenn Sie mehr RAM für Ihre VMs brauchen, können Sie entweder eine weitere CPU-Lizenz erwerben oder auf eine höhere Version aufrüsten.

## Lizenzierung der Betriebssysteme

Die Frage, wie es mit den Lizenzkosten in den virtuellen Maschinen aussieht, lässt sich leicht beantworten: Betrachten Sie alle Server wie physische Maschinen. Sie benötigen für jede lizenzpflichtige Software innerhalb einer virtuellen Maschine eine Lizenz. Auch jedes Hostsystem benötigt je nach Produkt eine Lizenz.

Reden Sie mit den Herstellern Ihrer Betriebssysteme bzw. Anwendungen. Die Erfahrung hat gezeigt, dass sich viele auf einen Kompromiss einlassen, also z.B. zehn Server, aber nur sieben Lizenzen. In Deutschland gilt nicht nur das »Buchprinzip« (also dass Sie eine Software oder ein Betriebssystem auf zwei Rechnern installieren können, wenn sichergestellt ist, dass nicht beide gleichzeitig in Betrieb sein können), sondern auch das Prinzip ein Betriebssystem pro Rechner!

Ein weiterer Streitpunkt kann die Lizenzierung bei der Anzahl der Prozessoren sein, da manche Hersteller nicht die Prozessoren innerhalb der virtuellen Maschine lizenzieren wollen, sondern das Wirtsystem. Hier hilft ein klärendes Gespräch mit dem jeweiligen Hersteller. Es empfiehlt sich darüber hinaus, mit dem Hersteller hinsichtlich seiner Preisvorstellung zu verhandeln, um so vielleicht die Kosten zu drücken.

## Logdateien des vCenter Servers

Da die Logdateien beim vCenter Server relativ zu ihren Umgebungsvariablen gespeichert werden, müssen diese Einstellungen zunächst überprüft werden. Auf der Kommandozeile kann der Befehl `set` dafür verwendet werden, sich die Informationen anzeigen zu lassen. Eine weitere Möglichkeit ist `SYSTEMSTEUERUNG → SYSTEM → ERWEITERT → UMGEBUNGSVARIABLEN`.

Die zweite Möglichkeit hat den Vorteil, dass man dort auch gleich Einstellungen verändern kann, die beim Neustart wieder vorhanden sind!

*Tabelle 10-12: Wichtige Einträge zu Umgebungsvariablen bis Server 2003*

| Variable          | Typischer Userwert                                                                    | Typischer Systemwert                        |
|-------------------|---------------------------------------------------------------------------------------|---------------------------------------------|
| %SystemRoot"      | C:\Windows                                                                            | C:\Windows                                  |
| %AllUsersProfile% | C:\Dokumente und Einstellungen\All Users                                              | C:\Dokumente und Einstellungen\All Users    |
| %UserProfile%     | C:\Dokumente und Einstellungen\%Username%                                             | C:\Dokumente und Einstellungen\Default User |
| %Tmp% %Temp%      | %UserProfile%\Lokale Einstellungen \Tmp\<br>%UserProfile%\Lokale Einstellungen \Temp\ | %SystemRoot%\Temp                           |

Tabelle 10-13: Wichtige Einträge zu Umgebungsvariablen ab Server 2008

| Variable          | Typischer Userwert                                                    | Typischer Systemwert |
|-------------------|-----------------------------------------------------------------------|----------------------|
| %SystemRoot"      | C:\Windows                                                            | C:\Windows           |
| %AllUsersProfile% | C:\ProgramData                                                        | C:\ProgramData       |
| %UserProfile%     | C:\Users\%Username%                                                   | C:\Users\Public      |
| %Tmp% %Temp%      | %UserProfile%\AppData\Local\Tmp\<br>%UserProfile%\AppData\Local\Temp\ | %SystemRoot%\Temp    |

Die so gesammelten Einträge in den textbasierten Dateien können über den vSphere Client oder einen Texteditor angezeigt werden.

## Logdateien zur Installation

Die Logdateien zur Installation des vCenter Servers können im *Temp*-Verzeichnis des Users gefunden werden, der die Installation durchgeführt hat, also z.B. *C:\Dokumente und Einstellungen\Ralph\Lokale Einstellungen\Temp* oder *C:\Users\Goepel\AppData\Local\VMware*.

Hat hingegen der Administrator die Installation durchgeführt, befinden sich die Dateien in *C:\Windows\Temp*, jedoch nur in der englischen Version. Beim deutschen Windows sind auch dann die Logdateien unter dem Userverzeichnis abgespeichert.

Tabelle 10-14: Mögliche Dateinamen der jeweiligen Logdateien

| Name der Logdatei                             | Beschreibung                                                 |
|-----------------------------------------------|--------------------------------------------------------------|
| <i>vim-vcs-msi.log</i>                        | Installations-Logdatei von vCenter Server und Unterprozessen |
| <i>vim-ngc-msi.log</i>                        | VMware vSphere Web Client-Installation                       |
| <i>vim-qs-msi.log</i>                         | vCenter Inventory Service                                    |
| <i>vmware-vci-vciInstallUtils-log4cpp.log</i> | Installations-Logdatei zur Vorbereitung des Update Managers  |
| <i>vim-um-msi.log</i>                         | Installations-Logdatei des Update Manager-msi-Pakets         |
| <i>vminst.log</i>                             | VMware Enterprise-Erweiterungen wie WebAccess                |
| <i>vmceservermsi.log</i>                      | VMware vCenter Converter-Installation                        |
| <i>vim-vci-msi.log</i>                        | vSphere Client-Installation                                  |

Im User-Temp-Verzeichnis befindet sich noch eine Logdatei für die Installation des VMware Orchestrators, und bei *C:\Dokumente und Einstellungen\<Benutzername> \ Lokale Einstellungen\Anwendungsdaten\vpv\viclient-n.log* oder *C:\Users\ <Benutzername>\AppData\Local\VMware\vpv\viclient-n.log* gibt es bis zu zehn Logdateien des vSphere Clients. Dabei werden diese Dateien fortlaufend von 0 bis 9 durchnummeriert. Die aktuelle Datei ist also die mit der höchsten Nummer. Ist man mehrfach angemeldet, kann die Datei *viclient-n-000x.log* auch mehrfach vorkommen.

Ist die höchste Nummer erreicht, wird wieder von vorne begonnen. Dann braucht man nur in die XML-Datei *viclient-index.xml* zu sehen, die die jeweilige Nummer der aktuellen Datei und die maximale Anzahl der Logdateien enthält.

## vCenter Agent Logs

Über die Logdateien nach der Installation des ESXi Host wurde in Kapitel 3 ja schon einiges gesagt. Zuständig für die Protokollierung ist der Daemon *vm syslogd*, über den auch Speicherort, Größe der Dateien und Anzahl der aufzuhebenden Dateien eingestellt werden. Das können Sie über den vSphere Client unter KONFIGURATION → ERWEITERTE EINSTELLUNGEN → SYSLOG tun (siehe Abbildung 10-10).

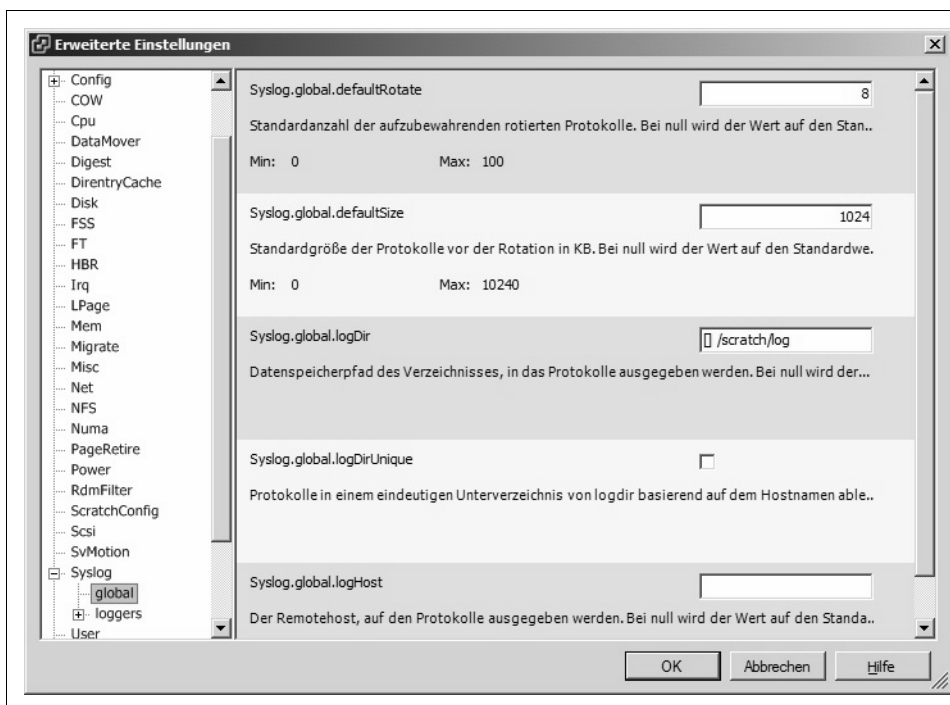


Abbildung 10-10: Erweiterte Einstellungen des ESXi Hosts

Die Änderungen, die Sie hier vornehmen, landen in der Datei */etc/vmsyslog.conf.d/vpxa.conf*.

Nachdem der Host zum vCenter Server hinzugefügt wurde, werden zusätzliche Dateien für die Fehlersuche angelegt: Diese finden Sie z.B. unter */scratch/log/*, wobei das wiederum (meistens) ein Link auf ein VMFS-Volumen ist. Die dortigen Logdateien entsprechen dem obigen Beispiel. Die Datei */var/log/vpxa.log*, die auch schon vorher existiert, zeigt als Link immer auf die aktuelle Logdatei im Ordner */scratch/log/* und entspricht

ungefähr der Datei *vpx-index* unter Windows. Die Logdateien heißen auf dem ESXi Server *vpxa-n.log*, wobei *n* wieder fortlaufende Zahlen sein können.

Weiterhin existieren auf dem ESXi Server in dem Ordner, in dem sich auch die Datei */etc/vmsyslog.conf.d/vpxa.conf* befindet (in der man die Einstellungen für das Protokollieren vornehmen kann), auch einige weitere *.conf*-Dateien für die Protokollierung, die ähnlich aufgebaut sind.

Auch eine HTML-basierte Datei finden Sie unter */etc/vmware/vpxa/* – schauen Sie sich den Inhalt an. Dort ist z.B. festgelegt, welche Informationen (Level) abgespeichert werden. Statt des Standardwerts *verbose* können auch folgende Werte stehen: *trivia*, *info*, *warning*, *error* oder *none*.

Der Wert *maxFileSize* liegt üblicherweise bei 1.048.576, was einem MByte entspricht, der Wert für *maxFileNum* liegt normalerweise bei 10. Das muss aber nicht unbedingt in der Datei stehen, da es sich dabei um Standardwerte handelt.

Beachten Sie auch, dass in der lokalen Ereignisanzeige des vCenter Servers Informationen zu VMware abgespeichert werden (siehe Abbildung 10-11):

| Anwendung Anzahl von Ereignissen: 2.123 |                     |                                          |             |                   |
|-----------------------------------------|---------------------|------------------------------------------|-------------|-------------------|
| Ebene                                   | Datum und Uhrzeit   | Quelle                                   | Ereignis-ID | Aufgabenkategorie |
| Informationen                           | 03.11.2011 14:34:59 | VMUpgradeHelper                          | 272         | Keine             |
| Informationen                           | 03.11.2011 14:34:59 | VMUpgradeHelper                          | 108         | Keine             |
| Informationen                           | 27.10.2011 14:53:35 | VMUpgradeHelper                          | 105         | Keine             |
| Informationen                           | 27.10.2011 15:10:28 | VMware vCenter Update Manager UFA-Dienst | 1           | Keine             |
| Informationen                           | 03.11.2011 14:23:29 | VMware vCenter Update Manager-Dienst     | 1           | Keine             |
| Informationen                           | 02.11.2011 14:23:18 | VMware vCenter Update Manager-Dienst     | 1           | Keine             |
| Informationen                           | 27.10.2011 16:19:09 | VMware vCenter Update Manager-Dienst     | 1           | Keine             |
| Informationen                           | 03.11.2011 14:32:42 | VMware vCenter Update Manager-Dienst     | 1           | Keine             |
| Informationen                           | 27.10.2011 15:10:27 | VMware vCenter Update Manager-Dienst     | 1           | Keine             |
| Informationen                           | 27.10.2011 16:27:03 | VMware vCenter Update Manager-Dienst     | 1           | Keine             |
| Fehler                                  | 27.10.2011 16:19:09 | VMware VirtualCenter Server              | 1000        | Keine             |
| Informationen                           | 27.10.2011 16:27:03 | VMware VirtualCenter Server              | 1000        | Keine             |
| Informationen                           | 27.10.2011 16:19:09 | VMware VirtualCenter Server              | 1000        | Keine             |
| Fehler                                  | 27.10.2011 16:19:09 | VMware VirtualCenter Server              | 1000        | Keine             |

Abbildung 10-11: Ereignisanzeige auf dem vCenter Server

## vCenter Server-Startprobleme beheben

Zunächst sollten Sie die Ereignisanzeige des vCenter Servers begutachten und auf Einträge überprüfen und anschließend schauen, ob die notwendigen Dienste für VMware alle korrekt gestartet wurden.

Falls ein Dienst nicht wie im Starttyp angegeben läuft, überprüfen Sie die Abhängigkeiten dieses Diensts, indem Sie sich die Eigenschaften anzeigen lassen und dann auf die Registerkarte ABHÄNGIGKEITEN klicken (siehe Abbildung 10-12). Läuft ein Dienst nicht, zu dem eine Abhängigkeit gegeben ist, versuchen Sie, ihn manuell erneut zu starten. Hinter-

her aktualisieren Sie die Anzeige, um den aktuellen Status sehen zu können, und starten dann den VMware-Dienst.

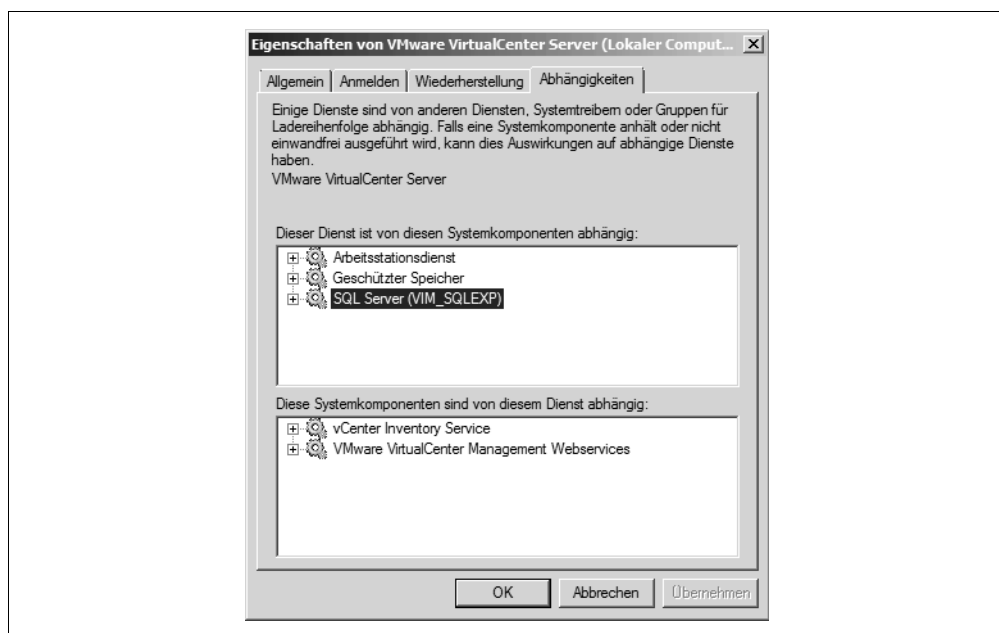


Abbildung 10-12: Abhängigkeiten des vCenter Server-Diensts



Der Virtual Center Server-Dienst ist abhängig vom SQL-Server-Dienst, wenn dieser auf demselben Rechner läuft. Die Abhängigkeit wird aber von VMware oft während der Installation nicht eingetragen. Das können Sie in der Registry nachholen: Fügen Sie bei DependOnService den SQL-Dienst mit MSSQL\$VIM\_SQLEXP hinzu (siehe Abbildung 10-13).

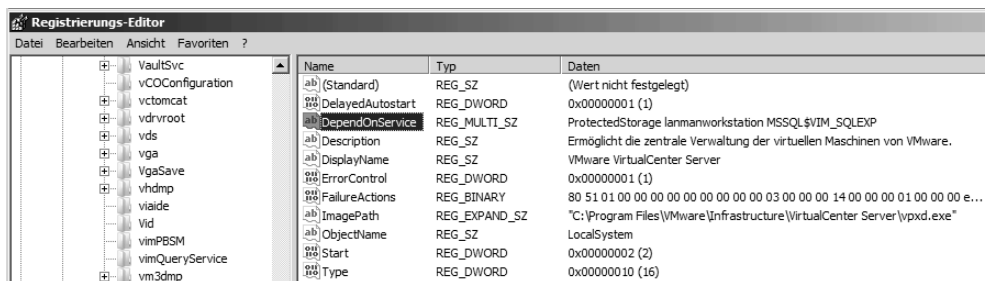


Abbildung 10-13: Virtual Center Server-Dienst: Abhängigkeiten

Sollte es wiederum zu Problemen kommen, schauen Sie in der Ereignisanzeige nach, ob dort hilfreiche Informationen zu finden sind. Weiterhin können Sie auf der Registerkarte WIEDERHERSTELLEN zum jeweiligen

Dienst auswählen, was bei einem aufgetretenen Fehler passieren soll. Vielleicht möchten Sie ja einstellen, dass der Dienst bei einmaligem Ausfall automatisch wieder gestartet wird.

Sollten Sie keinen Eintrag in der Ereignisanzeige finden, kann es sein, dass versucht wurde, die VMware-Komponenten zu starten, bevor die Protokollierung einsetzte. Dafür gibt es das Programm *vpxd* unter *C:\Programme\VMware\Infrastructure\Virtual Center Server\*.

Rufen Sie *vpxd* mit dem Parameter *-s* auf, um eine Ausgabe der Informationen zu erhalten. Mit dem Parameter *-?* bekommen Sie eine kurze Hilfestellung zu diesem Programm und können damit vielleicht noch andere Probleme lösen.

Die Protokolldateien finden Sie über den vSphere Client unter VERWALTUNG → SYSTEMPROTOKOLLE oder im Verzeichnis *C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\VMware\VMware VirtualCenter\Logs*.

Probleme bei der Kommunikation zwischen dem vCenter Server und den ESXi Server-Hosts können auch an der Netzwerkumgebung liegen. Beachten Sie die Ausgabe von *netstat -a*, um die offenen und verbundenen Ports auf den beteiligten Rechner zu überprüfen. Achten Sie immer auch auf DNS-Einträge oder Hosts-Dateien.

Auf einem Windows 2003 Server sollten Sie das Programm *netstat* auch mit dem Parameter *-b* aufrufen, um die aktiven Verbindungen zu VMware-hostd (*vpxd.exe*) zu überprüfen. Die Portnummern sehen Sie ebenfalls unter den Firewall-Einstellungen.

## Anmeldung am vCenter Server

Beim ersten Anmelden am vCenter Server landen Sie im Fenster *Home*. Wenn Sie sich das nächste Mal mit ihm verbinden, werden Sie üblicherweise zum letzten aktuellen Fenster geleitet. Das *Home*-Fenster unterteilt sich zunächst in die drei Bereiche *Bestandsliste*, *Verwaltung* und *Management* (siehe Abbildung 10-14). Welche Symbole angezeigt werden, hängt von der erworbenen Lizenz und der Installation von möglichen zusätzlichen Komponenten ab. Wenn Sie über die Menüleiste PLUG-INS hinzufügen, kommt ein vierter Bereich dazu, in dem Sie die installierten Zusätze finden. Data Recovery erscheint erst, nachdem Sie lokal das MSI-Paket installiert haben.

## Hosts hinzufügen

Sobald Sie sich mit dem vCenter Server verbunden haben, besteht der nächste Schritt darin, die ESXi Server mit ihren virtuellen Maschinen und Storages sowie Netzwerkswitches in ihn zu integrieren, um von hier aus alle weiteren Einstellungen vornehmen zu können.

Die Voraussetzung dafür, dass die Hosts hinzugefügt werden können, ist allerdings ein Datacenter. Klicken Sie im HOME-Bereich auf das Symbol HOSTS UND CLUSTER und dann mit der rechten Maustaste auf Ihren vCenter Server und wählen NEUES DATENCENTER. Vergeben Sie einen aussagekräftigen Namen, z.B. den Ihrer Firma.



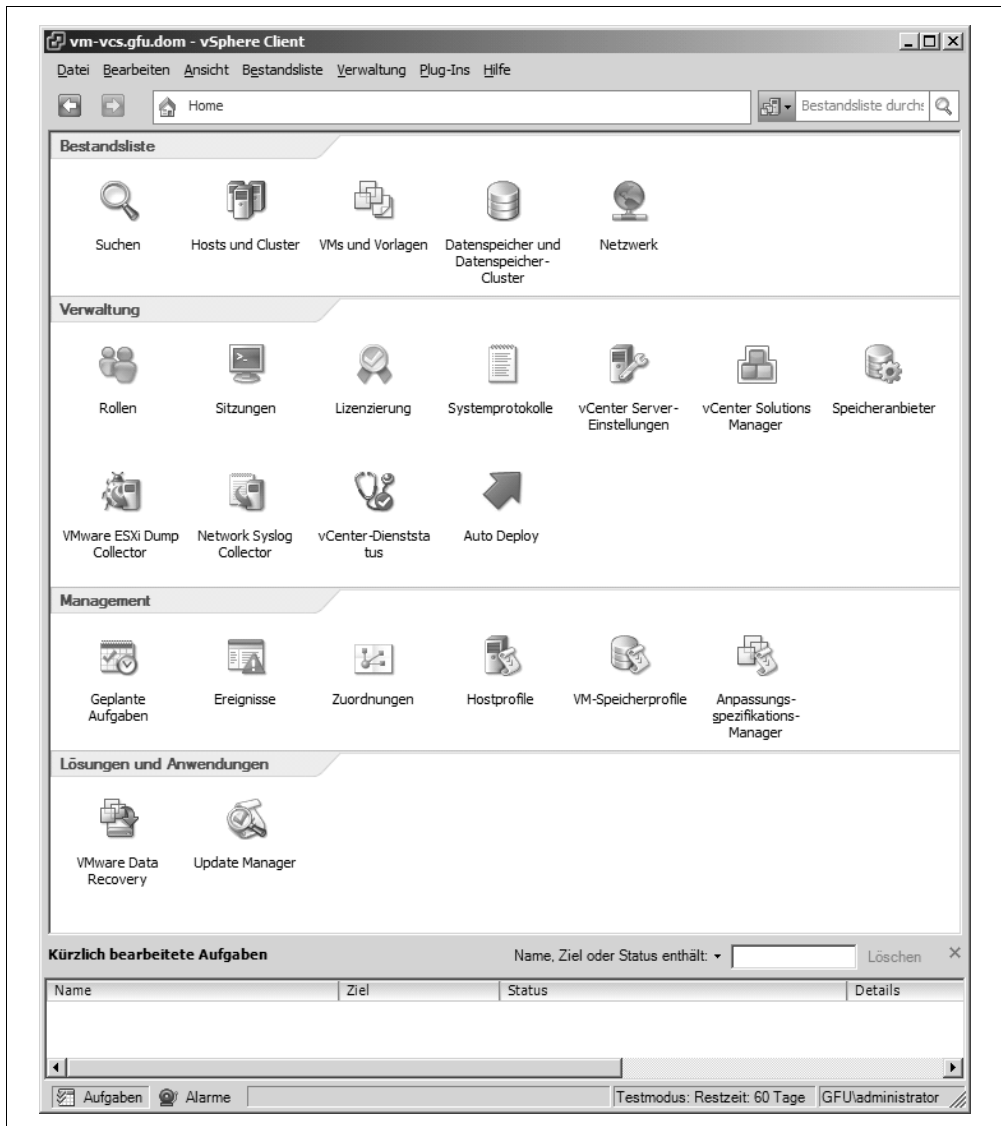


Abbildung 10-14: Startseite bei der ersten Anmeldung

Zum Datacenter können Sie jetzt Ihre ESXi Server aus dem Kontextmenü der Reihe nach hinzufügen. Funktioniert DNS oder wurden die Hosts-Dateien ergänzt, können Sie den Namen des Servers eingeben; wenn nicht, erscheinen hinterher in der Bestandsliste auch nur die IP-Adressen anstelle der Namen. Das lässt sich nachträglich nur ändern, indem der Host entfernt und wieder hinzugefügt wird.



Wenn das Hinzufügen mit dem Namen nicht geht, beheben Sie zuerst diesen Mismatch. Fügen Sie die Hosts möglichst nicht mit der IP-Adresse hinzu, weil Fehler bei der Namensauflösung weitere Komplikationen nach sich ziehen.

Als Benutzernamen geben Sie hier root ein sowie das Passwort, das Sie bei der Installation für diesen User vergeben haben. Die folgende Sicherheitswarnung bezüglich des Fingerabdrucks (SHA-Footprint, Zertifikat) kann ignoriert werden, also klicken Sie auf JA.

Im folgenden Fenster wird eine Kurzbeschreibung des Hosts mit den darauf registrierten virtuellen Maschinen aufgeführt, wie in Abbildung 10-15 beispielhaft zu sehen ist. Klicken Sie auf WEITER.

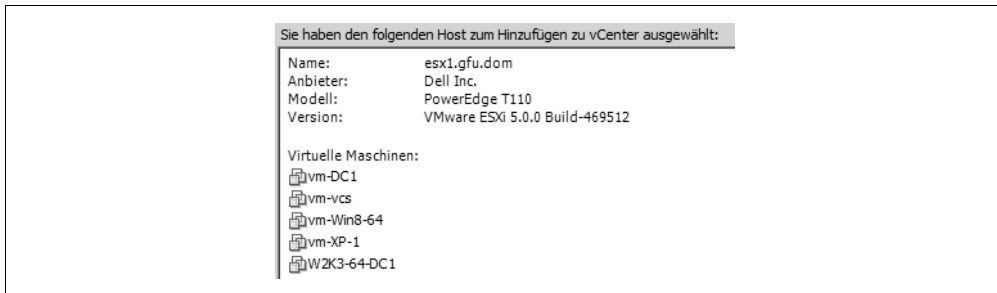


Abbildung 10-15: Hosts hinzufügen

Jetzt kann – falls notwendig – der Lizenzschlüssel eingegeben werden. Im Übersichtsfenster klicken Sie auf BEENDEN. Jetzt können Sie die weiteren Hosts hinzufügen.



Ein ESXi Server kann immer nur zu einem vCenter Server gehören. Bei dem Versuch, ihn einem weiteren vCenter Server hinzuzufügen, bekommen Sie eine Fehlermeldung (siehe Abbildung 10-16).

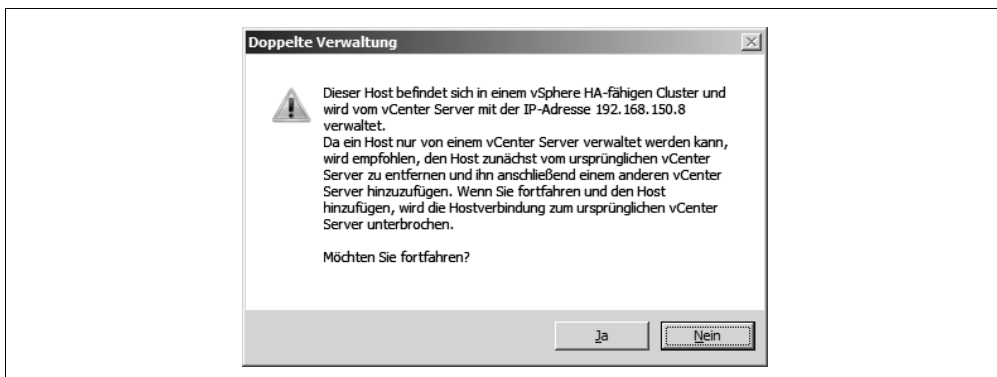


Abbildung 10-16: Das Hinzufügen zu mehreren vCenter Servern ist nicht zulässig.

Im Datacenter werden anschließend die Summen für die Hosts, die virtuellen Maschinen und Vorlagen, die verfügbaren Netzwerkschwitches für die VMs und die Anzahl der Storages angezeigt.

## Einen Cluster erstellen

Der nächste logische Schritt besteht darin, einen Cluster zu erstellen, die Hosts hinzuzufügen und die Clusterumgebung zu konfigurieren.

Ein Cluster ist eine Gruppe von Hosts, deren Ressourcen (CPU, RAM usw.) vom vCenter Server gemeinsam verwaltet werden, ähnlich einem alles umfassenden Ressourcenpool. Nur im Cluster können Funktionen wie vMotion, Fault Tolerance, DRS und HA genutzt werden.

Bei den meisten VMs funktionieren die bei der Erstellung zugewiesenen Standardressourceneinstellungen (NORMAL) ohne weiteren Eingriff. Sie können bei Bedarf später verändert werden, um Prioritäten, also einen anteilsabhängigen Prozentsatz für CPU, Arbeitsspeicher, Festplattenspeicherzugriff und Netzwerkgeschwindigkeit, oder eine garantierte CPU- und Arbeitsspeicherzuteilung zuzuweisen (siehe Kapitel 18). Beim Einschalten der virtuellen Maschine überprüft der vCenter Server, ob ausreichende Ressourcen verfügbar sind, und ermöglicht dann gegebenenfalls das Einschalten – oder auch nicht. Dieser Vorgang, den man auch außer Kraft setzen kann, wird als *Zugangssteuerung* bezeichnet.

Aus dem Kontextmenü des Datacenters lässt sich der Assistent für das Erstellen eines Clusters aufrufen. Sie können auch mehrere Cluster erstellen und Ihre Hosts und VMs dann aufteilen. Haben Sie unterschiedliche CPUs in Ihren Servern, sollten Sie sich überlegen, ob Sie dieses Konstrukt anwenden möchten.



Wenn Sie einen weiteren Cluster erstellen, können Hosts im Wartungsmodus vom einen zum anderen Cluster mit der Maus verschoben werden. Die auf diesem Host ausgeschalteten oder im Suspend-Modus befindlichen Maschinen werden mitverschoben. Laufende VMs können von einem Cluster zum anderen migriert werden, wenn die sonstigen Voraussetzungen (gleicher Storage, gleiche CPU usw.) gegeben sind. Beim Entfernen des Clusters werden auch die Hosts und VMs entfernt und müssen dann wieder manuell dem anderen hinzugefügt werden – oder Sie verschieben vorher alle Objekte und löschen den leeren Cluster.

Beachten Sie bitte, dass es beim einzelnen Host zwar immer noch die Konfiguration für den automatischen Start der VMs gibt und dass Sie diesen Punkt wieder aktivieren können, aber nach dem nächsten Neustart wird dieser wieder deaktiviert.

## Wie funktioniert HA?

*VMware High Availability* (HA), also Hochverfügbarkeit, ist eine Funktion, bei der der Ausfall einer Hosthardware erkannt wird und die darauf ehemals laufenden VMs auf

einem oder mehreren verbliebenen ESXi Servern neu gestartet werden. Beim Ausfall der Hardware ist der Inhalt des Arbeitsspeichers der VM natürlich weg. Die Maschine wird auf einem anderen Host neu gestartet, und aus ihrer Sicht sieht es so aus, als hätten Sie sie hart ausgeschaltet.

Um den Ausfall des ESXi Servers erkennen zu können, wird regelmäßig ein Signal (Heartbeat) über das Management Network (am besten zwei davon in unterschiedlichen Subnetzen) an andere Hosts und das Standardgateway gesendet. Bleibt dieses Signal aus, schaut der andere beteiligte Host auf den gemeinsamen Storage, um den »Lock« der VM-Festplatten zu überprüfen. Wenn dort keine Sperrung mehr gesetzt ist, müsste in der Konfigurationsdatei (.vmx, unter CleanShutdown) ein Hinweis zum Herunterfahren, Anhalten oder Abschalten der VM stehen. Ist das nicht der Fall (CleanShutdown="FALSE"), wird versucht, die Maschine neu zu starten. Weitere Details finden Sie weiter unten beim Einrichten von HA.

## Wie funktioniert vMotion?

In der Terminologie von VMware wird das Verschieben einer virtuellen Maschine von einem ESXi Server zu einer anderen *Migration* genannt. Auch die Verlagerung von Dateien der VM auf einen anderen Datenträger (natürlich mit VMFS) heißt so. Vereinfacht gesagt: Bei vMotion wird zunächst der Arbeitsspeicher der VM von einem Host zum anderen übertragen. Während dieser Zeit landen die Änderungen innerhalb des Arbeitsspeichers der VM in einer Deltadatei. Ist das RAM übertragen, wird die erste Deltadatei kopiert und Änderungen landen in einer neuen Datei. Der Vorgang wird so lange fortgeführt, bis das letzte Delta im Bruchteil einer Sekunde übertragen werden kann. Im Prozessor der VM wird eine Ausnahmebedingung (Exception) ausgelöst, um den Cache zu leeren. Anschließend wird die virtuelle CPU auf dem anderen Host aktiviert – die Maschine läuft jetzt dort weiter.

Beim Verschieben kann ein Ping-Signal verloren gehen, aber die User bleiben angemeldet und Daten bleiben konsistent.

Bei Storage vMotion ist der Vorgang ähnlich, nur dass hier der Inhalt der Festplatte und alle Konfigurationsdateien verschoben werden.



Wenn Sie eine virtuelle Maschine in der Bestandsliste vor dem Verschieben umbenennen, werden auf dem Ziel das Verzeichnis der VM, aber nicht die betroffenen Dateien umbenannt. Innerhalb der Konfigurationsdateien findet die Umbenennung ebenfalls nicht mehr statt. Die Funktionalität der VM wird dadurch nicht beeinträchtigt.

## Wie funktioniert DRS?

Das Planungsprogramm *Distributed Resource Scheduling* (DRS) steuert die Arbeitslast der laufenden virtuellen Maschinen und die Ressourcenauslastung der Hosts, um Ressour-

cen automatisch zuweisen zu können und VMs mithilfe von vMotion nach Last zu verteilen. Der vCenter Server schaut also jeweils bei den Hosts die Auslastung bezüglich CPU und RAM an und vergleicht die Abweichung zu den anderen. Ist ein ESXi Server durch die auf ihm laufenden VMs stärker ausgelastet als ein anderer, werden die Maschinen automatisch anders verteilt (siehe Abbildung 10-17).

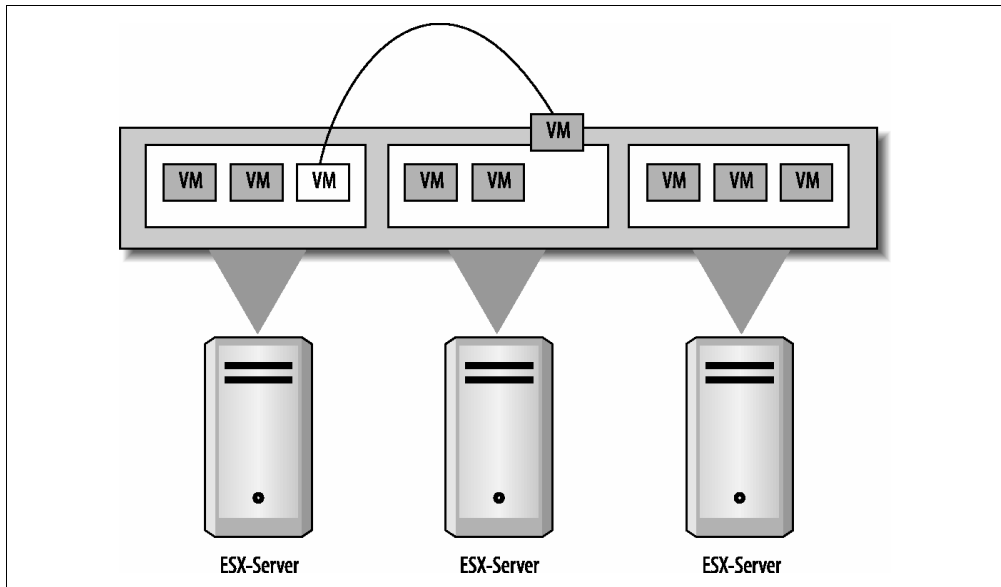


Abbildung 10-17: Funktionsprinzip von DRS

Dabei wird auch die kurzfristige Last einer VM berücksichtigt und diese nicht sofort verschoben.

## Wie funktioniert DPM?

Das DPM (*Distributed Power Management*) ist eine Energieverwaltung für den Cluster. Über die eingerichtete Funktionsweise des DRS werden bei Bedarf laufende virtuelle Maschinen auf andere Hosts verschoben, und anschließend wird ein freier Host in den Suspend-Modus versetzt. Das wird so lange fortgesetzt, wie genügend freie Ressourcen auf den verbleibenden Hosts zur Verfügung stehen. Das kann auch bedeuten, dass die Failover-Kapazität des HA außer Kraft gesetzt wird und nur noch ein Host aktiv läuft (siehe Abbildung 10-18).

Sollten die Kapazitäten nicht mehr ausreichen, werden so viele Hosts neu gestartet, bis allen VMs genügend CPU-Leistung und Arbeitsspeicher zur Verfügung steht. Voraussetzung dafür ist die richtige Konfiguration der Umgebung.

| Name         | Zustand   | Status | % CPU | % Arbeitsspeicher | Betriebszeit | Letztes Beenden des Standby-Modus |
|--------------|-----------|--------|-------|-------------------|--------------|-----------------------------------|
| esx3.gfu.dom | Verbunden | Normal | 4     | 65                | 15 Stunden   | Nie                               |
| esx1.gfu.dom | Standby   | Normal |       |                   | N/A          | 24.12.2011 16:28:56 - Erfolg      |
| esx4.gfu.dom | Standby   | Normal |       |                   | N/A          | 24.12.2011 16:37:16 - Erfolg      |
| esx2.gfu.dom | Standby   | Normal |       |                   | N/A          | 24.12.2011 16:25:23 - Erfolg      |

Abbildung 10-18: Drei ESXi Server im Standby-Modus



Bei Tests habe ich Folgendes festgestellt:

Von vier zur Verfügung stehenden ESXi Servern mit insgesamt 25 laufenden virtuellen Maschinen, die keine große Auslastung hatten, wurden nach und nach alle VMs nach der Einrichtung von DPM auf nur noch einen ESXi Server verschoben. Die anderen drei gingen in den Suspend-Modus.

Als ich durch ein Programm auf jeder VM eine hohe Last erzeugte und der verbliebene ESXi Server bei 100 % Auslastung war, dauerte es weitere zwei Minuten, bis der vCenter Server einen der schlafenden Server reanimierte. Es wurde ein Neustart durchgeführt, und nach sechs Minuten war der Server wieder vorhanden. Nach weiteren vier Minuten begann der vCenter Server, die erste VM zu verschieben. Wenn Sie diese Funktion nutzen wollen, testen Sie sie vorher also unbedingt aus!

## Wie funktioniert FT?

Bei FT (*Fault Tolerance*) wird eine wichtige VM auf einem anderen ESXi Server nach dem Einrichten gespiegelt. Beide Maschinen, die primäre und die sekundäre, greifen auf denselben Datenbestand auf dem Storage zu, wobei die sekundäre nicht schreiben darf: Ihre Schreib Anforderungen laufen ins Leere. Der Inhalt der Arbeitsspeicher und der Cache der Prozessoren werden durch einen zusätzlichen Agenten (vLockstep) auf beiden VMs ständig synchronisiert. Anfragen aus dem Netz bekommen beide gleichzeitig zugesandt, somit müsste bei der gleichen Aufgabe auch das gleiche Ergebnis herauskommen. Auch direkte Eingaben an der Konsole werden zur sekundären VM geschickt.

Kommt es zum Ausfall des Hosts mit der primären Maschine – was durch ein Taktsignal erkannt werden kann –, übernimmt die sekundäre sofort deren Aufgaben. User bleiben angemeldet und alle Daten bleiben vorhanden.

## Wie funktioniert EVC?

Bei EVC (*Enhanced vMotion Compatibility*) werden alle im Cluster vorhandenen Prozessoren – wenn möglich – auf einen gemeinsamen Nenner gebracht. Haben Sie nur identische CPUs in Ihren Hosts verbaut, sollten Sie diesen Modus nicht einschalten. Liegen aber Unterschiede vor, dann kann es sein, dass eine VM Funktionen eines Prozessors nutzt, die die andere CPU auf dem anderen ESXi Host nicht hat. Somit kann die virtuelle Maschine natürlich nicht zur Laufzeit auf den anderen Host verschoben werden. Beim

Einschalten von EVC versucht der vCenter Server, die Funktionen auszublenden, die nicht bei allen Host-CPU's vorhanden sind, damit diese von den VMs gar nicht erst gesehen werden.

## Clusterkonfiguration für HA

Im Assistenten für das Erstellen eines Clusters können Sie sowohl HA als auch DRS sofort mit anwählen und konfigurieren. Sobald das jeweilige Kontrollkästchen aktiviert ist, erweitert sich im linken Teil des Fensters die Liste der möglichen Einstellungen.

HA (intern immer noch als »DAS« bezeichnet) ist die erste zu konfigurierende Komponente. Dabei gibt es in einem Cluster nur einen Master und ggf. mehrere Slave Hosts. Die Anzahl der Knoten ist in einem Cluster auf 32 beschränkt, deshalb können auch nur maximal 31 Hostausfälle ignoriert werden. Derjenige Host, der die meisten Zugriffe auf gemeinsame Storages hat, oder der erste, wenn alle Storage-Zugriffe gleich sind, wird als Master initialisiert. Fällt der Master aus, wird ein anderer ESXi Server als Master ausgewählt. Das passiert auch, wenn der Master heruntergefahren, im Wartungsmodus oder im Standby-Modus ist oder aus dem Cluster entfernt wird.

Der Master ist für die Überwachung der Slave-Knoten und der Zugriffe auf die Storages zuständig. Die Slaves senden ihre Statusinformationen und die ihrer VMs sowie die sekundlichen Heartbeats nur an diesen. Weiterhin kann nur er darüber entscheiden, welche ausgefallene VM neu gestartet wird.

1. Nachdem Sie das Häkchen bei HA gesetzt haben, können folgende Einstellungen für High Availability (HA) konfiguriert werden (siehe Abbildung 10-19).
  - Der HOSTÜBERWACHUNGSSTATUS ist für kurzfristige Netzwerkarbeiten gedacht, wenn die Konnektivität zwischen den Hosts gefährdet ist. Der HA Agent auf dem ESXi Server nutzt für die Kommunikation den Management Network-Port, nicht einen anderen VMkernel-Port.
  - Die ZUGANGSSTEUERUNG regelt das Neustarten der VMs auf anderen Servern nach einem Ausfall. Überlegen Sie sich, ob lieber alle Maschinen ein bisschen langsamer laufen sollen (DEAKTIVIEREN) oder gar nicht erst gestartet werden, wenn nicht mehr genügend Ressourcen vorhanden sind (AKTIVIEREN). Normalerweise werden z.B. in einem Vierercluster 25 % der Ressourcen reserviert, im Dreiercluster 33 % usw.
  - Bei der ZUGANGSSTEUERUNGSRICHTLINIE wählen Sie die Anzahl der zu tolerierenden Hostfehler (maximal 31) oder den Prozentsatz der für HA zu reservierenden Ressourcen aus. Bei einem tolerierten Hostfehler würden die VMs nicht neu gestartet, wenn zwei Hosts ausfallen. Die für HA reservierten Ressourcen stehen keiner VM zur Verfügung, es sei denn, ein Host ist ausgefallen.

**Hostüberwachungsstatus**  
 ESX-Hosts in diesem Cluster tauschen Netzwerktahtsignale aus. Deaktivieren Sie diese Funktion, wenn Sie Netzwerkwartungsarbeiten verrichten, die Isolierungsreaktionen verursachen könnten.  
☒ Hostüberwachung aktivieren

**Zugangssteuerung**  
 Die Richtlinie für die vSphere HA-Zugangssteuerung legt die Clusterkapazität fest, die für VM-Failover reserviert wird. Das Reservieren einer größeren Failover-Kapazität ermöglicht eine höhere Ausfalltoleranz, reduziert aber die Anzahl der VMs, die ausgeführt werden können.  
☒ Aktivieren: VM-Einschaltvorgänge nicht zulassen, die gegen die Verfügbarkeitseinschränkungen verstoßen  
☐ Deaktivieren: VM-Einschaltvorgänge zulassen, die gegen die Verfügbarkeitseinschränkungen verstoßen

**Zugangssteuerungsrichtlinie**  
 Geben Sie den Typ der Richtlinie an, für dessen Einhaltung die Zugangssteuerung sorgen soll.  
☒ Vom Cluster tolerierte Hostfehler:   
☐ Prozentsatz der Cluster-Ressourcen, der als Failover-Ersatzkapazität reserviert wird:  
      % CPU  
      % Arbeitsspeicher  
☐ Failover-Hosts angeben: 0 Hosts angegeben. Klicken Sie zum Bearbeiten.

[Erweiterte Optionen...](#)

Abbildung 10-19: Weitere Einstellungen zu HA

- FAILOVER-HOST ist der Server, der keine virtuellen Maschinen besitzt. Erst im HA-Fall wird dieser zum Pool mit hinzugenommen, und die VMs werden dann auf alle verbliebenen ESXi Server verteilt. Über den Link 0 HOSTS ANGEGEBEN... bekommen Sie eine Liste aller im Cluster befindlichen ESXi Server und können sich dann auf der linken Seite einen oder mehrere Hosts als Failover aussuchen.



Wenn Sie bei der Zugangssteuerung den oberen Punkt (AKTIVIEREN) gewählt haben, werden die Ressourcen für die virtuellen Maschinen im Cluster sofort eingeschränkt. Haben Sie nur zwei Hosts, können Ihre VMs maximal 50 % der gesamten CPU-Leistung und des Arbeitsspeichers bekommen.

2. Allgemeine OPTIONEN FÜR VIRTUELLE MASCHINEN können im nächsten Fenster gesetzt werden.

- Die VM-NEUSTARTPRIORITÄT steht zunächst auf MITTEL. Da Sie im nächsten Schritt jede einzelne VM anders einstellen können, sollten Sie hier das für die meisten VMs Richtige auswählen.
- Was ist, wenn eine HOSTISOLIERUNGSREAKTION auftritt, wenn also ein Host die anderen ESXi Server und sein Standardgateway nicht mehr erreicht? Legen Sie fest, ob er die noch auf ihm laufenden VMs herunterfahren oder ausschalten soll oder die VMs eingeschaltet bleiben sollen (siehe Abbildung 10-20).



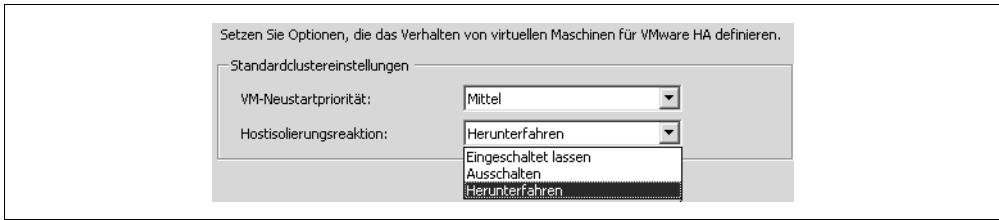


Abbildung 10-20: Optionen für die virtuellen Maschinen



Solange eine virtuelle Maschine auf dem ESXi Server eingeschaltet ist, befindet sich ihre Festplattendatei im aktiven Lock-Modus. Bevor also versucht wird, eine VM auf einem anderen Host zu starten, wird dieser Modus überprüft. Da es sich hier um einen aktiven Modus handelt, ist der Lock automatisch weg, wenn der Host nicht mehr läuft (oder sich »aufgehängt« hat). Falls Sie einen NAS- oder iSCSI-Storage haben, kann es mit dem HERUNTERFAHREN manchmal Probleme geben. Stellen Sie dann die VMs auf AUSSCHALTEN (Siehe auch weiter unten).



Damit der Zustand der HOSTISOLIERUNGSREAKTION auch einwandfrei festgestellt werden kann, muss eine Portgruppe für das Management Network über zwei Netzwerkkarten verfügen, oder es muss über eine weitere Netzwerkkarte eine zweite PG eingerichtet worden sein. Fehlt diese bei der Erstellung des Clusters, wird eine Warnmeldung vom vCenter Server beim Host angezeigt (siehe Abbildung 10-21). Haben Sie das Problem behoben, klicken Sie aus dem Kontextmenü des ESXi Hosts NEU KONFIGURIEREN FÜR VSPHERE HA an.

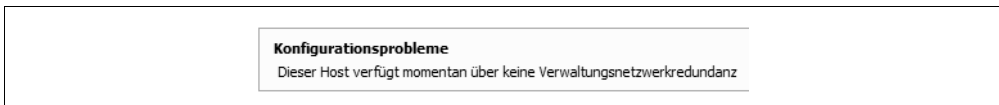


Abbildung 10-21: Meldung über HA-Konfigurationsprobleme

3. Im nächsten Fenster kann für die VMs eine Überwachung eingestellt werden, die auf den Heartbeat der Agenten der VMware Tools angewiesen ist. Kommt das Signal nicht in einem festgelegten Zeitraum, wird ein Zähler inkrementiert. Passiert das mehrmals in einem bestimmten Zeitraum, wird die Maschine resettet. Sie können zwischen NIEDRIG, MITTEL, HOCH und BENUTZERDEFINIERT wählen.

## Hostisolierungsreaktion richtig einstellen

Viele meiner Kunden hatten große Probleme mit der korrekten Einstellung der Hostisolierungsreaktion in ihrem Umfeld. Deshalb gehe ich auf die drei möglichen Einstellungen an dieser Stelle detailliert ein.

Das Wichtigste vorweg: Eine Empfehlung zum Ausschalten, Laufenlassen oder Herunterfahren der virtuellen Maschinen kann man ohne genaue Kenntnis der Verkabelung nicht treffen. Die folgenden Schilderungen sollen Ihnen dabei helfen, für Ihre Umgebung die richtige Einstellung zu finden.

Der ESXi Server stellt fest, dass er isoliert ist, indem er keine Heartbeats mehr von anderen Hosts im HA Cluster bekommt und sein Standardgateway nicht mehr auf einen Ping-Befehl antwortet. Das ist auch der Grund dafür, dass man in so einem Cluster eine Redundanz für das Management Network haben muss. Wichtig ist dabei auch, ob die laufenden VMs auf dem Server noch eine Verbindung zu Ihrem Storage haben. Haben Sie beispielsweise ein SAN über Fibre-Channel angeschlossen, können die virtuellen Maschinen ohne Probleme weiterhin auf ihre Festplatten zugreifen. In Abbildung 10-22 sehen Sie ein Beispiel dafür.

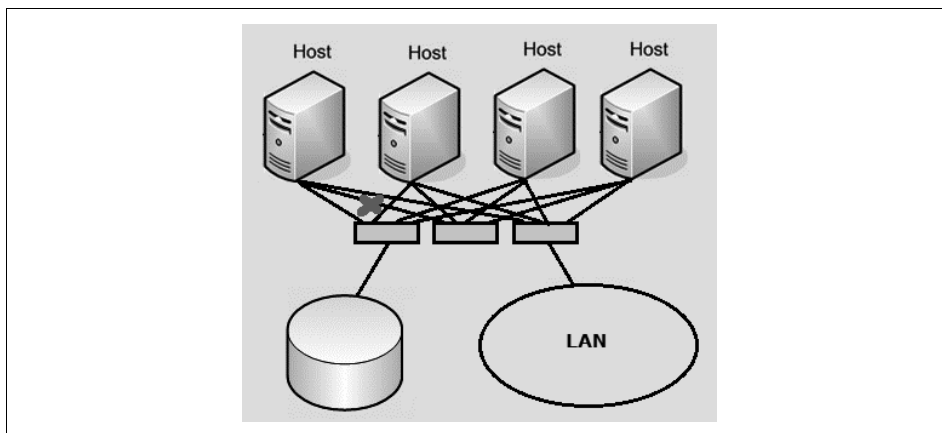


Abbildung 10-22: HA-Hostisolierungsreaktion: eingeschaltet lassen

Hier ist lediglich die Kommunikation zwischen den Hosts gestört, die User können aber weiterhin auf die VMs zugreifen, und diese über einen zusätzlichen Switch eine Verbindung zu ihren Daten haben. Die richtige Einstellung für den Hostisolierungsmodus wäre in diesem Fall also **EINGESCHALTET LASSEN**.

Anders sieht es im zweiten Beispiel aus: In der vereinfachten Darstellung in Abbildung 10-23 sehen Sie, dass nicht nur die Kommunikation der Hosts untereinander gestört ist, sondern auch keine Verbindung mehr zum LAN besteht und die Benutzer nicht mehr an die auf den Servern liegenden Daten herankommen.

Die VMs laufen zwar noch weiter, aber das hilft den Usern nicht. Die korrekte Einstellung wäre in so einem Fall **HERUNTERFAHREN**. Dabei wird aber in der Konfigurationsdatei der jeweiligen Maschine ein Hinweis gegeben, damit die anderen ESXi Hosts diese VMs neu starten können (CleanShutdown="FALSE"). Nach kurzer Zeit werden die auf dem isolierten Host ehemals laufenden VMs auf den anderen ESXi Servern neu gestartet und die Benutzer können weiterarbeiten.

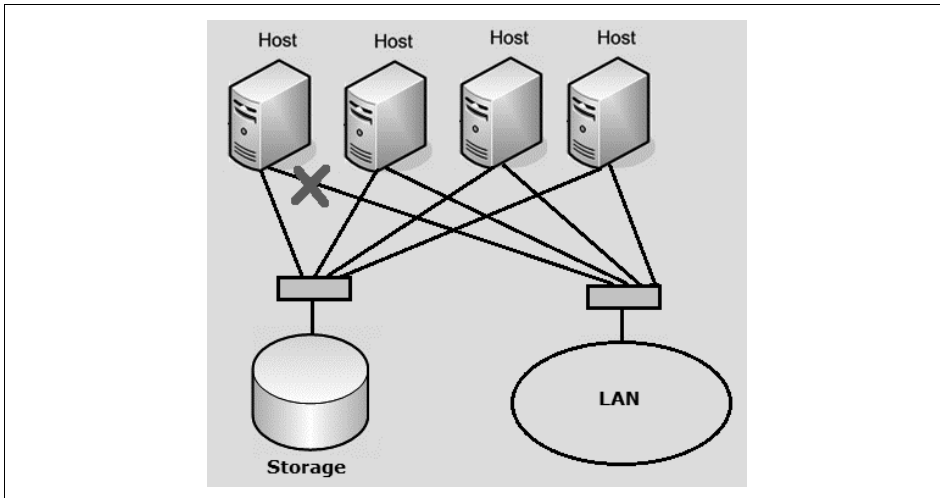


Abbildung 10-23: HA-Hostisierungsreaktion: herunterfahren

Sollte durch die Isolierung auch der Zugriff auf die Festplatte der VMs verloren gehen, können die Maschinen nicht heruntergefahren werden. Üblicherweise hängen sich die Betriebssysteme auf, wenn sie nicht mehr an ihre Festplatten herankommen. Der Lock der VMDK-Dateien geht verloren, da der ESXi Server auch keinen Zugriff mehr hat, und die beteiligten Rechner werden auf anderen Hosts neu gestartet. Sie laufen dann doppelt im System. Um Konflikte in so einer Umgebung zu vermeiden, müssen die VMs auf dem isolierten Host ausgeschaltet werden, eine andere Möglichkeit besteht nicht. Hier ist also AUSSCHALTEN die richtige Wahl. Dieser Zustand ist – vereinfacht – in Abbildung 10-24 dargestellt.

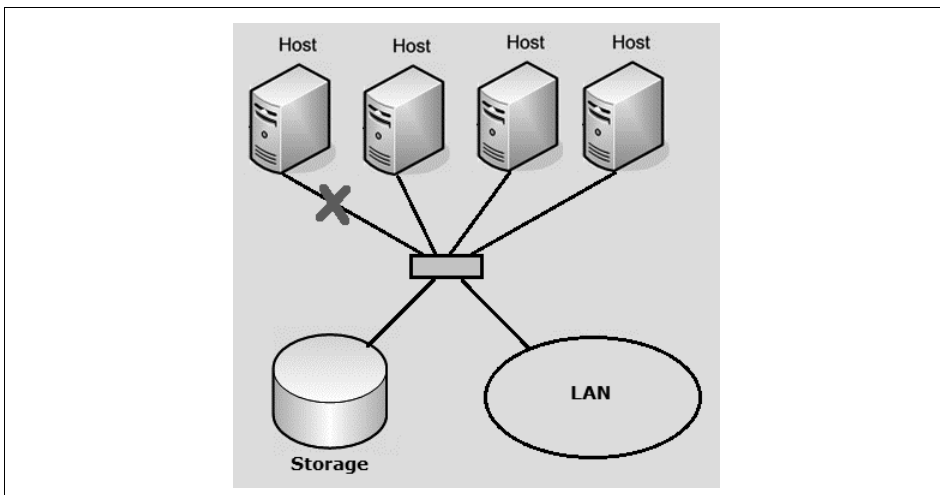


Abbildung 10-24: HA-Hostisierungsreaktion: ausschalten

Wenn im letzten Fall der Fehler behoben wird, bevor die isolierten VMs abgeschaltet wurden, bekommen Sie in Ihrem Netzwerk ein heilloses Chaos! Nicht nur weil die »Zombie«-VMs extreme Last im LAN verursachen, sondern auch weil sie im Gesamtsystem nun doppelt vorhanden sind. Das ist auf alle Fälle zu vermeiden – ein Ausschalten der betroffenen VMs und dadurch ein eventueller Datenverlust ist bei Weitem nicht so schlimm wie dieses Szenario.

## HA-Einstellungen der VM

Bei OPTIONEN FÜR VIRTUELLE MASCHINEN kann für jede einzelne Maschine das Verhalten bezüglich HA gewählt werden. Die wichtigsten Maschinen oder die, die zuerst neu gestartet werden sollen, stellen Sie bei VM-NEUSTARTPRIORITÄT auf HOCH, weniger wichtige lassen Sie auf MITTEL oder CLUSTEREINSTELLUNGEN VERWENDEN und noch weniger wichtige auf NIEDRIG (siehe Abbildung 10-25). Auch DEAKTIVIERT kann hier ausgewählt werden, also kein Neustart.

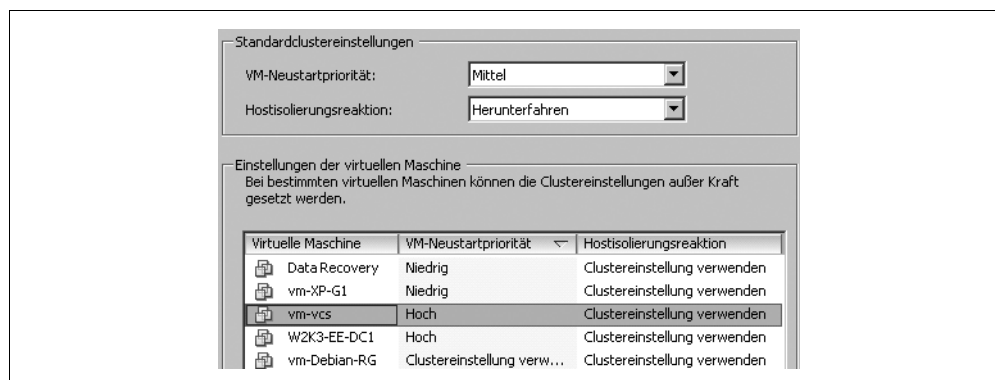


Abbildung 10-25: Virtuelle Maschinen individuell einstellen

Im Fenster VM-ÜBERWACHUNG können Sie jetzt für jede VM einzeln eine Überwachung – auch benutzerdefiniert – zum Laufzeitverhalten einstellen.

Klicken Sie dazu die gewünschte Maschine an und wählen Sie bei VM-ÜBERWACHUNG BENUTZERDEFINIERT aus. Es erscheint das in Abbildung 10-26 gezeigte Fenster, in dem Sie Ihre Konfiguration auswählen können.

Die MINIMALE BETRIEBSZEIT sollte nicht zu kurz gewählt werden, weil die VMware Tools ja erst geladen sein müssen. Das dreimalige Zurücksetzen innerhalb einer Stunde soll vermeiden, dass die VM im gewähltem Zeitfenster öfter als drei Mal neu gestartet wird.

Bei der Überwachung werden nicht nur die VMware Tools, sondern auch die Aktivität der VM auf dem Storage überprüft. Können die Tools keine Heartbeats mehr senden, ist aber die I/O-Aktivität im Zeitintervall von 120 Sekunden weiterhin feststellbar, so wird die VM nicht neu gestartet.

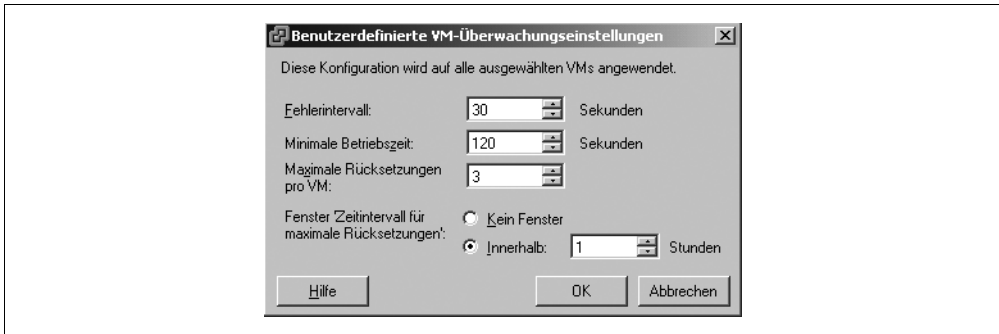


Abbildung 10-26: VM-Überwachungseinstellungen

Die Anwendungsüberwachung funktioniert nur über das Software Development Kit mithilfe von VMware Application Monitoring. Damit kann dann eine Anwendung auf der Maschine wie bei der VM-Überwachung überprüft und die VM ggf. neu gestartet werden.

## Datenspeicher-Taktsignale

Eine weitere neue Funktion, die mit der aktuellen Version von vSphere eingeführt wurde, sind die Taktsignale, die über Datenspeicher ausgetauscht werden. Dies ist eine Komponente, die die Hostisolierung eindeutig feststellen soll und Maßnahmen zum Neustart von ausgefallenen VMs veranlasst. Die Datenspeicher-Taktsignale kommen erst in Betracht, wenn der Host mit der Master-HA-Rolle nicht mehr mit einem Slave-HA-Host über das Management Network kommunizieren kann. Wird über den Storage ebenfalls kein Taktsignal mehr empfangen, gilt der jeweilige ESXi Server als isoliert oder ausgefallen. Dann erst werden die VMs neu gestartet.

Der vCenter Server stellt nur Datenspeicher für diese Funktion zur Verfügung, der von mindestens zwei im Cluster vorhandenen Hosts erreicht wird. Welche Storages der vCenter Server selbst gewählt hat, sieht man über das Fenster STATUS DES VSPHERE HA-CLUSTERS auf der Registerkarte TAKTSIGNAL-DATENSPEICHER. Diese müssen nicht denen entsprechen, die manuell in den Clustereigenschaften angeklickt wurden, weil letztendlich der vCenter Server selbst entscheidet, welche er nimmt.

Auf diesem Storage wird dann pro Cluster ein verstecktes Verzeichnis mit Namen *.vSphere-HA* angelegt, das meist unter VMFS5 ca. 3 MByte und unter VMFS3 bis zu 2 GByte Platz beansprucht.

Wenn Sie bei der HA-Hostisolierungsreaktion AUSSCHALTEN gewählt haben, ergeben Datenspeicher-Taktsignale keinen Sinn – schalten Sie diese dann besser ab.

## Clusterkonfiguration für DRS

Nach der Konfiguration von HA können Sie direkt mit dem Einstellen von DRS weitermachen. Erscheinen die Details zu DRS nicht, müssen Sie unter CLUSTERFUNKTIONEN erst das Häkchen bei DRS setzen.

1. Lesen Sie sich den angezeigten Text durch und wählen Sie die Automatisierungsebene.
2. Bei DISTRIBUTED RESOURCE SCHEDULER haben Sie folgende Möglichkeiten:
  - **MANUELL:** Der vCenter Server gibt Empfehlungen dafür, wie das Load-Balancing zwischen den Hosts bezüglich CPU- und Arbeitsspeicherlast am besten verteilt werden sollte. Es werden keine VMs verschoben
  - **TEILAUTOMATISIERT:** Es werden keine laufenden VMs verschoben. Beim Einschalten (nicht beim Neustart) einer VM schaut der vCenter Server nach den Ressourcen und wählt den Host aus, der am wenigsten belastet ist.
  - **VOLLAUTOMATISCH:** Beim Einschalten einer VM nimmt der vCenter Server den Host, der am wenigsten belastet ist. Laufende virtuelle Maschinen werden auf andere ESXi Server migriert, wenn die Last nicht ausgeglichen ist. Wie konservativ oder aggressiv das geschehen soll, wird über den Schieberegler bei MIGRATIONSSCHWELLENWERT eingestellt.



Im produktiven Einsatz hat sich die mittlere Einstellung (1, 2 und 3, siehe Abbildung 10-27) am besten bewährt. VMs werden dann beim Hochfahren oder wenn Sie kurzfristig viel Last brauchen nicht unnötig verschoben. Erst wenn die Balance einige Minuten im Ungleichgewicht gestört ist, werden Migrationen durchgeführt. DRS überprüft nur alle fünf Minuten die Lasten.

In Tabelle 10-15 sind die verfügbaren Migrationsschwellenwerte aufgelistet.

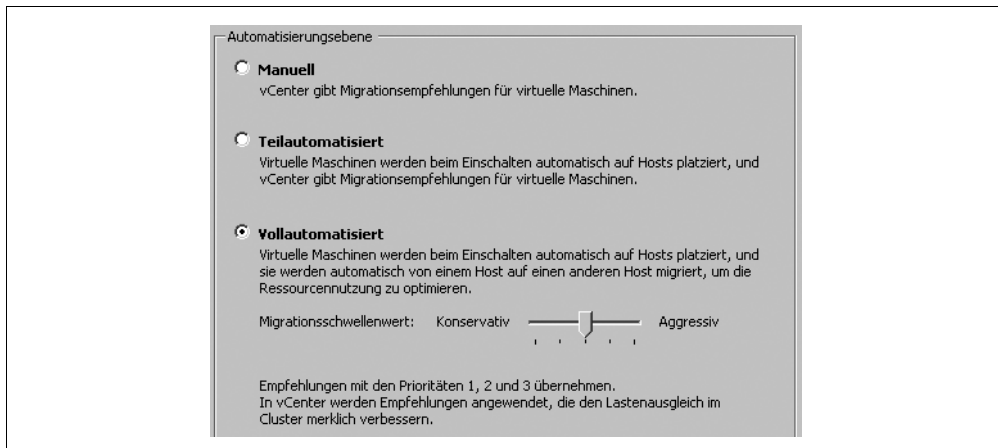


Abbildung 10-27: DRS-Automatisierungsebene

Tabelle 10-15: Migrationsschwellenwerte

| Schwellenwert             | Anwendung                                                                                                                                                              |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stufe 1, sehr konservativ | Nur Empfehlungen mit Priorität 1. Wendet Empfehlungen an, die befolgt werden müssen, um Clusterbedingungen zu erfüllen, zum Beispiel Affinitätsregeln und Hostwartung. |

Tabelle 10-15: Migrationsschwellenwerte (Fortsetzung)

| Schwellenwert           | Anwendung                                                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stufe 2                 | Empfehlungen mit Priorität 2 oder höher. Umfasst sowohl Empfehlungen der Ebene 1 als auch Empfehlungen, die bei einer erheblichen Abweichung der Lastverteilung des Clusters einsetzen.       |
| Stufe 3                 | Empfehlungen mit Priorität 3 oder höher. Umfasst sowohl Empfehlungen der Ebenen 1 und 2 als auch Empfehlungen, die bei einer deutlichen Abweichung der Lastverteilung des Clusters einsetzen. |
| Stufe 4                 | Empfehlungen mit Priorität 4 oder höher. Umfasst sowohl Empfehlungen der Ebenen 1 bis 3 als auch Empfehlungen, die bei einer mäßigen Abweichung der Lastverteilung des Clusters einsetzen.    |
| Stufe 5, sehr aggressiv | Alle Empfehlungen. Umfasst sowohl Empfehlungen der Ebenen 1 bis 4 als auch Empfehlungen, die bei einer leichten Abweichung der Lastverteilung des Clusters einsetzen.                         |

## DRS-Regeln und Gruppen

Wenn Sie DRS in Ihrem Unternehmen einsetzen können, haben Sie ebenfalls die Möglichkeit, Regeln für virtuelle Maschinen und Gruppen für ESXi Hosts einzurichten. Gerade wenn sich mehrere Hosts in einem Cluster befinden, ist es oft sinnvoll, die VMs nach Bedarf anders zu verteilen, als es vom vCenter Server rein über die Last gesteuert wird.

Haben Sie zwei örtlich getrennte Rechenzentren, garantiert eine Gruppenbildung über mehrere Hosts, dass die VMs zum Beispiel regional getrennt laufen können. Das ist z.B. nützlich, wenn Sie mehrere Domänencontroller (DC) haben und diese auf unterschiedlichen ESXi Servern oder sogar Standorten laufen sollen.

Die Regeln für die VMs umfassen das Zusammenhalten und das Separieren. Für DCs wäre also das Separieren sinnvoll, aber für einen Anwendungsserver, der über das Netzwerk auf eine externe Datenbank zugreift, das Zusammenhalten, damit der Netzwerkverkehr nur über den virtuellen vSwitch läuft.

- **VIRTUELLE MASCHINEN ZUSAMMENHALTEN**, ist für VMs gedacht, die sich z.B. viel über das Netzwerk unterhalten. Sind diese auf demselben Host, ist die Datenübertragung deutlich höher, weil die Pakete die Netzwerkkarte gar nicht erst erreichen. Beim VMCI (Virtual Machine Communication Interface) müssen die beteiligten VMs auf demselben Host bleiben.
- **SEPARATE VIRTUELLE MASCHINEN** laufen immer (außer eventuell bei einem HA-Fall) auf unterschiedlichen Hosts. Das ist sinnvoll, wenn man z.B. einen Microsoft-Cluster aufbauen möchte: Fällt ein Host aus, sind nicht gleich beide Maschinen betroffen.

Lassen Sie mich das an einem einfachen Beispiel verdeutlichen:

Einer meiner Kunden hat zwei Serverräume, die durch eine Feuerschutzwand voneinander getrennt sind. Die insgesamt vier ESXi Server haben auf einen gemeinsamen Storage Zugriff, auf dem sich alle VMs befinden. Zwei der Hosts laufen links, die anderen beiden rechts. Er möchte seine Domänencontroller separieren und seinen Datenbank- und Anwendungsserver auf einem Host zusammenhalten. Weiterhin sollen alle XP-Clients

nur im linken Serverraum laufen, weil dort die beste Anbindung über VMware View (Virtual Desktops) für die Thin-Clients besteht.

Zuerst erstellen wir zwei Gruppen für die ESXi Server:

1. Wählen Sie auf der linken Hälfte des Fensters den DRS-GRUPPENMANAGER an.
2. Klicken Sie im unteren Teil, unter HOST-DRS-GRUPPEN auf HINZUFÜGEN und Tippen Sie bei NAME *Links* ein. Übernehmen Sie die beiden Hosts für diese Gruppe. Wenn Sie auf OK klicken, kehren Sie automatisch zurück.
3. Wiederholen Sie den Vorgang für die Gruppe *Rechts*.
4. Unter VM-DRS-GRUPPEN können wir jetzt die Gruppe der virtuellen Maschinen für VMware View erstellen. Klicken Sie auf den Button HINZUFÜGEN im oberen Teil des Fensters.
5. Tippen Sie bei NAME »View Clients« ein. Übernehmen Sie die gewünschten VMs für diese Gruppe (das geht auch mit einem Doppelklick). Wenn Sie auf OK klicken, kehren Sie automatisch zurück.
6. Nun wählen wir REGELN aus und klicken auf HINZUFÜGEN.
7. Geben Sie den Namen *View Links* ein, wählen Sie unter Typ VIRTUELLE MASCHINEN ZU HOSTS. Bei CLUSTER-VM-GRUPPE steht die angelegte Gruppe bereits drin. Überlegen Sie sich, ob die XP-Maschinen links laufen müssen oder sollten, und klicken Sie auf OK.
8. Zurückgekehrt klicken wir wieder auf HINZUFÜGEN. Geben Sie den Namen DATENBANKSERVER ein und wählen Sie unter Typ VIRTUELLE MASCHINEN ZUSAMMENHALTEN. Anschließend wählen Sie HINZUFÜGEN und aktivieren die Kästchen für Ihre beiden Datenbank- und Anwendungsserver. Da wir hier nicht festlegen müssen, ob diese links oder rechts laufen, brauchen wir nichts weiter zu tun.
9. Die Regel für die Domänencontroller können wir mit SEPARATE VIRTUELLE MASCHINEN allein leider nicht erschlagen, denn einer soll ja links und der andere rechts laufen. Dafür müssen wir für jeden DC wieder eine Gruppe erstellen und diese dann aufteilen. Der Vorgang ist ähnlich wie bei der View-Gruppe, deshalb wiederhole ich ihn nicht extra.
10. Haben Sie alle Regeln eingetragen, bekommen Sie das Bild, das in Abbildung 10-28 zu sehen ist.
11. Die Gruppe *Rechts* hätte nicht extra erstellt werden müssen, denn Sie können für den zweiten DC im Gruppenmanager auch wählen DARF NICHT AUF HOSTS IN DER GRUPPE AUSGEFÜHRT WERDEN. Das geht zwar, ist aber unübersichtlich.



Beachten Sie dabei, dass sowohl bei DARF NICHT AUF ... als auch bei MUSS AUF ... die Regel bestimmt, dass bei einem HA-Fall diese Rechner nicht auf den anderen ESXi Host neu gestartet werden. Wenn Sie umgekehrt »sollte« wählen, kann der Lastausgleich bei DRS dafür sorgen, dass die VMs trotzdem gegen diese Regeln verstoßen.



| Name                                                         | Typ                                | Definiert von |
|--------------------------------------------------------------|------------------------------------|---------------|
| <input checked="" type="checkbox"/> Datenbankserver          | Virtuelle Maschinenzusammenfassung | Benutzer      |
| vm-W2K3-64                                                   |                                    |               |
| vm-W2K3-Test                                                 |                                    |               |
| <input checked="" type="checkbox"/> View Links               | VMs auf Hosts ausführen            | Benutzer      |
| View Clients                                                 | Cluster-VM-Gruppe                  |               |
| Links                                                        | Clusterhostgruppe                  |               |
| <input checked="" type="checkbox"/> Domänencontroller links  | VMs auf Hosts ausführen            | Benutzer      |
| View Clients                                                 | Cluster-VM-Gruppe                  |               |
| Links                                                        | Clusterhostgruppe                  |               |
| <input checked="" type="checkbox"/> Domänencontroller rechts | VMs auf Hosts ausführen            | Benutzer      |
| Domänencontroller rechts                                     | Cluster-VM-Gruppe                  |               |
| Rechts                                                       | Clusterhostgruppe                  |               |

Abbildung 10-28: DRS-Gruppen

12. Haben Sie Regeln erstellt, die sich widersprechen oder nicht erfüllt werden können, wird das meist bereits in diesem Fenster angezeigt. Zur Sicherheit können Sie aber auch auf der Registerkarte DRS auf die Schaltfläche FEHLER klicken. Dort werden auch Fehler angezeigt, die erst zur Laufzeit aufgetreten sind bzw. erkannt wurden. Grundsätzlich gilt, dass bei gegensätzlichen Regeln die zuerst erstellte gültig ist und die jüngere ungültig.



Durch falsche Regeln können Sie verhindern, dass DRS korrekt funktioniert. Können VMs nicht verschoben werden, funktioniert auch das DPM nicht und der Host kann nicht in den Wartungsmodus versetzt werden. Somit scheitert auch der Update Manager!

## Optionen für virtuelle Maschinen

An diesem Punkt kann die Automatisierungsebene für die einzelnen VMs außer Kraft gesetzt werden. Bestimmen Sie, ob eine einzelne VM verschoben werden soll (VOLLAUTOMATISCH), nur beim Einschalten automatisch platziert wird (TEILAUTOMATISIERT) oder immer auf demselben Host läuft (DEAKTIVIERT).

## Energieverwaltung

Ob Sie die Energieverwaltung verwenden wollen, bleibt Ihnen überlassen. Standardmäßig ist sie deaktiviert. Reichen für die laufenden VMs, z.B. nachts, die Ressourcen von nur einem Teil der Hosts aus, wird ein Host freigeräumt und anschließend in den Schlafmodus gesetzt. Gegebenenfalls wird das Prozedere wiederholt, bis nur noch ein ESXi Server alle VMs hostet. Über Wake on LAN, IPMI oder ein ILO-Board werden bei Bedarf ein oder mehrere Hosts reaktiviert.

Sie können gegebenenfalls unter DRS → ENERGIEVERWALTUNG → HOSTOPTIONEN einzelne ESXi Server auswählen, die nicht in den Suspend-Modus gehen oder nur manuell dort hingeschickt werden sollen (siehe Abbildung 10-29).

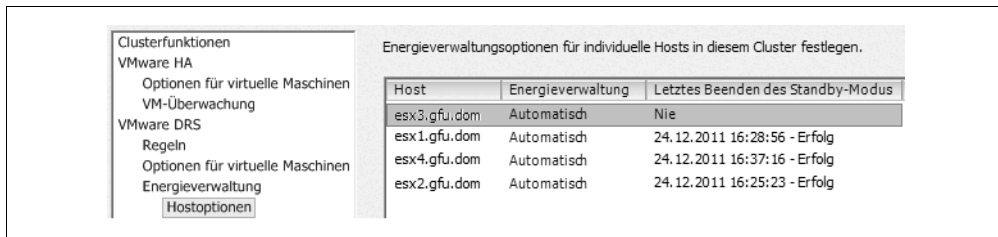


Abbildung 10-29: Hostoptionen für die Energieverwaltung



Die Automatisierungsebene von DPM entspricht nicht der von DRS. So wird z.B. bei MANUELL nur eine Empfehlung gegeben.



Wenn das oben erwähnte Szenario in Ihrem Betrieb sinnvoll ist, testen Sie die Funktionalität und den Zeitbedarf des Wiedererweckens vorher aus. Wollen morgens um acht Uhr alle Mitarbeiter gleichzeitig auf Ihre Server zugreifen, müssen die Hosts aus dem Suspend-Modus kommen und neu gestartet werden, und die VMs müssen alle wieder verteilt (migriert) werden.

Seit der Version 4.1 von VMware vSphere gibt es die Möglichkeit, einen geplanten Task zu erstellen, der die DPM-Einstellungen zu einem bestimmten Zeitpunkt ändert. Sie können also z.B. den DPM-Modus jeden Abend nach der Datensicherung automatisch einschalten. Der erste Host fährt erst in den Suspend-Modus, wenn die Last dementsprechend niedrig ist. Für den Morgen können Sie dann DPM ca. eine Stunde vor Dienstbeginn wieder ausschalten, damit die ESXi Server bis zum Dienstantritt alle gestartet sind und die VMs nach Last über DRS verteilt haben (siehe auch »DPM einrichten« weiter unten).

## VMware EVC

EVC (*Enhanced vMotion Compatibility*) steht für den Kompatibilitätsmodus der beteiligten Prozessoren aller Hosts, die beim Migrieren der VMs beteiligt sind. So kann verhindert werden, dass Hosts zum Cluster hinzugefügt werden, die nicht kompatibel sind. Weiterhin werden für alle beteiligten VMs die Masken für die CPU-Funktionen angeglichen, damit bei vMotion keine Fehler passieren.



Die in Abbildung 10-30 dargestellte Meldung sollten Sie genau lesen. Es werden diejenigen VMs angezeigt, die Funktionen nutzen, die die anderen beteiligten Hostprozessoren nicht haben. Die Meldung über nicht kompatible ESXi Server-Prozessoren im Cluster sieht genauso aus.

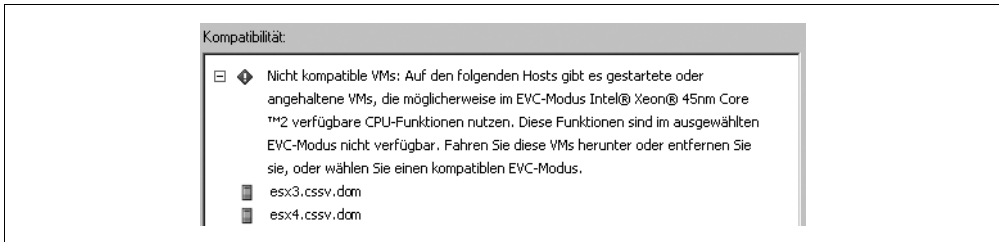


Abbildung 10-30: EVC-Modusmeldung: nicht kompatible virtuelle Maschinen

## Speicherort der Auslagerungsdatei

Für alle im Cluster befindlichen VMs kann hier der Ort der Auslagerungsdatei festgelegt werden. Diese Einstellung überschreibt keine anderen explizit gewählten Optionen, z. B. in den Einstellungen der VM. Beachten Sie aber, dass die *.vswp*-Datei der virtuellen Maschine auf einem anderen Storage die Performance negativ beeinflussen kann.

Wenn Sie alle Einstellungen vorgenommen haben und das Assistentenfenster geschlossen wurde, werden auf den Hosts die HA-Agenten aktiviert und für den Cluster konfiguriert. Im unteren Teil des Bildschirms bei KÜRZLICH BEARBEITETE AUFGABEN sehen Sie die Fortschrittsbalken der einzelnen Hosts.



Sind alle ESXi Server mit dem Vorgang fertig und werden weiterhin gelbe Dreiecke für Warnungen oder rote Rauten für Fehlermeldungen angezeigt, stimmt meist etwas nicht mit dem Netzwerk. DNS funktioniert nicht (Sie müssen die Hosts manuell hinzufügen), die IP-Adresse wurde einem anderen Rechner zugewiesen, oder die Hosts-Datei enthält einen Schreibfehler. Sobald der Fehler behoben ist, klicken Sie mit der rechten Maustaste auf den Host und wählen im Kontextmenü NEU KONFIGURIEREN FÜR VMWARE HA.

Bei der Registerkarte ÜBERSICHT wird eine Anzeige mit den vier Teilen ALLGEMEIN, VMWARE HA, VMWARE DRS und SPEICHER des Clusters mit Ihren Einstellungen gefüllt. Bei HA und DRS gibt es nochmals Links, über die weitere Infos in einem separaten Fenster geboten werden. Die weiteren Registerkarten bieten eine gute Zusammenfassung, die folgende Punkte betreffen:

- VIRTUELLE MASCHINEN – alle laufenden virtuellen Maschinen
- HOSTS – die Ressourcenauslastung aller Hosts
- DRS – Empfehlungen, Fehler und Verlauf von Load-Balancing
- RESSOURCENZUTEILUNGEN für RAM, CPU und Storage IO der VMs mit ihren prozentualen Anteilen
- LEISTUNG – zweigeteilte Übersicht mit Leistungsdiagrammen und einem Überblick über die Hosts und virtuellen Maschinen (häufig mehrere Seiten, die man über die Schaltflächen ganz rechts aufruft, siehe Abbildung 10-31)

Abbildung 10-31: Weitere Seiten zur Performance anwählen

- AUFGABEN UND EREIGNISSE von allen untergeordneten Objekten, also Clustern, Hosts und VMs
- ALARME – Ausgelöste Alarmer und ihre Definitionen (dazu später mehr in Kapitel 15)
- BERECHTIGUNGEN, die von hier auf alle untergeordneten Objekte vererbt werden,
- ZUORDNUNGEN – eine grafische Darstellung der Beziehungen zwischen Host, VMs, Datenspeicher und VM-Netzwerkswitches
- PROFIL-ÜBEREINSTIMMUNG – Hostprofile (siehe weiter unten detailliert in Kapitel 11)
- SPEICHERANSICHTEN – aufgeteilt in eine Übersicht des Platzverbrauchs der einzelnen VMs (BERICHTE) und die grafischen ZUORDNUNGEN

## DPM einrichten

Voraussetzung für *Distributed Power Management* ist zunächst ein Cluster, der über einen vCenter Server ausgeführt wird. Nur so können ESXi Hosts in den Suspend-Modus geschickt und auch neu gestartet werden. Für das Erwachen bzw. den Neustart benötigen die Hosts eines von drei Energieverwaltungsprotokollen mit unterstützter Hardware:

- IPMI – Intelligent Platform Management Interface,
- iLO – Hewlett-Packard Integrated Lights-Out oder
- WOL – Wake on LAN.

Hat ein Host mehrere der drei obigen Möglichkeiten, wird eine feste Reihenfolge von VMware definiert: IPMI, iLO, WOL.

Beachten Sie bei der Konfiguration die Hinweise des Hardwareherstellers und die Einstellungen im BIOS jedes Systems, damit das Erwecken auch erfolgreich ist. Bei IPMI unterstützt VMware nur die MD5- und textbasierte Authentifizierung. Die notwendigen Informationen für das Erwecken können Sie am Host über die Registerkarte KONFIGURATION → ENERGIEVERWALTUNG → EIGENSCHAFTEN einrichten.

### Einrichten von WOL für DPM

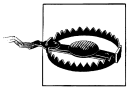
Zunächst sollten Sie überprüfen, welche von Ihren Netzwerkkarten überhaupt WOL unterstützen. Das finden Sie beim Host über die Registerkarte KONFIGURATION → NETZWERKADAPTER heraus (siehe Abbildung 10-32). Merken Sie sich die Adapter und schauen Sie nach, ob die VMkernel-Portgruppe für vMotion eine unterstützte Karte angeschlossen hat, sonst funktioniert es nicht.

| Netzwerkkarten                                                                           |                 |                         |          |
|------------------------------------------------------------------------------------------|-----------------|-------------------------|----------|
| Gerät                                                                                    | Geschwindigkeit | Wake-on-LAN unterstützt | Switch   |
| <b>82571EB Gigabit Ethernet Controller</b>                                               |                 |                         |          |
|  vmnic1 | 1000 Voll       | Nein                    | vSwitch2 |
|  vmnic0 | 1000 Voll       | Ja                      | vSwitch1 |
| <b>NetXtreme BCM5722 Gigabit Ethernet</b>                                                |                 |                         |          |
|  vmnic2 | 1000 Voll       | Ja                      | vSwitch0 |

Abbildung 10-32: Ansicht der Netzwerkkarten, die WOL unterstützen

Weiterhin müssen Sie im Cluster mindestens zwei unterstützte Hosts ab Version 3.5 haben, und der vMotion-Netzwerkverkehr darf nicht geroutet werden, muss sich also im selben Subnetz befinden.

Beachten Sie, dass manche NICs WOL nur unterstützen, wenn sie auf die automatische Geschwindigkeit und den Duplexmodus gestellt sind, also z.B. nicht auf 1000/Voll.



Überprüfen Sie unbedingt die korrekte Funktionalität anhand eines manuellen Suspend-Modus für jeden beteiligten Host, sonst kann es passieren, dass ein nicht unterstützter Server bei Bedarf nicht wieder automatisch startet. Weiterhin sollten Sie den vordefinierten Alarm *Fehler bei Standby-Beendigung* unbedingt für eine Meldung einrichten.



Beachten Sie auch andere installierte Überwachungssoftware, z.B. SNMP, sonst bekommen Sie unnötige Meldungen, wenn ein Host in den Standby-Modus geht.

## Fault Tolerance einrichten

Wie bereits oben erwähnt, kann man wichtige laufende VMs auf einen anderen Host »spiegeln«, damit bei einem Ausfall der Hardware diese VMs weiterlaufen und alle Daten konstant bleiben (siehe Abbildung 10-33). Die angemeldeten User merken von dem Ausfall dann nichts. Der Ressourcenverbrauch ist durch zwei Maschinen zwar doppelt so hoch, da die sekundäre Maschine aber keine Anfragen aus dem Netz beantwortet, ist die Performance der VM nicht höher.

Als Voraussetzung für den Einsatz von FT ist einiges mitzubringen:

1. Sie müssen einen funktionierenden HA-Cluster mit mindestens zwei Hosts haben, die als FT-tauglich ausgewiesen sind (siehe <http://www.vmware.com/resources/compatibility/search.php>).
2. Mindestens zwei Hosts im Cluster müssen die gleichen, von FT unterstützten Prozessoren haben. Dazu gehören z.B. Intel Xeon-Prozessoren der Serien 31xx, 33xx bis 36xx, 52xx, 54xx bis 56xx, 74xx und 75xx und AMD-Prozessoren der Serien 13xx, 23xx, 24xx, 61xx, 83xx und 84xx. Je nach Prozessor und Gastbetriebssystem muss die VM ausgeschaltet sein, damit FT aktiviert werden kann (siehe auch <http://kb.vmware.com/kb/1008027>).

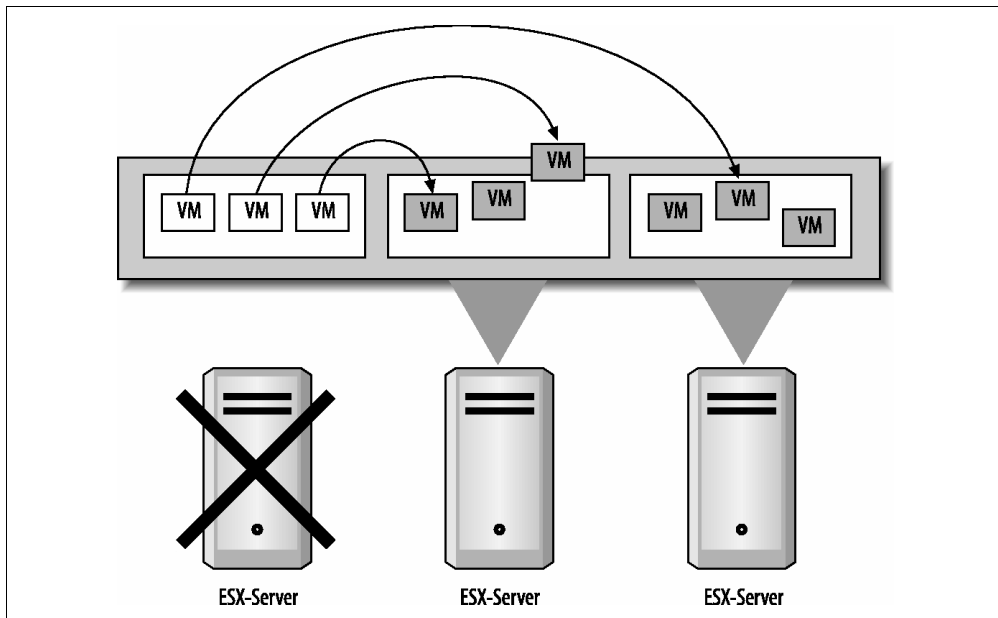


Abbildung 10-33: Funktionsprinzip von Fault Tolerance

3. Im BIOS des ESXi Servers muss die Hardwarevirtualisierung (HV) eingeschaltet sein.
4. Es muss jeweils ein VMkernel-Port für FT (Protokollierung der Fehlertoleranz mit vLockstep) eingerichtet sein (nur IPv4) und sollte wegen der Bandbreite nicht gleichzeitig für vMotion oder iSCSI-Zugriff genutzt werden. Hier werden 10-GBit-Ethernet und Jumbo-Frames empfohlen. vMotion wird zusätzlich gebraucht. Weiterhin sollten Sie für die beteiligten Portgruppen denselben Namen verwenden und aus Datensicherheitsgründen ein getrenntes Netz oder VLAN verwenden. Alle Daten werden von VMware vLockstep ohne Verschlüsselung übertragen.
5. Die Hostzertifikatsüberprüfung muss für alle Hosts aktiviert sein.
6. Alle Hosts müssen dieselbe Version und dasselbe Patch-Level haben, erkennbar auf der ESXi-Seite über den Registern.
7. Die VMs dürfen keine »Thin-Provisioning«-Festplatten (schnelle Bereitstellung) haben, diese können aber im Zuge der FT umgewandelt werden.
8. Es sollten nicht mehr als 16 virtuelle Festplatten zur VM gehören.
9. Raw Device Mapping (RDM) wird nicht unterstützt, und auch keine Bindung von CD oder Floppy am Host und keine paravirtuellen Festplatten.
10. Das Hinzufügen von USB und Soundkarten wird nicht unterstützt.
11. N\_Port-ID-Virtualisierung (NPIV) darf die virtuelle Maschine nicht nutzen.
12. Die NIC-Passthrough-Funktion wird von der Fehlertoleranz nicht unterstützt und muss daher ausgeschaltet werden.

13. Netzwerkschnittstellen für Legacy-Netzwerkhardware, also veraltete Netzwerkkarten, sind nicht möglich. Nehmen Sie möglichst eine vmxnet2-, vmxnet3- oder E1000-Karte.
14. Es kann keine Hardware im laufenden Betrieb hinzugefügt werden.
15. Die virtuelle Maschine darf keine Paravirtualisierung (VMI) verwenden, da sie sonst nicht ordnungsgemäß eingeschaltet wird.
16. Der zugewiesene RAM der VM wird als Reservierung gesetzt und muss komplett auf beiden ESXi Servern vorhanden sein. Weiterhin wird EPT/RVI automatisch deaktiviert.
17. Die Dateien der VM müssen von beiden beteiligten Hosts erreichbar sein. Zu den akzeptierten gemeinsam genutzten Speicherlösungen gehören Fibre-Channel, iSCSI (Hardware und Software), NFS und NAS.
18. Nur Ein-Prozessor-Maschinen werden unterstützt.
19. VMware DRS ist für die gespiegelten Maschinen nicht verfügbar, sie kann also nicht auf einen anderen Server geschoben werden.
20. Gemachte Snapshots müssen vorher entfernt werden, und während der Spiegelung können keine erstellt werden. Damit ist auch keine Datensicherung über DataRecovery möglich.
21. Storage vMotion ist für virtuelle Maschinen mit aktivierter Fehlertoleranz nicht möglich. Wenn Sie es dennoch benötigen, sollten Sie die Fehlertoleranz vorübergehend deaktivieren und die Storage vMotion-Aktion durchführen. Danach können Sie die Fehlertoleranz wieder aktivieren.
22. Die VM darf keine serielle oder parallele Schnittstelle verwenden.
23. Bei der Grafikkarte wird kein 3-D unterstützt.

Folgende Gastbetriebssysteme werden unterstützt:

- Microsoft Windows NT 4.0, 2000, XP 32 und 64 Bit, Server 2003 32 und 64 Bit, Vista, Server 2008 und Windows 7
- alle Linux-Distributionen, die in der Liste der Gastbetriebssysteme auf dem ESXi aufgelistet sind
- Solaris 10 32 und 64 Bit
- alle FreeBSD-Versionen, die in der Liste der Gastbetriebssysteme auf dem ESXi aufgelistet sind

## Fehlertoleranz einschalten

Über die rechte Maustaste auf einer VM können Sie die Fehlertoleranz einschalten. Wenn Ihr Versuch, die Fehlertoleranz für eine virtuellen Maschine einzuschalten, die Validierungsprüfungen besteht, wird die sekundäre virtuelle Maschine erstellt, und der

gesamte Zustand der primären virtuellen Maschine wird kopiert. Die Platzierung und der sofortige Status der sekundären virtuellen Maschine sind davon abhängig, ob die primäre virtuelle Maschine eingeschaltet oder ausgeschaltet war, als Sie die Fehlertoleranz eingeschaltet haben.

Wenn die primäre virtuelle Maschine eingeschaltet ist, ...

- ... wird die sekundäre virtuelle Maschine auf einem separaten kompatiblen Host erstellt und eingeschaltet, sofern die freien Ressourcen das zulassen.
- ... lautet der im vSphere Client auf der Registerkarte ÜBERSICHT für die virtuelle Maschine angezeigte Fehlertoleranzstatus GESCHÜTZT.

Wenn die primäre virtuelle Maschine ausgeschaltet ist, ...

- ... wird die sekundäre virtuelle Maschine sofort erstellt und bei einem Host im Cluster registriert (sie wird möglicherweise auf einen besser geeigneten Host verschoben, wenn sie eingeschaltet wird).
- ... wird die sekundäre virtuelle Maschine erst eingeschaltet, wenn die primäre virtuelle Maschine eingeschaltet wurde.
- ... lautet der im vSphere Client auf der Registerkarte ÜBERSICHT für die virtuelle Maschine angezeigte Fehlertoleranzstatus NICHT GESCHÜTZT, VM WIRD NICHT AUSGEFÜHRT (siehe Abbildung 10-34).

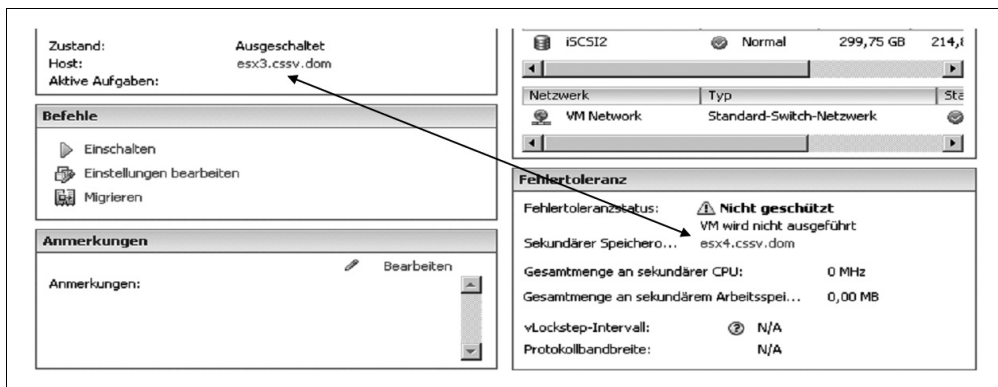


Abbildung 10-34: Fault Tolerance-Status

- ... werden die oben aufgeführten zusätzlichen Überprüfungen durchgeführt, wenn Sie versuchen, die primäre virtuelle Maschine einzuschalten, nachdem die Fehlertoleranz eingeschaltet wurde.
- ... werden die primäre und die sekundäre virtuelle Maschine eingeschaltet und auf separaten, kompatiblen Hosts platziert, wenn diese Tests bestanden wurden. Der im vSphere Client auf der Registerkarte ÜBERSICHT für die virtuelle Maschine angezeigte Fehlertoleranzstatus lautet dann GESCHÜTZT (siehe Abbildung 10-35).



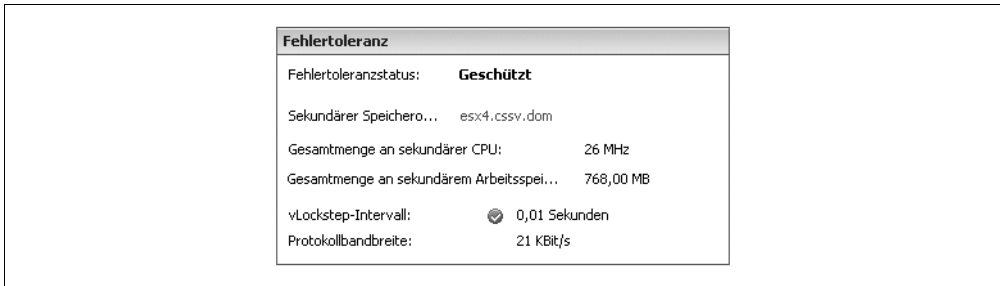


Abbildung 10-35: Meldung über geschützten FT-Status

Nach dem Erstellen der Fault Tolerance befinden sich im Ordner der virtuellen Maschine sechs neue Dateien:

- *shared.vmtx* sieht in etwa so aus:

```
.encoding = "UTF-8"
generation = "1"
primary.uuid = "52 23 64 62 6a f8 c0 95-1d 0f 1a d8 44 68 7a fb"
primary.vmxFilePath = "/vmfs/volumes/4a5cb7b6-92291a54-0ac0-001b2117d9be/XP-4/XP-4.vmx"
secondary.secondary0.enabled = "1"
secondary.secondary0.uuid = "50 23 fb ed f2 10 f2 18-42 d2 83 8e 74 df 50 d5"
secondary.secondary0.valid = "1"
secondary.secondary0.vmxFilePath = "/vmfs/volumes/4a5cb7b6-92291a54-0ac0-001b2117d9be/XP-4/XP-4_1.vmx"
uuid = "50 23 fb ed f2 10 f2 18-42 d2 83 8e 74 df 50 d5"
```

- *VM1\_1.vmx* ist fast identisch mit der Originaldatei *VM1.vmx*.
- *VM1\_1.vmx* ist fast identisch mit dem Original – lediglich der Name hat einen Unterstrich mit einer 1 (*\_1*).
- Nach dem Einschalten bekommt die sekundäre VM noch eine BIOS-Datei namens *VM1\_1.nvram*.
- Die Logdateien werden ebenfalls für beide Maschinen separat gehalten. Für die primäre ist es weiterhin *vmware.log*, für die sekundäre *vmware-<name>.log*. Auch die Auslagerungsdatei der VMs gibt es jetzt doppelt, allerdings ist sie jeweils 0 Byte groß.
- Schauen Sie direkt auf der Kommandozeile und nicht mit dem Datastore-Browser nach, sehen Sie noch eine versteckte leere Datei mit Namen *.ft-generation2*.

Haben Sie an alles gedacht und hat alles funktioniert, sollten Sie den Status bei der primären VM sehen können, der in Abbildung 10-36 dargestellt ist.



Abbildung 10-36: Anzeige der primären und sekundären VM

Sollten Sie Probleme mit der Aktivierung von Fault Tolerance bei Ihrem Gast haben, empfehle Ihnen ich das ca. 6 MByte große, kostenlose Tool *SiteSurvey* von VMware, das Sie unter [http://www.vmware.com/download/shared\\_utilities.html](http://www.vmware.com/download/shared_utilities.html) herunterladen können.

Nur wenige Sekunden nach der Installation zeigt das Programm über den Standardbrowser die Ergebnisse an. Achten Sie auf die kompatiblen Hosts und vor allem auf die roten Kästchen bei den VMs, die die Begründung für das erfolglose Einschalten von FT anzeigen.



In der normalen Bestandsliste sehen Sie anschließend nur die primäre Maschine. Auf dem ESXi Server oder dem Cluster können Sie aber das Register VIRTUELLE MASCHINEN anklicken, dann sehen Sie beide (siehe Abbildung 10-36): Die in kräftigem Blau ist die primäre, die mit dem fast weißen Symbol die sekundäre VM.

Sollten trotz aller Maßnahmen Fehler bei den gespiegelten VMs auftreten, hilft Ihnen die deutschsprachige PDF-Datei *vsphere-esxi-vcenter-server-50-availability-guide.pfd* ab Seite 37 weiter (auf der Website zum Buch).

Übrigens sollten Sie die HA-Funktion nicht ausschalten, wenn Fault Tolerance aktiv ist (siehe Abbildung 10-37).

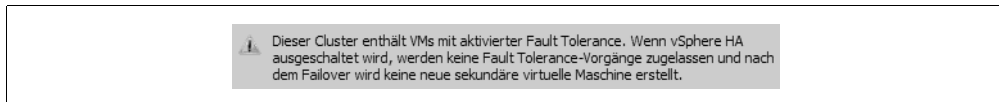


Abbildung 10-37: Fault Tolerance bedingt High Availability.

Jetzt kennen Sie die wichtigsten Komponenten und Funktionen des vCenter Servers. Was es sonst noch alles gibt und welche Möglichkeiten sich dadurch bieten, ist Gegenstand der folgenden Kapitel.

# VSA und Hostprofile

Wenn Sie nur zwei oder drei ESXi Hosts haben, können Sie vSphere Storage Appliance nutzen, und wenn Sie viele ESXi Server der Version 5 haben (nur die werden unterstützt), können Sie Hostprofile nutzen, um Unterschiede in der Konfiguration der Hosts festzustellen. Wollen Sie eine sehr große Anzahl von ESXi Servern schnell bereitstellen, nehmen Sie vSphere Auto Deploy.

Bei den Hostprofilen können Sie sich einen Referenzhost aussuchen und von ihm ein Profil erstellen und dann die anderen Server damit vergleichen. Sie müssen auch nicht jeden Host einzeln über die grafische Oberfläche oder die Kommandozeile manuell einstellen. Die Funktionen *Hostprofile* und *Auto Deploy* sind nur in der Enterprise Plus-Version verfügbar oder auch, solange Sie Ihre Lizenz noch nicht eingespielt haben – im Evaluierungsmodus stehen Ihnen alle Funktionen bis zu 60 Tage zur Verfügung.

Von einem Referenzhost werden Netzwerkeinstellungen, Storages (bedingt), Sicherheitsprofil (Firewall), NTP-Einstellungen und einiges mehr in einem Hostprofil abgespeichert. Das erstellte Profil kann auch auf einen Cluster angewendet werden, damit alle darin befindlichen Server überprüft werden.

## Hostprofil erstellen

Richten Sie sich einen Host vollständig nach Ihren Bedürfnissen und Erfordernissen ein und erstellen Sie anschließend von ihm ein Hostprofil. Achten Sie auf die genauen Einstellungen Ihres Referenzhosts (siehe auch Kapitel 5 – Konfiguration und Einstellungen des ESXi Servers), denn folgende Konfigurationen werden dabei berücksichtigt:

### *Arbeitsspeicher*

Die Reservierung für den Arbeitsspeicher sollte auf einen festen Wert eingestellt sein.

### *Speicherkonfiguration*

Die hinterlegten Werte für NFS, FCoE (Fibre Channel over Ethernet), Multipathing und iSCSI

## Netzwerk

Die Anzahl der virtuellen Netzwerkswitches und ihre Portgruppen, Einstellungen zum Standardgateway, Duplexmodus und Geschwindigkeit der Netzwerkkarten, Sicherheitseinstellungen beim vSwitch und seinen untergeordneten Portgruppen und gegebenenfalls Gruppierungsrichtlinien (NIC-Teaming)

## Datum und Zeit

Die NTP-Konfiguration mit der Serverzeitzone und NTP-Servereinträgen

## Dienste und Firewall

Die Einstellungen zur Firewall mit geöffneten oder geschlossenen Ports (nicht die Einstellungen, die gegebenenfalls auf der Kommandozeile vorgenommen wurden) und den zugehörigen Diensten bzw. Daemons

## Sicherheitskonfiguration

Passwort des Users root und SSH-Schlüssel für ihn

## Erweiterte Konfiguration

Eingestellte Werte in der erweiterten Konfiguration des ESXi Servers. Falls Sie hier Änderungen vorgenommen haben, weil der VMware-Support Sie dazu aufgefordert hat, werden diese auch in das Profil übernommen.

## Benutzer und Gruppen

Die erstellten Benutzer und Gruppen

## Weitere Optionen

Ressourcenpools, Energierichtlinien, Host-Cache-Einstellungen etc.

Haben Sie an alles gedacht und alle Einstellungen vorgenommen, klicken Sie mit der rechten Maustaste auf den fertigen ESXi Server und wählen aus dem Kontextmenü HOSTPROFIL → PROFIL VOM HOST ERSTELLEN.

Geben Sie einen Namen und eine Beschreibung für das Profil an (siehe Abbildung 11-1). Es ist von Vorteil, den Namen des Hosts mit anzugeben, damit später die Identifikation einfacher ist.

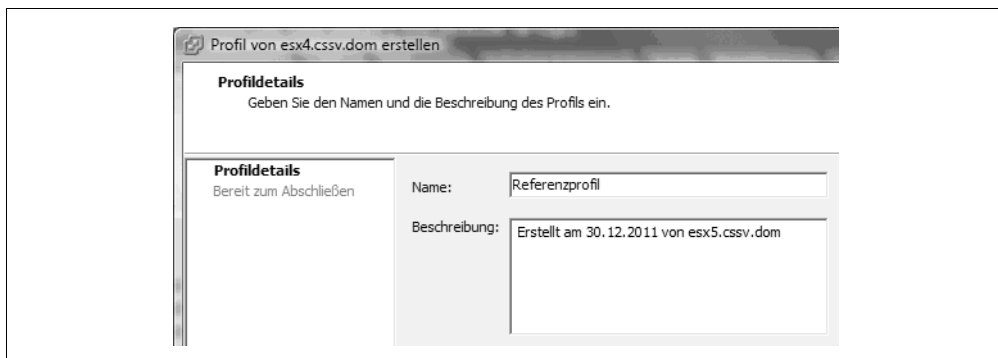


Abbildung 11-1: Referenzprofil von einem Host erstellen

Klicken Sie auf WEITER und anschließend auf BEENDEN – kurze Zeit später ist das Profil erstellt.

Über HOME → HOSTPROFILE können Sie Ihr Werk begutachten. Dort haben Sie auch die Möglichkeit, die Angaben zu bearbeiten (PROFIL BEARBEITEN) und abzuspeichern (PROFIL EXPORTIEREN). Letzteres speichert die Datei im VMware-Profilformat (.vpf).



Überprüfen Sie das Profil und nehmen Sie ggf. die Einstellungen zum iSCSI heraus. Sie sehen die Probleme nach der Übernahme nicht sofort, sondern erst, wenn der Host neu gestartet wurde. Dann kann der Hosts gegebenenfalls keine VM mehr starten oder per vMotion bekommen, die dort residiert.

In diesem Menü können Sie übrigens auch ein neues PROFIL ERSTELLEN. Über den Assistenten können Sie hier ebenfalls einen ESXi Server auswählen, der als Referenzhost gelten soll.

Möchten Sie sich die Einstellungen für später aufheben oder einen anderen Cluster damit konfigurieren, können Sie das Profil im VMware-Profilformat \*.vpf exportieren und z.B. im Netzwerk oder auf einem USB-Stick abspeichern. Zum Importieren gehen Sie wieder den gleichen Weg wie vorher: Über HOME → HOSTPROFILE klicken Sie auf das Symbol PROFIL ERSTELLEN. Im Assistenten wählen Sie die Option zum Importieren eines Profils, geben Speicherort und Dateinamen an und klicken auf WEITER. Wählen Sie einen aussagekräftigen Namen und gegebenenfalls eine Beschreibung und klicken Sie auf WEITER. Nachdem Sie auf BEENDEN geklickt haben, müsste das importierte Profil in der Liste erscheinen.

## Hostprofil bearbeiten

Wenn Sie sich ein Profil erstellt haben, können Sie es natürlich nachträglich noch bearbeiten oder ändern. Manchmal fällt einem erst nach einer gewissen Zeit auf, dass die eine oder andere gewählte Einstellung oder Richtlinie vielleicht doch nicht so toll war.

Über HOME → HOSTPROFILE wählen Sie das zu bearbeitende Profil aus und klicken auf HOSTPROFIL BEARBEITEN. Jetzt können Sie den Namen oder die Beschreibung ändern und die Richtlinie bearbeiten oder deaktivieren. Aktivieren Sie anschließend die Übereinstimmungsprüfung für die Richtlinie und klicken Sie auf OK, um den Profileditor zu schließen.

### Eine Richtlinie bearbeiten

Eine Richtlinie beschreibt, wie eine bestimmte eingestellte Konfiguration angewendet werden soll. Mit dem Profileditor können Sie diese Richtlinien bearbeiten.

Auf der linken Seite des Profileditors können Sie das Hostprofil erweitern, um die Unterprofile anwählen zu können, die nach Funktionsgruppen und Konfigurationsinstanzen

festgelegt sind. Jedes Unterprofil enthält einige Richtlinien, die die für das Profil relevanten Konfigurationen beschreiben.

Wenn Sie sich bis zu der zu ändernden Einstellung durchgehängt haben, wählen Sie auf der rechten Seite die Registerkarte KONFIGURATIONSinFORMATIONEN. Jetzt können Sie über das Drop-down-Menü eine Richtlinienoption auswählen und den gewünschten Parameter festlegen.

### Deaktivieren von Richtlinien

Bei den Hostprofilrichtlinien können Sie festlegen, ob eine Übereinstimmungsprüfung für jede Richtlinie durchgeführt werden soll. Im Profileditor navigieren Sie zur gewünschten Richtlinie und wählen auf der rechten Seite des Fensters die Registerkarte ÜBEREINSTIMMUNGSDetails aus. Soll diese Richtlinie ausgenommen werden, deaktivieren Sie einfach das Kontrollkästchen. Alle anderen Richtlinien werden weiterhin geprüft.

## Hostprofil anhängen

Nachdem Sie ein Profil einer beispielhaften Konfiguration erstellt haben, können Sie den zweiten ESXi Server auswählen und – wie oben – über das Kontextmenü ein Profil anhängen. Sie haben außerdem die Möglichkeit, die gesamten im Cluster befindlichen Hosts gemäß dem erstellten Profil zu überprüfen und auch das Referenzprofil allen Hosts im Cluster gleichzeitig zuzuweisen.



Vom Übernehmen eines Profils auf Clusterebene rate ich im Produktivbereich dringend ab, weil der jeweilige Host in den Wartungsmodus gesetzt werden muss. Sollten Probleme bei der Übernahme auftreten, befinden sich die Hosts gegebenenfalls in einem Zustand, in dem keine VM mehr gestartet werden kann. Wenn Änderungen an den Netzwerkeinstellungen vorgenommen werden müssen, bekommen Sie unnötig viele Alarmmeldungen.

Es gibt insgesamt vier Möglichkeiten, einem Host oder Cluster ein Profil anzuhängen:

1. über die Hauptansicht HOSTPROFIL,
2. über das Kontextmenü eines Hosts,
3. über das Kontextmenü eines Clusters oder
4. über die Registerkarte PROFIL-ÜBEREINSTIMMUNG des Clusters.

Wählen Sie aus dem Kontextmenü auf dem Host HOSTPROFIL → PROFIL VERWALTEN aus. In der Übersicht des ESXi Servers erscheint das angehängte Profil. Der nächste Schritt ist die Überprüfung auf Übereinstimmung der Konfiguration.

Klicken Sie im Kontextmenü auf HOSTPROFIL → ÜBEREINSTIMMUNG PRÜFEN. In der Registerkarte ÜBERSICHT sehen Sie das Ergebnis der Überprüfung. Falls dort eine

Unstimmigkeit aufgetaucht ist, können Sie über den Link ein weiteres Meldungsfenster öffnen und den Text begutachten. Ein Beispiel sehen Sie in Abbildung 11-2.

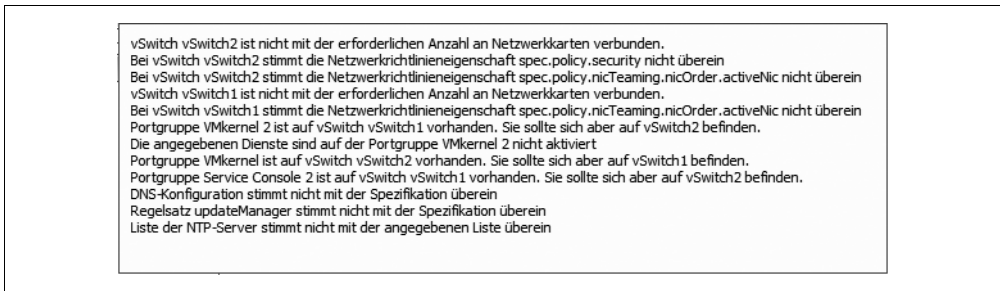


Abbildung 11-2: Meldung der Differenzen zum Referenzprofil

Sie können jetzt manuell die einzelnen Punkte durchgehen und verändern oder den ESXi Server in den Wartungsmodus versetzen und das Profil dann übernehmen, wie in Abbildung 11-3 beispielhaft zu sehen ist.

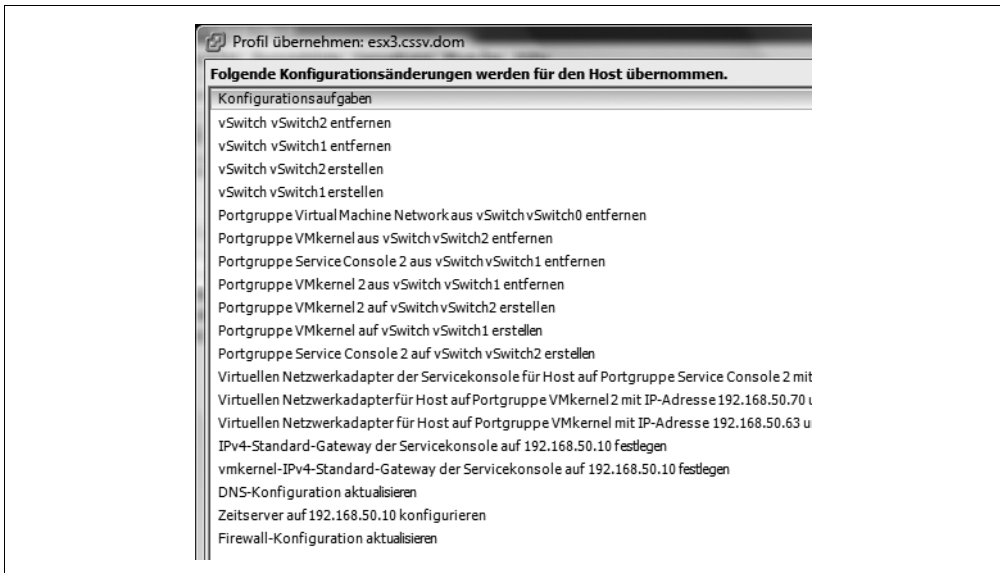


Abbildung 11-3: Fenster Profil übernehmen (Ausschnitt)

Klicken Sie auf die Schaltfläche BEENDEN, damit die Übernahme erfolgt.



Wenn der Vorgang abgeschlossen ist, wird die Fehlermeldung nicht automatisch zurückgesetzt. Klicken Sie erneut auf HOSTPROFIL → ÜBEREINSTIMMUNG PRÜFEN, bevor Sie nach möglichen Fehlern suchen. Als Ergebnis sollten Sie etwas Ähnliches wie in Abbildung 11-4 sehen.

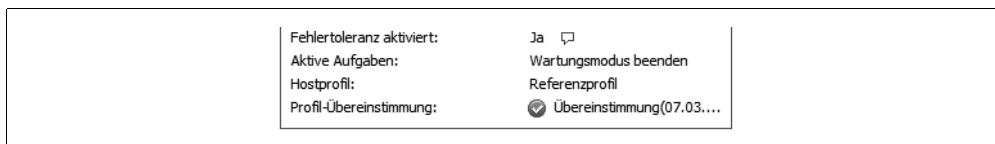


Abbildung 11-4: Meldung zur Übereinstimmung des Profils

Sollte bei Ihnen keine Übereinstimmung mit dem Referenzprofil zustande kommen, klicken Sie auf den blauen Link, neben *Profil-Übereinstimmung*, um Details zu sehen. Eventuell ist ein Neustart des Hosts nötig, damit er die Änderungen an seiner Konfiguration übernehmen kann. Wenn Sie in Ihrer Konfiguration auch unterschiedliche Management Network-Switches hatten, wird der Switch oder die Portgruppe gelöscht und anschließend neu mit der vorgegebenen Konfiguration erstellt. Dabei ist die Verbindung zum vCenter Server natürlich kurz unterbrochen. Sie werden also auf der Registerkarte ALARME → AUSGELÖSTE ALARME einen Eintrag finden, der besagt, dass die Netzwerkverbindung unterbrochen ist bzw. war.

Überprüfen Sie dann in den Einstellungen unter KONFIGURATION → NETZWERK, ob alles richtig geändert wurde und die Netzwerkkarten korrekt wieder verbunden sind, also die Verbindung wieder steht. Schauen Sie außerdem nach der richtigen Übertragungsrate der NICs, also z.B. 1000/Voll. Wenn alles in Ordnung ist, setzen Sie den Alarm auf grün, indem Sie ihn über das Kontextmenü löschen (rechte Maustaste).

Leider ist diese sehr hilfreiche Funktion nur in der teuersten Edition der Lizenzmodi enthalten, vSphere Enterprise Plus. Da man die Konfiguration der ESXi Server aber immer am Anfang der Einrichtung der virtuellen Welt vornimmt, kann man diese Funktion im nicht lizenzierten 60-Tage-Modus (der Evaluierungsmodus heißt bei VMware »Bewertungsmodus«) fast zwei Monate lang ausprobieren.

Auch wenn Sie ein Upgrade von Infrastructure 3.5 oder vSphere4 auf vSphere5 planen, sind die Hostprofile ein sehr nützliches Tool. Da ich in Umgebungen mit bis zu zehn ESX Servern und bis zu 300 virtuellen Maschinen ein etwas anderes Vorgehen bevorzuge, als VMware empfiehlt, habe ich für meine Kunden dieses Tool schon häufiger eingesetzt.

Dazu ein Beispiel: Sie haben drei ESX oder ESXi Server, mehrere virtuelle Maschinen und einen Virtual Center Server. Sie greifen üblicherweise mit dem Infrastructure Client auf den Virtual Center Server zu. VMware empfiehlt, als Erstes den Virtual Center Server auf den neuesten Stand zu bringen. Dann können Sie aber nicht mehr mit dem Infrastructure Client darauf zugreifen. Auf der CD zum vCenter Server befindet sich der vSphere Client, der auch üblicherweise beim Autostart der CD zur Installation angeboten wird. Weiterhin können Sie diesen einzeln von der Webseite des Unternehmens herunterladen.

Nach der Installation des Clients und des vCenter Servers können Sie den *Update Manager* installieren, um hinterher Ihre Hosts auf den neuesten Stand zu bringen. Sie müssen nur unter den Plugins auf dem vCenter Server die Erweiterung für Ihren vSphere Client installieren (*Update Manager Plug-In*).



Den Virtual Center Server können Sie nicht updaten, da er mittlerweile ein 64-Bit-Betriebssystem benötigt, was vorher nicht möglich war. Besser installieren Sie den vCenter Server neu und binden die »alten« ESX oder ESXi Hosts wieder an. Sie können die Daten aus der Datenbank des Virtual Center Servers exportieren und in den neuen vCenter Server importieren – wenn Sie das für notwendig erachten. Sie können aber auch den alten Server herunterfahren und später ggf. auf diesem die alten Daten nachsehen.

Haben Sie bereits eine vSphere 4.1-Umgebung, können Sie den vCenter Server natürlich updaten, ohne ihn neu installieren zu müssen. Details zum Upgraden einer alten auf die neue Version erhalten Sie in Kapitel 13.

## vSphere Auto Deploy

In großen Umgebungen kann man die Installation der gewünschten ESXi Hosts mithilfe von Skripten deutlich vereinfachen und beschleunigen (siehe Kapitel 3, *Der Hypervisor*). Ein standardmäßig installierter Host kann, wie bereits erwähnt, durch Hostprofile an die Clusterumgebung angepasst werden. vSphere Auto Deploy bietet eine weitere Möglichkeit, eine große Anzahl von ESXi Servern in kürzester Zeit an den Start zu bringen. Auch hier werden Skripten und Hostprofile eingesetzt.

Die heutige Hardware für die ESXi Server besitzt Netzwerkkarten, die beim Starten Informationen über PXE (*preboot execution environment*) aus dem Netzwerk ziehen können. Dabei muss eine gewisse Infrastruktur vorliegen, die in Abbildung 11-5 schematisch dargestellt ist.

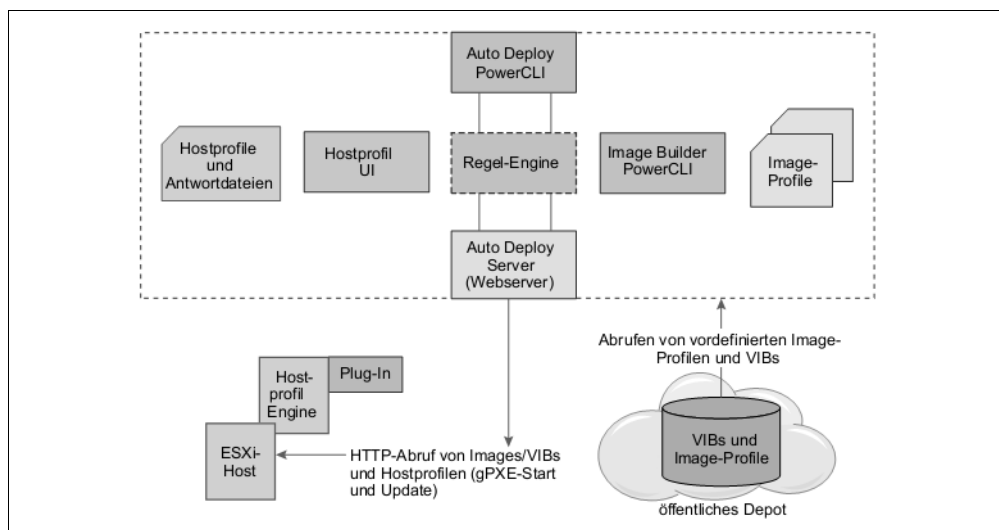


Abbildung 11-5: vSphere Auto Deploy-Komponenten

Sie brauchen also zunächst einen korrekt eingerichteten vCenter Server. Die vCenter Server Appliance auf Basis von SuSE Linux kann dafür ebenfalls genutzt werden, aber ESXi Autodeploy muss auf ihr ggf. separat gestartet werden. Weiterhin benötigen Sie

- die Installation des ESXi Dump Collectors,
- (optional, aber empfohlen) den Syslog Collector,
- das Paket vSphere Auto Deploy,
- das Image des ESXi Servers, das direkt in den Arbeitsspeicher des Hosts geladen wird,
- ein Auto Deploy Repository,
- ggf. einen vSphere Authentication Proxy und
- eine oder mehrere Antwortdateien.

Zu den Einzelheiten gibt es ein teilweise auf Deutsch und Englisch verfasstes PDF-Dokument von VMware namens *vsphere-esxi-vcenter-server-50-installation-setup-guide.pdf*. Dort wird ab Seite 63 detailliert die Vorgehensweise beschrieben, weshalb ich sie hier nicht wiederholen möchte. Einzelheiten zum Hostprofil können Sie diesem Dokument entnehmen, Installationsskripten dafür werden in Kapitel 3, *Der Hypervisor* beschrieben.

## VSA Storage

Mit der vSphere Storage Appliance, kurz VSA, wurde in Version 5 von VMware vSphere eine ganz neue Technologie für einen gemeinsamen Storage eingeführt. Das Besondere daran ist die gemeinsame Nutzung von lokalen Platten der beteiligten ESXi Server.

Und wie funktioniert es? Der Name »Appliance« sagt aus, dass es sich um eine vorgefertigte virtuelle Maschine handelt. Diese wird auf jedem Host (zwei oder drei) installiert bzw. als OVF-Vorlage bereitgestellt. Die VM nimmt sich den gesamten lokalen VMFS-Speicher und teilt ihn in zwei Bereiche auf: Der sogenannte *VSA Storage Cluster* repliziert einen Bereich jeweils auf den Nachbarhost und stellt damit dem jeweils anderem Host einen gespiegelten NFS-Storage zur Verfügung (siehe Abbildung 11-6). Beim Ausfall eines ESXi Servers steht der gespiegelte Bereich weiterhin dem anderem Host zur Verfügung, so dass HA weiterhin funktioniert.

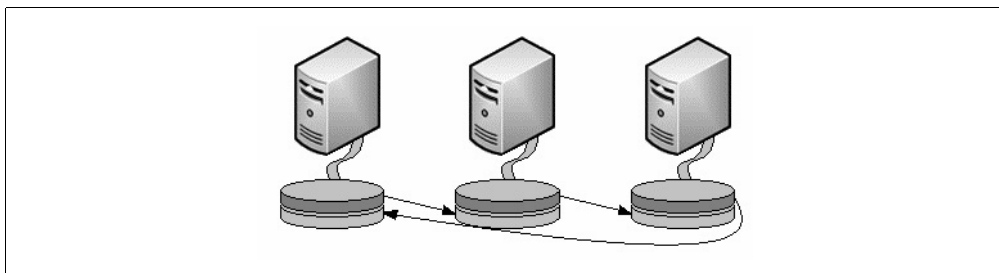


Abbildung 11-6: Funktionsprinzip eines VSA-Storage

## VSA-Einschränkungen

Bevor Sie mit der Installation des vSphere Storage Appliance Managers anfangen, lesen Sie bitte die folgenden Informationen durch und überlegen Sie sich dann, ob Sie es noch wollen.

Voraussetzungen für einen VSA Storage:

- Der VSA Manager muss auf einem aktuellen vCenter Server (5.0) installiert werden.
- Dieser Server kann nur eine VSA-Instanz für zwei oder drei Hosts zur Verfügung stellen, auch wenn in Ihrem Cluster mehr als drei Hosts vorhanden sind.
- Er braucht mindestens 3 GByte RAM und mindestens 4 GByte Festplattenspeicher.
- Er darf nur eine Netzwerkkarte und auch nur eine IP-Adresse haben.
- Er darf nicht auf einem lokalen Storage der ESXi Servers liegen, also entweder ein physischer Rechner oder eine VM in einem SAN.
- Die vSphere vCenter Server Appliance unterstützt diese Funktion nicht.
- Mindestens 75 % der lokalen Festplattenkapazität der Hosts gehen verloren, da lokal ein RAID 10 eingerichtet und davon die Hälfte auf einen anderen Host gespiegelt wird. Die kleinste Festplatte im Verbund bestimmt die Größe des Volume. Wenn Sie also lokal in jedem Ihrer drei ESXi Server 4 TByte Plattenplatz haben, bleiben für den VSA Storage von den 12 GByte insgesamt nur 3 GByte Platz übrig.
- Die ESXi Server müssen einen unterstützten Raid-Controller mit RAID 10 installiert haben und alle im selben Cluster sein.
- Es dürfen keine manuell erstellten vSwitches vorhanden sein, sondern nur der eine vSwitch, der während der Installation angelegt wurde, und keine zusätzlichen Portgruppen.
- Es müssen mindestens vier lokale Platten vorliegen (maximal 8), die alle vom selben Modell sein und die gleiche Performance und möglichst auch Kapazität haben müssen.
- Unterstützt werden nur Festplatten ab 7.500 U/Min. als SAS2 oder SATA mit maximal 2 TByte Platz, aber kein Mischbetrieb mit SAS- und SATA-Platten.
- Für die Hosts brauchen Sie mindestens 6 GByte RAM, empfohlen sind 24 GByte.
- Sie brauchen vier freie 1-GBit-Netzwerkanschlüsse und 9 bis 14 freie IP-Adressen in dem Subnetz.
- Die Hosts dürfen nicht in einem Cluster sein.
- Physisch brauchen Sie mindestens einen GBit-Netzwerkswitch, zwei sind empfohlen.
- Es gibt nur statische IP-Adressen im Subnetz des vCenter Servers und der Hosts, optional VLAN.
- Die ESXi Server dürfen noch keine VMs in ihrer Bestandsliste haben, auch nicht den vCenter Server.

- Die Hosts müssen CPUs aus derselben Familie besitzen und die gleiche Hardware haben.
- Adobe Flash und Internet Explorer 7 oder höher müssen auf dem vCenter Server installiert sein.
- Sie dürfen Ihren VMs nicht mehr Arbeitsspeicher geben, als der jeweilige Host physisch zur Verfügung stellt (Memory-Overcommitment wird nicht unterstützt).
- VSA unterstützt nur die aktuelle Version 5, keine früheren Versionen von vSphere.

Wie bereits in Kapitel 7, *Storage-Konfiguration* ausführlich beschrieben, gibt es für kleine, mittlere und große Umgebungen genügend einfach zu installierende Alternativen.

Ich empfehle Ihnen dringend, vor der Installation des VSA Managers ein Backup Ihres vCenter Servers zu machen. Haben Sie eine virtuelle Maschine dafür eingesetzt, machen Sie einen Snapshot, damit Sie die Installation ggf. rückgängig machen können. In den Unterlagen zu VSA von VMware wird zwar erklärt, wie man die Deinstallation durchführen kann, aber leider funktioniert das meistens nicht.

## VSA installieren

Der vSphere Storage Appliance Manager muss auf einem aktuellen vCenter Server installiert werden. Nach der Installation steht dort ein zusätzlicher Dienst mit dem Namen *VMware VSA Cluster Service* zur Verfügung. Dieser Manager kann nur eine VSA-Instanz für zwei oder drei Hosts zur Verfügung stellen, auch wenn in Ihrem Cluster mehr als drei Hosts vorhanden sind. Auch weitere, nachträglich hinzugekaufte Lizenzen können Sie nur unter einem anderen vCenter Server installieren – aber nicht auf der SuSE vCenter Appliance.

Die ausführbare Datei zur Installation heißt *VMware-vsamanager-en-<Version>-<Build-Nummer>.exe* und kann von der Webseite von VMware heruntergeladen werden. Diese Möglichkeit hat man ab der Lizenz *Essentials Plus*, aber auch in der Evaluierungsversion. VSA kann man aber auch für andere Lizenzmodelle einzeln erwerben.

Sie müssen lokaler Administrator sein, um die Software installieren zu können; ein Domänen-Adminkonto reicht nicht aus.

Im Assistenten für die Installation nicken Sie die EULA ab und klicken auf WEITER. Die Informationen über den vCenter Server werden angezeigt und müssen meist nur bestätigt werden. Bei den Ports für VSA sollten Sie tunlichst nichts ändern, sonst funktioniert es hinterher oder spätestens bei einem Update nicht mehr. Achten Sie bei einem Server 2003 auf die Firewall und ob die Ports 2181, 2888, 3888 und 2375 schon belegt sind. Das können Sie z. B. über die Kommandozeile mit dem Befehl *netstat -an* tun.

Sie können anschließend einen Lizenzschlüssel eingeben oder den Testmodus wählen. Klicken Sie auf die Schaltfläche zum Installieren der Anwendung. Kurze Zeit später sehen Sie das Fenster zum Beenden des Assistenten.

Wenn Sie sich anschließend mit dem vCenter Server verbinden, sehen Sie die zusätzliche Registerkarte VSA MANAGER unter dem Datencenter. Sehen Sie diese Karte nicht, versuchen Sie unter PLUG-INS den VSA Manager zu aktivieren. Über den zusätzlichen Kartenreiter können Sie die weitere Konfiguration für VSA mit einem Assistenten (VSA Installer) vornehmen (siehe Abbildung 11-7).

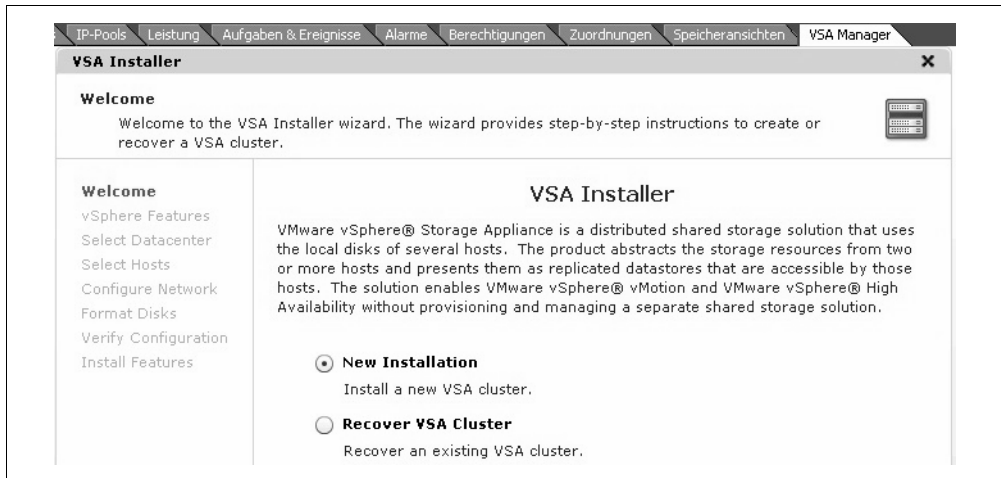


Abbildung 11-7: Installation eines VSA Storage

1. Nachdem Sie das Zertifikat installiert oder ignoriert haben, öffnet sich im vCenter Server ein eingebettetes Browserfenster.
2. Wählen Sie dort zunächst NEW INSTALLATION und klicken Sie auf die Schaltfläche NEXT.
3. Nach der Erklärung der Features wählen Sie ein Datacenter aus.
4. Im nächsten Fenster sehen Sie alle zum Datacenter gehörenden ESXi Server mit der Information, ob diese für VSA geeignet sind oder nicht. Hosts, bei denen rote Karos angezeigt werden, können nicht ausgewählt werden.
5. Wählen Sie zwei oder drei Hosts für Ihren Storage aus und klicken Sie auf NEXT.
6. Konfigurieren Sie im nächsten Schritt das Netzwerk der VSA-Umgebung (wie bei der Auflistung der Voraussetzungen beschrieben).
7. Auf der letzten Seite kann angegeben werden, wann die Festplatten formatiert werden sollen. Dabei bleibt die Installation des ESXi Servers unangetastet.

Anschließend konfiguriert der Installer das Netzwerk mit zwei Switches mit jeweils zwei Adaptern. Dann wird die Appliance auf jedem beteiligten Host zur Verfügung gestellt und so eingestellt, dass die Hälfte des Speicherplatzes als Replikat eines anderen Storage einem anderen Host zur Verfügung gestellt wird.

Danach wird aus den beteiligten ESXi Servern ein VSA-Cluster mit HA und vMotion erstellt und Sie müssen die geforderten IP-Adressen für den Clusterdienst, für den VSA Cluster, für den Verwaltungsserver, den Datenspeicher (NFS), das ESXi Funktionsnetzwerk und eine Backend-IP-Adresse angeben.

Klicken Sie anschließend auf YES, wird die Installation und Konfiguration gestartet. Nach einer Weile können Sie CLOSE anklicken und sich das Ergebnis im Kartenreiter VSA MANAGER ansehen.

Über HOME → DATENSPEICHER UND DATENSPEICHERCLUSTER können Sie sich die VSA-Storages von jedem Host ansehen. Gehen Sie auch auf die Registerkarte KONFIGURATION eines jeden Hosts und schauen Sie dort bei SPEICHER nach, ob der VSA Storage als *Online* markiert ist.

Jetzt können Sie Ihre virtuellen Maschinen in den neuen Storage legen oder erstellen.

# VMware vApp und Fernzugriff auf virtuelle Maschinen

Für den Zugriff auf eine virtuelle Maschine haben wir bisher nur den vSphere Client kennengelernt. Das ist auch die komfortabelste Lösung dafür. Für Benutzer, die auf den Desktop der VMs zugreifen sollen, möchte man aber vielleicht nicht dieses Programm installieren, da zu viele Informationen angezeigt werden. Ein weiterer Grund ist die Darstellung mit vielen Optionen, die der User nicht sehen oder ändern soll. Sicherlich kann man einiges über Rechte und Rollenvergabe erledigen, aber es gibt auch andere Möglichkeiten, sich den Desktop der VM zu holen, die nicht nur einige Geschwindigkeitsvorteile bieten.

Auf die wichtigsten alternativen Möglichkeiten werde ich im zweiten Teil dieses Kapitels eingehen.

Eine Funktion, die mit Version 4 von vSphere eingeführt wurde, ist die sogenannte *vApp*. Mit einer vApp können virtuelle Maschinen ähnlich wie in einem Ressourcenpool zusammengefasst und gemeinsam verwaltet werden. Auf einem einzelnen ESXi Host haben Sie diese Möglichkeit nicht – sie wird also über den vCenter Server bereitgestellt, der die Informationen in einer Datenbank speichert. Eine vApp kann eine oder mehrere virtuelle Maschinen enthalten, kann ein- und ausgeschaltet sowie geklont werden und läuft unabhängig von einem ESXi Host im Cluster.

Sie können eine vApp nutzen, um zum Beispiel mehrere voneinander abhängige virtuelle Maschinen mit einem Applikationsservice-Level zusammenzufassen. Wenn Sie eine Datenbankanwendung auf dem einen und die eigentlichen Daten auf einem anderen PC haben, können Sie diese in einer vApp zusammenfassen und Ressourcen sowie Regeln für die vApp erstellen.

Ähnlich wie bei einer einzelnen virtuellen Maschine kann eine gesamte vApp in das OVF-Format exportiert werden, um z.B. eine Sicherung mit allen Metadaten davon zu erstellen oder die gesamte vApp inklusive aller Einstellungen und virtuellen Maschinen anderen als Demoversion zur Verfügung zu stellen.

Eine vApp wird über den vSphere Client sowohl in der Ansicht HOSTS UND CLUSTER als auch in der Ansicht VMS UND VORLAGEN angezeigt. Die Ansichten aller Registerkarten sind dabei gleich: Die Übersichtsseite mit dem aktuellen Status und die relevanten zusammengefassten Informationen geben z. B. alle genutzten Storages der VMs wieder.



Nur wenn Sie einen Cluster mit aktiviertem DRS haben, lässt sich eine vApp erstellen, sonst ist der Eintrag zur Erstellung ausgegraut. Haben Sie bereits eine vApp und deaktivieren DRS, bekommen Sie eine Meldung, die Ihnen mitteilt, dass alle Ressourcenpools verschwinden. Von vApp ist dabei zwar nicht die Rede, aber es wird ebenfalls aufgelöst, und die Maschinen befinden sich wieder im Cluster.

## Eine vApp erstellen

Über das Kontextmenü auf dem Cluster oder über das Menü DATEI → NEU → vAPP können Sie eine neue vApp erstellen. Das geht übrigens auch im Ressourcenpool, je nach Konfiguration in einem Ordner und auf einem Host und auch in einer vApp.

Geben Sie einen treffenden Namen für diese Zusammenfassung an und teilen Sie ihr auf der Seite RESSOURCENZUTEILUNG CPU- und Arbeitsspeicherressourcen zu. Klicken Sie auf BEENDEN, um sie zu erstellen.

Jetzt können Sie in diesem Objekt neue virtuelle Maschinen erstellen oder auch bereits konfigurierte mit der Maus (per Drag-and-Drop) dort hineinschieben. Falls Sie dabei eine Warnmeldung erhalten (siehe Abbildung 12-1), sollten Sie die Ressourcen nochmals anpassen.

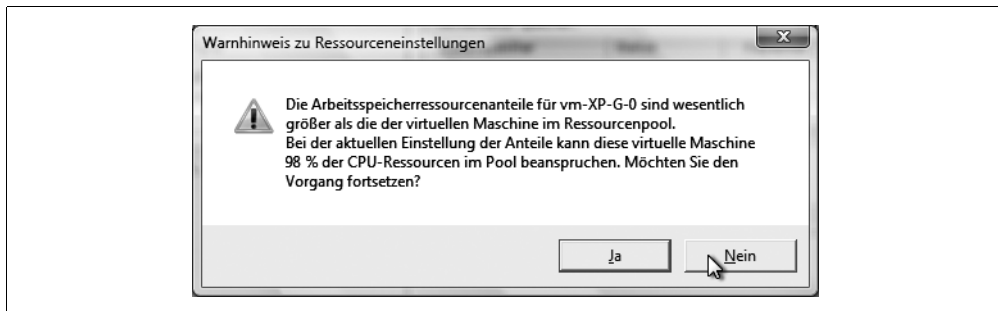


Abbildung 12-1: Warnhinweis zu den Ressourceneinstellungen

Nach der Erstellung einer vApp haben Sie einige Einstellungsmöglichkeiten, die vorher nicht auswählbar sind – ähnlich wie beim Erzeugen eines Clusters.

## vApp-Einstellungen

Jetzt können mehrere Aspekte der vApp bearbeitet und konfiguriert werden, z. B. Startreihenfolge, Ressourcen und benutzerdefinierte Eigenschaften (siehe Abbildung 12-2).



- RESSOURCEN: Wie bei der virtuellen Maschine werden hier CPU-Zeit und RAM verteilt. Das Maximale, das vom Cluster angeboten wird, wird dabei angezeigt.
- EIGENSCHAFTEN: Dieses Fenster ist zunächst leer. Erst wenn benutzerdefinierte Felder unter ERWEITERT festgelegt wurden, erscheint hier etwas.

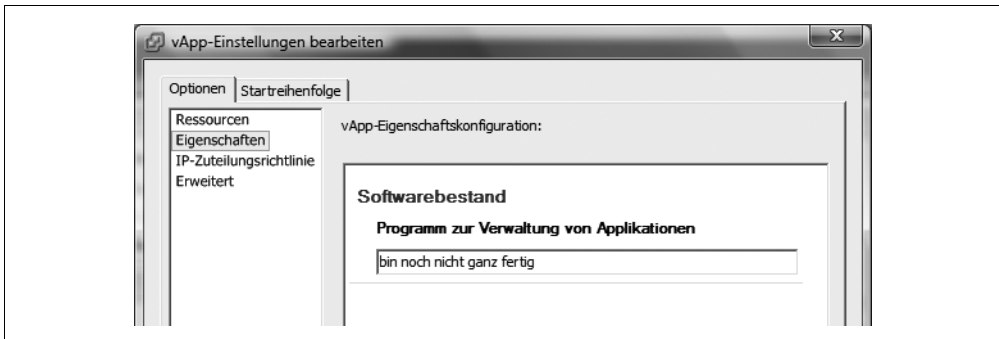


Abbildung 12-2: Konfiguration der Eigenschaften von vApp

- IP-ZUTEILUNGSRICHTLINIE: Hier kann ebenfalls zunächst nichts ausgewählt werden.
- ERWEITERT: Hier können zunächst Informationen zur vApp eingetragen werden. Sind die Felder XXX-URL: ausgefüllt, wird über den Link ANZEIGEN diese Seite mit dem Standardbrowser geöffnet.
- ERWEITERT → EIGENSCHAFTEN ist für benutzerdefinierte Zusatzinformationen gedacht.
- ERWEITERT → IP-ZUTEILUNG: Hier wird zunächst nur eingestellt, ob an der Portgruppe der beteiligten VMs ein DHCP-Server zur Verfügung steht oder die OVF-Umgebung IP-Informationen verteilen soll. Dabei kann IPv4, IPv6 oder beides gewählt werden. Wenn Sie hier OVF-UMGEBUNG auswählen, können Sie hinterher bei IP-ZUTEILUNGSRICHTLINIE zwischen festen oder vom vCenter Server zugewiesenen Informationen wählen. Haben Sie OVF und DHCP angeklickt, haben Sie drei Auswahlmöglichkeiten auf der Seite.



Beachten Sie, dass die vApp-Optionen in den Einstellungen der VM, Register OPTIONEN auf AKTIVIEREN gesetzt sein muss, damit das funktioniert. Diese Auswahl haben Sie bei der VM erst, wenn diese in einem Cluster über den vCenter Server gemanagt wird.

- STARTREIHENFOLGE: Ähnlich wie bei den VMs auf einem einzelnen Host kann man über die Reihenfolge Verzögerungen usw. beim Starten und Herunterfahren der untergeordneten Objekte erreichen. Dabei können auch Gruppen zusammengefasst werden.



Eine Festlegung der Startreihenfolge für alle Maschinen unter dem vCenter Server gibt es leider nicht. Lediglich über die Priorisierung bei HA kann man bedingt etwas Ähnliches erreichen.

## IP-Pools konfigurieren

Damit die VMs in der vApp IP-Adressinformationen über den vCenter Server erhalten, kann ein IP-Pool angelegt werden. Dazu wählen Sie auf der Seite VAPP-EINSTELLUNGEN BEARBEITEN unter OPTIONEN den Punkt ERWEITERT und dann IP-ZUTEILUNG. Dort legen Sie zunächst das Schema und die Protokollversion fest (siehe Abbildung 12-3).

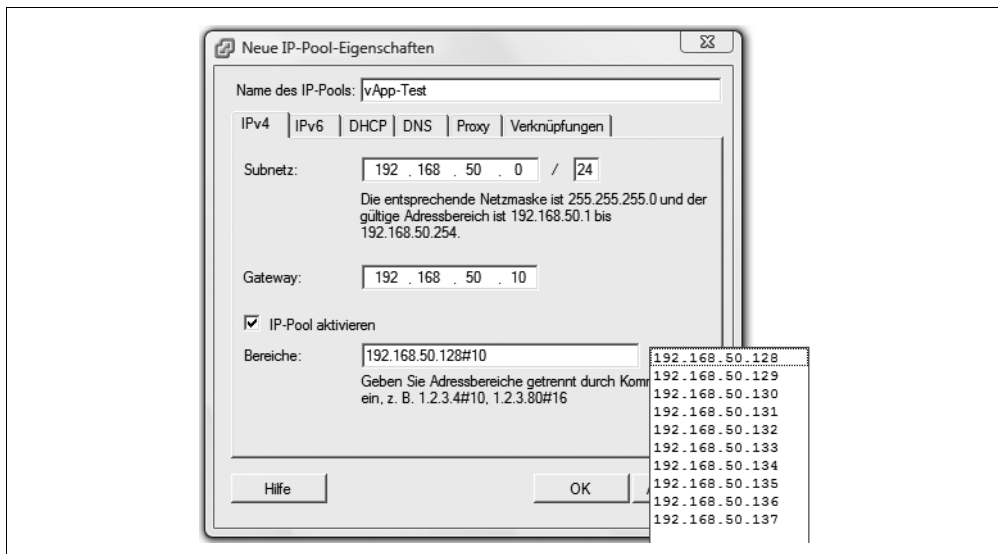


Abbildung 12-3: IP-Pool-Zuweisungen

Die eigentliche Festlegung eines IP-Pools mit den dazugehörigen Optionen erledigt man über das Datacenter.

Auf der Registerkarte IP-POOLS können DHCP-Optionen und -Bereiche entfernt, bearbeitet und hinzugefügt werden. Dazu klicken Sie auf den Link HINZUFÜGEN auf der Seite oben links.

Die Angabe des IP-Bereichs ist ein wenig gewöhnungsbedürftig. Die Adressbereiche werden angegeben, indem man die erste zu verteilende IP-Adresse angibt, danach ein # setzt und die Anzahl der zu vergebenen Adressen anfügt. Nach einem Komma kann man weitere Bereiche oder auch einzelne Adressen angeben.

Die Einstellung /24, die als Standard dort erscheint, legt die Subnetzmaske fest, hierfür also 255.255.255.0, denn das sind binär gesehen 24 Bit, und es bleiben 8 Bit für die IP-

Adressen übrig (von 1 bis 254). Sie können anhand der Subnetzmaske auch größere oder kleinere Netze einrichten, indem Sie die Zahl verringern oder erhöhen. Die anderen Einstellungen entsprechen der normalen Funktionsweise eines DHCP-Servers.

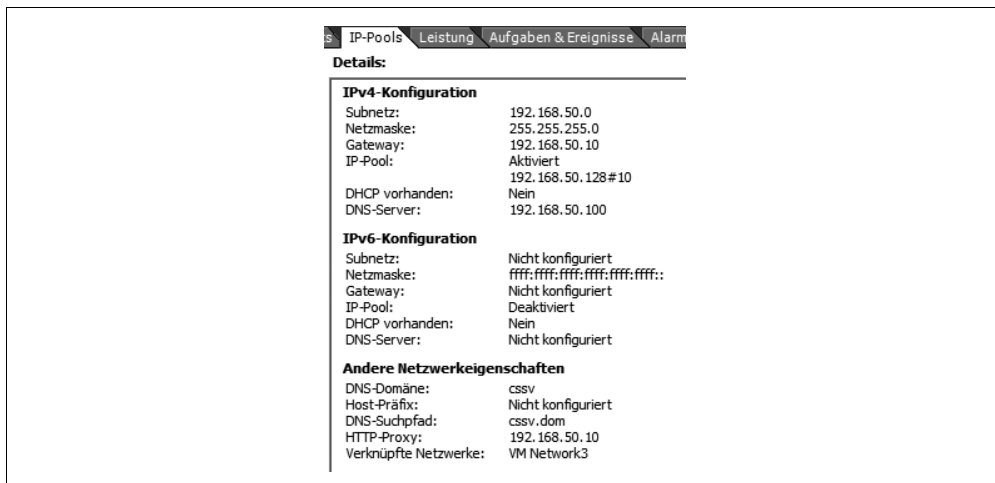


Abbildung 12-4: IP-Konfiguration für die vApp

Einem IP-Pool kann mindestens ein Netzwerkport der virtuellen Maschinen zugewiesen werden, die im Register VERKNÜPFUNGEN aufgelistet sind (siehe Abbildung 12-4). Umgekehrt kann einer Netzwerkportgruppe nur ein IP-Pool auf einmal zugewiesen werden.

## vServices für vApps

vServices sind eine Art abhängige Dienste oder Funktionserweiterungen für VMs und vApps, die meist von VMware oder Drittanbietern als Appliance oder fertige vApp angeboten werden. Bei Computern im Netzwerk kann beispielsweise ein DHCP-Server so eine Abhängigkeit darstellen.

Über das SDK von VMware können eigene vServices programmiert werden. Weiterhin gibt es im Portfolio auf dem vSphere Marketplace einige fertige Lösungen – schauen Sie sich da mal um, es lohnt sich.

Die Konfiguration von vServices für VMs und vApps kann nur im ausgeschalteten Zustand durchgeführt werden. Auf der Registerkarte vServices können anschließend die Abhängigkeiten der vApp oder VM zu einem oder mehreren Diensten hergestellt werden. Gehen Sie dazu wie folgt vor:

1. Klicken Sie auf die gewünschte, ausgeschaltete vApp (alle VMs darin müssen ausgeschaltet sein).
2. Aus dem Kontextmenü über die rechte Maustaste wählen Sie EINSTELLUNGEN BEARBEITEN aus.

3. Wählen Sie die Registerkarte `VSERVICES` und klicken Sie auf `HINZUFÜGEN`.
4. Suchen Sie sich über den Assistenten einen Dienst aus und klicken Sie auf `WEITER`.
5. Wählen Sie einen aussagekräftigen Namen und geben Sie möglichst eine Beschreibung dazu ein. Wenn eine Abhängigkeit von diesem Dienst erforderlich ist, klicken Sie die dafür vorgesehene Schaltfläche an. Sie können diese Informationen aber auch nachträglich bearbeiten und sie erscheinen dann auf einer zusätzlichen Registerkarte bei der vApp.
6. Ihre Eingaben werden anschließend überprüft. Klicken Sie zum Abschluss auf `BEENDEN`.

Fertige vApps können Sie auch über das Kontextmenü mithilfe eines Assistenten klonen oder komplett mit allen Abhängigkeiten im OVF-Format exportieren.

## vApps löschen

Seien Sie beim Löschen von vApps vorsichtig! Lesen Sie den Hinweis, der beim Löschen erscheint:

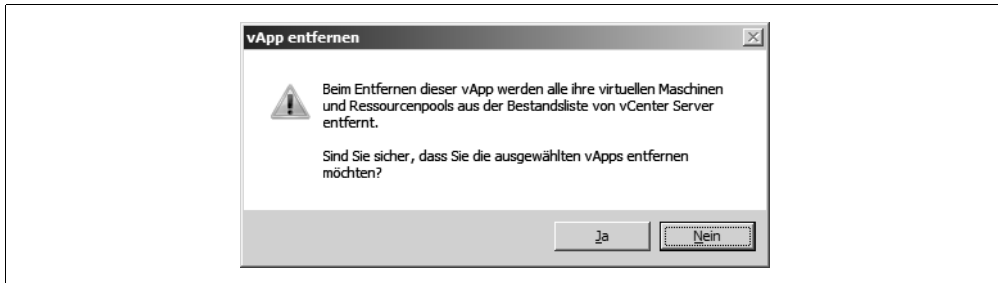


Abbildung 12-5: Warnmeldung beim Entfernen eines vApp

Die enthaltenen virtuellen Maschinen werden nicht nur aus der Bestandsliste entfernt, sondern tatsächlich alle Dateien der VMs gelöscht, daher die Warnmeldung (siehe Abbildung 12-5). Wenn Sie Ihre VMs behalten wollen, sollten Sie diese vorher aus dem Pool herausnehmen und dann erst die leere vApp löschen.

## VMware WebAccess

Der Zugriff auf die Informationen der virtuellen Maschine auf den vCenter Server ohne Installation einer zusätzlichen Software – einfach nur über einen Browser (vorzugsweise der Internet Explorer) von jeder Stelle mit Netzwerkzugriff heißt VMware WebAccess. Beim ESXi Server steht diese Funktion leider nicht zur Verfügung. Sie können aber das Programm *vmware-vmrc.exe* dafür nutzen, das weiter unten in diesem Kapitel behandelt wird.

Auf dem vCenter Server werden für den Zugriff per Browser das Programm *vSphere Web Client (Server)* installiert und der dazugehörige Dienst normalerweise automatisch gestar-

tet. Sollte er nicht laufen, dann überprüfen Sie zuerst, ob der VIRTUAL CENTER SERVER-DIENST läuft (der Dienst wurde nicht auf vCenter Server umbenannt). Der Webdienst ist vom VIRTUAL CENTER SERVER-DIENST abhängig. Mit diesem Tool haben Sie auch die (eingeschränkte) Möglichkeit, die ESXi Hosts zu verwalten.

Folgende Browser werden unterstützt und sind für die Verwendung von VMware für die Remote-Console (*vmrc*) zertifiziert:

- Microsofts Internet Explorer ab Version 7
- Mozilla Firefox ab Version 3.6 für Windows und Linux
- Adobe Flash Player Version 10.1 oder neuer muss installiert sein

Sollten Sie bei der Anmeldung am vCenter Server eine Fehlermeldung wie in Abbildung 12-6 dargestellt bekommen, wurde WebAccess noch nicht korrekt konfiguriert und der Server noch nicht als Web Client Server registriert. Melden Sie sich dann am Server lokal unter <https://<IP-Adresse oder Name>:9443/admin-app/> an und registrieren Sie den Server.

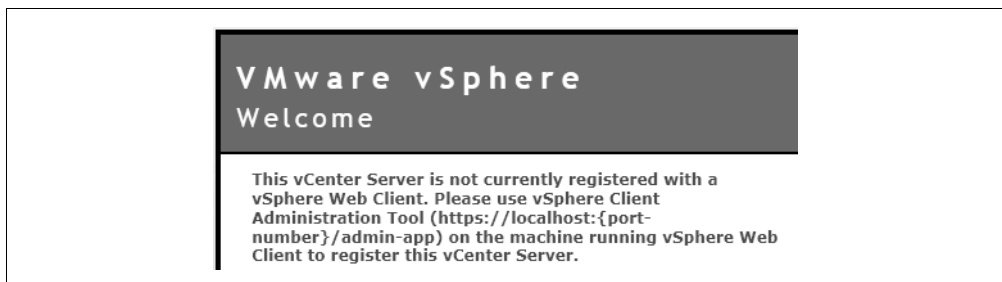


Abbildung 12-6: Fehlermeldung bei WebAccess

Leider ist die Anzeige nicht so performant, wie man es sich wünschen würde! Sehr häufig sieht man den Hinweis *Loading*, dann kommt lange nichts und erst dann endlich die gewünschte Anzeige.

Nach der Anmeldung am vCenter Server (siehe Abbildung 12-7) wird ein zweigeteiltes Fenster angezeigt, wobei auf der linken Seite die Bestandsliste und auf der rechten die Details zum links Ausgewählten angezeigt werden.



Abbildung 12-7: Anmeldung bei WebAccess

Einen direkten Zugriff auf die Seite bekommt man über die Eingabe im Browser, zum Beispiel von <https://vcs.cssv.dom:9443/vsphere-client/>.



VMware WebAccess ist auf ESXi Hosts nicht installiert und deshalb auch nicht möglich. Die VMware Remote-Console, die im nächsten Abschnitt besprochen wird, funktioniert allerdings.



VMware WebAccess erfordert die Zulassung von Pop-ups. Stellen Sie Ihren Browser dementsprechend ein.

Die Konsole von WebAccess bietet einen Remote-MKS (Mouse-Keybord-Screen, Maus-Tastatur-Bildschirm) für die virtuellen Maschinen. Sie können mit dem auf einer virtuellen Maschine ausgeführten Gastbetriebssystem kommunizieren und eine Remote-Verbindung mit der Maus, der Tastatur und dem Bildschirm der virtuellen Maschine herstellen. Dafür muss ein Plugin (*VMware Remote-Console*) installiert werden, das es leider nur für den IE und Mozilla Firefox gibt (siehe Abbildung 12-8).

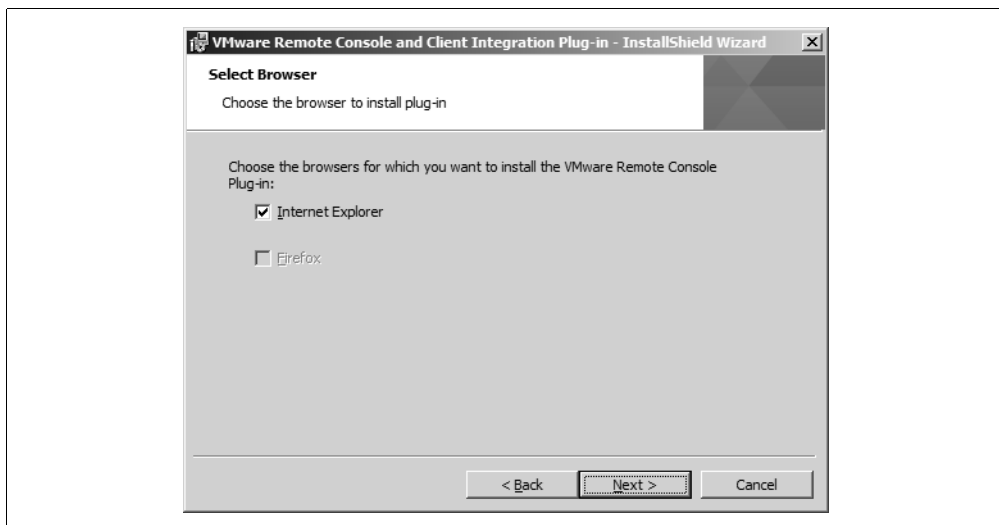


Abbildung 12-8: Meldung Remote-Console Plug-In

1. Klicken Sie in der Warnmeldung auf PLUG-IN INSTALLIEREN. Das Fenster DATEI-DOWNLOAD – SICHERHEITSWARNUNG wird angezeigt und Sie werden gefragt, ob Sie die Datei ausführen oder speichern möchten.
2. Klicken Sie auf AUSFÜHREN und im Fenster INTERNET EXPLORER – SICHERHEITSWARNUNG nochmals auf AUSFÜHREN.
3. Klicken Sie auf der Begrüßungsseite auf INSTALLIEREN (dafür darf der Browser nicht aktiv sein).

4. Nach Abschluss der Installation klicken Sie auf BEENDEN. Das VMware Remote-Console Plug-In für Internet Explorer ist jetzt installiert.
5. Starten Sie den Browser neu mit der gewünschten URL.
6. Das Plugin wird jetzt mit gestartet, eventuell müssen Sie das noch erlauben.
7. Nach dem Auswählen der Registerkarte ÜBERSICHT einer VM klicken Sie auf den schwarzen Bildschirm oder den Link KONSOLE STARTEN, dann wird in einem neuen Fenster der Desktop der virtuellen Maschine angezeigt.

In der Remote-Konsole können weder Änderungen und Informationen zur VM erreicht noch der Zustand des Betriebssystems beeinflusst werden. Sie können lediglich die Tastenkombination Strg+Alt+Entf an die VM senden oder den Vollbildschirm aktivieren (siehe Abbildung 12-9).

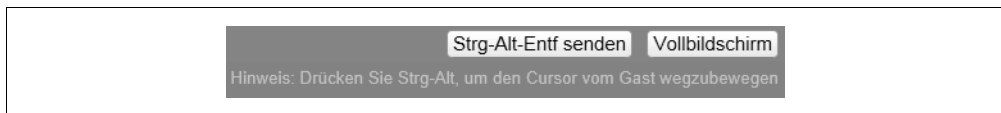


Abbildung 12-9: Menü der Remote-Konsole

Das Verbinden eines lokalen CD- oder DVD-Laufwerks sowie der Zugriff auf ein ISO-Image müsste also im ersten Fenster erfolgen (siehe Abbildung 12-10).



Wenn Sie die Hardwareversion der VM ändern möchten oder eine ältere VM importiert haben, müssen Sie die VM ausschalten und im Abschnitt *Status* der VM nur auf *Virtuelle Maschine aktualisieren* klicken. Vergessen Sie nicht, die aktuelle Version der VMware Tools möglichst vor dem Ausschalten zu installieren.

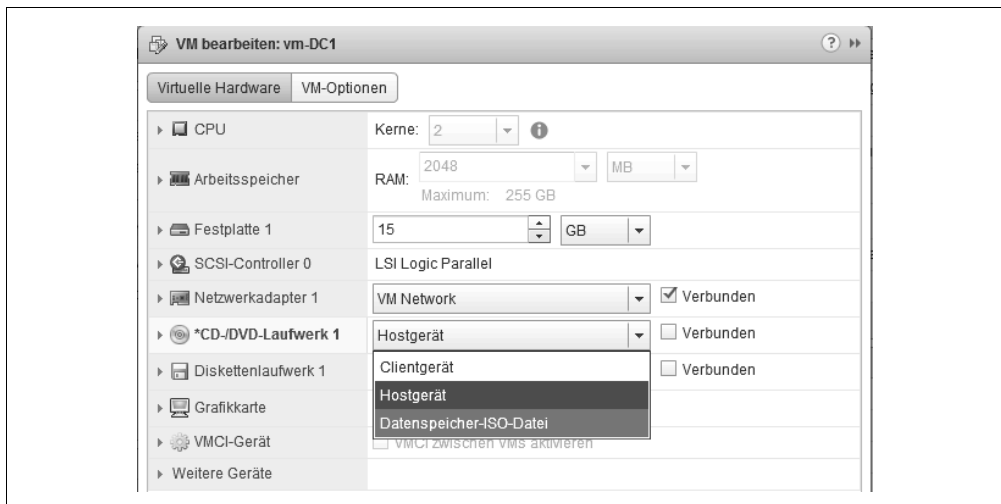


Abbildung 12-10: Laufwerke verbinden

In der rechten Hälfte des Fensters sieht man die verbundenen und nichtverbundenen Geräte (siehe Abbildung 12-11).

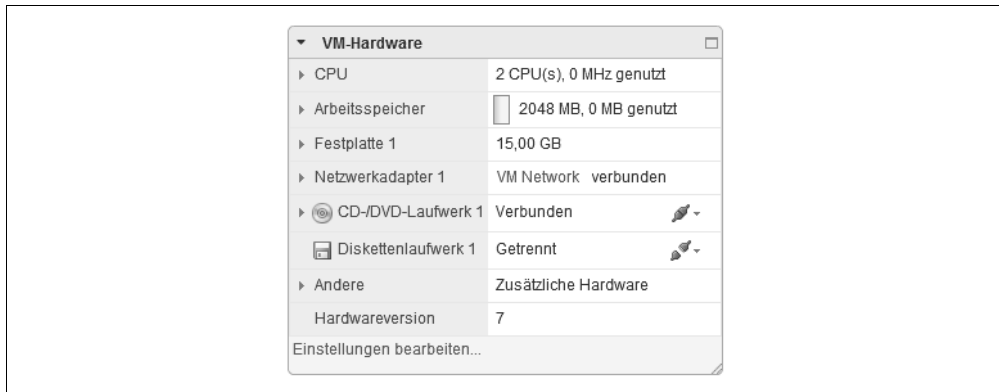


Abbildung 12-11: Hier ist das optische Laufwerk verbunden, das Floppy-Laufwerk getrennt.

Wie in Abbildung 12-12 zu sehen ist, ist es über WebAccess ebenfalls möglich, schon bestehende VMs auf einem Datastore zur Bestandsliste eines ESXi Servers oder vCenter Servers hinzuzufügen.

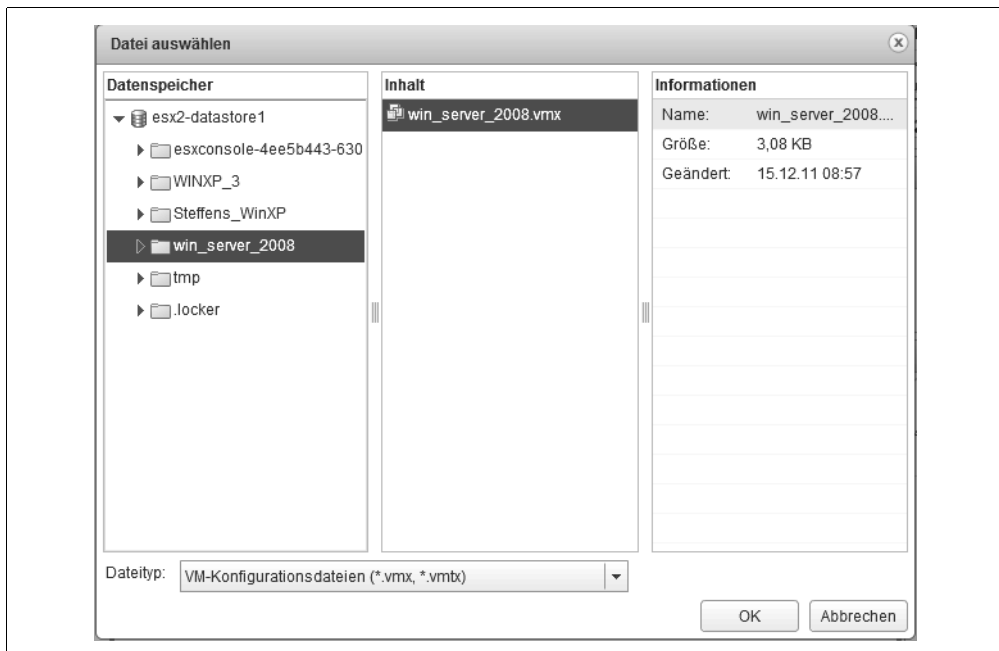


Abbildung 12-12: Hinzufügen einer vorhandenen virtuellen Maschine über deren vmx-Datei in WebAccess



1. Klicken Sie dazu im Fenster oben links auf das Symbol für den Datenspeicher, erweitern Sie die Anzeige und wählen Sie anschließend den gewünschten Storage aus.
2. Über das Kontextmenü wählen Sie dann BESTANDSLISTE → VM REGISTRIEREN aus.
3. Wählen Sie den Ordner der gewünschten virtuellen Maschine und anschließend im mittleren Teil des Fensters die Konfigurationsdatei der VM.
4. Bestätigen Sie die Registrierung, indem sie auf die Schaltfläche OK klicken.
5. Geben Sie ggf. einen neuen Namen an, unter dem die VM in der Bestandsliste angezeigt werden soll.
6. Beantworten Sie anschließend die weiteren Fragen des Assistenten und klicken Sie schließlich auf BEENDEN.
7. Wählen Sie das Symbol für die VMs und Vorlagen – dort müsste jetzt Ihre VM mit dem gewählten Namen erscheinen.

## Verknüpfung für die VMware Remote Console

Nachdem Sie das Plugin für die VMware Remote Console installiert haben, können Sie eine Desktopverknüpfung erstellen, über die die Remote-Konsole gestartet und eine Verbindung zur virtuellen Maschine hergestellt wird.

Sie müssen das VMware Remote Console Plug-In für Ihren Browser vorher installiert haben.

1. Wählen Sie im Bestandslistenfenster die virtuelle Maschine aus, von der aus eine Desktopverknüpfung erstellt werden soll.
2. Klicken Sie unter VM-HARDWARE auf EINSTELLUNGEN BEARBEITEN.
3. Wählen Sie die Registerkarte VM-OPTIONEN und anschließend OPTIONEN DER VMWARE-REMOTEKONSOLE.
4. Stellen Sie die gewünschten Optionen für die Verbindung ein (siehe Abbildung 12-13) und klicken sie auf OK.
5. Klicken Sie auf der Registerkarte ÜBERSICHT auf die Verknüpfung KONSOLE STARTEN.
6. Klicken Sie in die Anzeige der URL und kopieren Sie sich den Inhalt in die Zwischenablage.
7. Erstellen Sie eine neue Verknüpfung auf Ihrem Desktop und fügen Sie die kopierte URL ein. Geben Sie der Verknüpfung einen aussagekräftigen Namen.
8. Die Verknüpfung wird auf dem Desktop erstellt.
9. Starten Sie die Remote-Sitzung über die Verknüpfung.

Sie können die Desktopverknüpfung für den schnellen Zugriff auf die virtuelle Maschine benutzen.

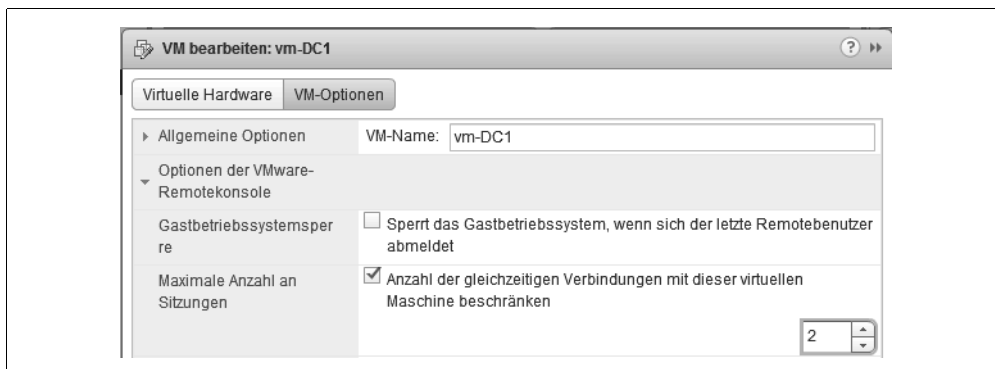


Abbildung 12-13: VM-Optionen für die Verknüpfung einrichten



Ist die virtuelle Maschine ausgeschaltet oder befindet sich im Suspend-Modus, wird sie nicht automatisch gestartet. Sie sehen dann nur einen schwarzen Bildschirm.

## Zugriffsrechte über WebAccess

Wenn Sie über den vCenter Server auf WebAccess zugreifen, müssen dort die jeweiligen Rechte gesetzt und die User bzw. Gruppen angelegt sein.

Der Zugriff auf die Einstellungen und Optionen einer virtuellen Maschine ist von den Benutzerberechtigungen für den Zugriff auf die Konfigurationsdatei der virtuellen Maschine abhängig. Die Berechtigungen legen fest, ob Sie eine virtuelle Maschine durchsuchen, mit ihr interagieren, sie konfigurieren und/oder administrieren können, und auch, ob Sie nur eine, mehrere oder alle VMs sehen können.

Der Zugriff und die Konfiguration des ESXi Servers sind auch möglich. Der vCenter Server kann dagegen auch mit administrativen Rechten nicht geändert werden.

Nutzen Sie am besten die jeweiligen Rollen, die sowohl auf dem ESXi als auch auf dem vCenter Server zur Verfügung stehen. Sehen Sie im Kapitel über die Rollen auf dem ESXi und vCenter Server nach den Möglichkeiten und Einschränkungen nochmals nach, wenn Sie unsicher sind. Probieren Sie die Einstellungen erst selber aus, bevor Sie z.B. einem User eine Webverknüpfung auf seinen Desktop legen.

## Tastenkombinationen für WebAccess

Sie haben die Möglichkeit, den Remote-Bildschirm in den Vollbildmodus zu bringen, indem Sie die Tastenkombination STRG+ALT+ENTER drücken. Um in den Fenstermodus zurückzukehren, drücken Sie erneut STRG+ALT+ENTER. Die Windows-Anmeldetastenfunktion STRG+ALT+ENTF sollten Sie vermeiden, weil das durch das Betriebssystem Ihres

Rechners abgefangen wird. Nehmen Sie statt STRG+ALT+ENTF lieber STRG+ALT+EINFG oder klicken Sie mit der Maus im Menü auf die Schaltfläche STRG+ALT+ENTF SENDEN.

## Fehlerbehebung

Oben habe ich schon etwas über den automatischen Start des Dienstes (vCenter Server) geschrieben. Der Fehlercode ist dabei üblicherweise 503 Dienst nicht verfügbar. Es können aber noch weitere Fehlfunktionen auftreten, die ich hier kurz erwähne:

1. Falls Sie mit dem Internet Explorer arbeiten, sollten Sie immer zunächst alle IE-Sitzungen beenden und es anschließend erneut versuchen – das hilft oft.
2. Um die Remote Console zu bekommen, muss ein Plugin installiert sein. Haben Sie es installiert, muss ggf. noch eine Bestätigung beim erneuten Aufruf des Browsers erfolgen. Es kann auch sein, dass Sie eine ältere Version haben (vor 2.5.0). Wenn dem so ist, installieren Sie das Plugin einfach erneut, nachdem Sie die ältere Version unter SYSTEMSTEUERUNG → SOFTWARE deinstalliert haben. Die erneute Installation erfolgt wie vorher: Gehen Sie im Browserfenster auf die virtuelle Maschine, klicken Sie auf den Link KONSOLE STARTEN und installieren Sie wieder das Plugin.
3. Falls Sie mit Firefox arbeiten, erkennen Sie die ältere Version unter EXTRAS → ADD-ONS. Ist die Version älter als 3.0, sollten Sie die neuere Version installieren. Auch wenn die Installation beim ersten Mal fehlgeschlagen ist, empfehle ich die Erneuerung.
4. Unter Linux ist der Firefox-Browser häufig schon bei der Installation des Betriebssystems dabei. Falls bei Ihnen Fehler auftreten, sollten Sie die neueste Version herunterladen und installieren.

## Die VMware Remote Console manuell einrichten

Eine etwas versteckte Möglichkeit für den Zugriff auf den Desktop der virtuellen Maschine, über die es auch keinerlei Dokumentation von VMware gibt, ist das Programm *vmware-vmrc.exe*, mit dem die VMware Remote Console (VMRC) gestartet wird. Das Programm wird sowohl bei Linux als auch bei Windows zusammen mit dem vSphere Client installiert. Unter Windows finden Sie das Programm unter *C:\Programme\VMware\Infrastructure\Virtual Infrastructure Client\5.0*, bei neueren Windows-Versionen unter *C:\Program Files (x86)\Common Files\VMware\VMware VMRC Plug-in\<Browser>*, und bei Linux hängt es von der jeweiligen Distribution und ggf. auch vom eingesetzten Browser ab. Durchsuchen Sie am besten Ihr System nach der Datei (ohne *.exe*).

Die ausführbare Datei *vmware-vmrc.exe* müssen Sie mit einigen Parametern aufrufen, damit Sie Ihre VM erreichen können. Ohne Parameter gibt es nur das leere VMRC-Fenster und eine Fehlermeldung über fehlende Angaben. Die anzugebenden Parameter sind für Linux und Windows gleich und setzen sich üblicherweise aus der Angabe von Hosts,

Username und Passwort (optional) sowie der gewünschten virtuellen Maschine zusammen. Geben Sie das Passwort und den Usernamen nicht mit an, werden sie vor der Verbindung abgefragt. Bei der virtuellen Maschine gibt es zwei Möglichkeiten: Entweder geben Sie die ID der VM oder den Pfad zur \*.vmx-Datei an. Die ID der Maschine ist nur schwer über den ESXi Server herauszubekommen, der Pfad zur Konfigurationsdatei ist einfach beim Datenspeicherbrowser zu sehen.



Über die Kommandozeile des ESXi Servers können Sie für die MOID (Managed Object ID) den Befehl `vim-cmd vmsvc/getallvms` nutzen. Dieser zeigt Ihnen zu jeder registrierten VM die zugehörige VMID an. Alternativ können Sie das Tool *RVTools* einsetzen, das in Kapitel 18 beschrieben wird.

In Tabelle 12-1 sind die wichtigsten Parameter mit Beispiel und Funktion aufgelistet:

*Tabelle 12-1: Wichtige Parameter für VMware Remote Console*

| Parameter        | Beispiel                              | Funktion                                                |
|------------------|---------------------------------------|---------------------------------------------------------|
| -h <hostname>    | -h esx4 oder -h 192.168.50.54         | Angabe des ESXi Servers, auf dem sich die VM befindet   |
| -u <username>    | -u Administrator oder -u goepel       | Name des Users mit Zugriffsrechten auf die Maschine     |
| -p <passwort>    | -p Geheim2010                         | Passwort des Benutzers im Klartext (optional)           |
| -M <moid>        | -M 4711                               | Die sogenannte »Managed Object ID« der VM               |
| -d <path to vmx> | -d "[datastore1] vm-XP-G/vm-XP-G.vmx" | Angabe des Speicherortes und des Pfades zur *.vmx-Datei |
| -X               | -X                                    | Vollbildschirm der VM                                   |

Gehen wir davon aus, dass der Speicherort der Datei *vmware-vmrc.exe* Standard ist, würde der Aufruf mit allen Parametern unter Windows folgendermaßen aussehen:

```
"C:\Programme\VMware\Infrastructure\Virtual Infrastructure Client\5.0\vmware-vmrc.exe" -h 192.168.50.54 -u root -p Geheim2010 -X -d "[datastore1] vm-1/vm-1.vmx"
```

Lassen Sie den Benutzer und das Passwort weg, dann bekommen Sie eine Anmeldemaske ähnlich wie bei WebAccess. Der Aufruf könnte dann so aussehen:

```
vmware-vmrc.exe" -h 192.168.50.54 -d "[datastore1] vm-1/vm-1.vmx"
```

Damit haben Sie eine einfache Möglichkeit, das fehlende WebAccess des ESXi Servers durch einen anderen Zugriff zu nutzen. Der Zugriff über den vCenter Server funktioniert so leider nicht – aber dort haben Sie ja die Möglichkeit, WebAccess zu nutzen.

Wollen Sie den Zugriff für andere User einrichten, müssen Sie den vSphere Client nicht installieren. Kopieren Sie einfach den gesamten Inhalt des Verzeichnisses, z.B. *C:\Program Files (x86)\Common Files\VMware\VMware VMRC Plug-in\Internet Explorer* auf

eine Netzwerkfreigabe und erstellen Sie für den jeweiligen Benutzer eine Verknüpfung zu der ausführbaren Datei (*vmware-vmrc.exe*) mit den gewünschten Parametern.

Beim Neustart des Betriebssystems der VM bleibt das Fenster geöffnet, so dass man sogar in das BIOS wechseln könnte. Beim Herunterfahren und Ausschalten wird das Fenster automatisch geschlossen. Ist die Maschine ausgeschaltet, wird zwar eine Verbindung aufgebaut, aber das Betriebssystem der VM nicht automatisch gestartet. Falls diese Maschine immer laufen soll, können Sie eine Alarmaktion dafür einrichten (siehe Kapitel 15).

Über das Menü am oberen Rand des Fensters haben Sie die Möglichkeit, über DEVICES ein CD/DVD- oder Floppy-Laufwerk mit einem Datenträger zu verbinden und die Netzwerkkarte zu konfigurieren. Verbundene Geräte werden dann am unteren Rand des Fensters angezeigt, wobei ein abgeblendetes Symbol bedeutet, dass das Gerät nicht verbunden ist. Neue Geräte können nicht hinzugefügt und die Einstellungen der VM nicht bearbeitet werden. Fügen Sie über den ESXi Host oder den vCenter Server ein Gerät hinzu, z. B. eine neue Festplatte, wird es am unteren Rand sofort angezeigt (siehe Abbildung 12-14).

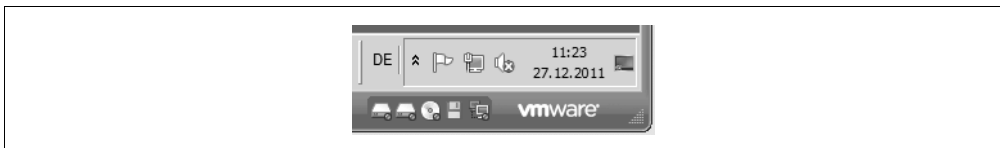


Abbildung 12-14: Geräte der VM bei *vmware-vmrc.exe*

Das Diskettenlaufwerk ist in der Abbildung nicht verbunden, deshalb wird es abgeblendet dargestellt.

Über die Schaltfläche VMWARE REMOTE CONSOLE am oberen Rand des Fensters haben Sie folgende Optionen:

- ABOUT VMWARE REMOTE CONSOLE: Zeigt Produktinformationen und erweiterte Informationen zu Rechner, der die Verbindung aufgebaut hat.
- SEND CTRL+ALT+DEL: Sendet die Tastenkombination Strg+Alt+Entf an das Betriebssystem, z. B. um sich anzumelden, den Computer zu sperren und so weiter.
- RESTART GUEST: Gibt dem Benutzer die Möglichkeit, das Gastbetriebssystem neu zu starten – das Fenster wird dabei nicht geschlossen.
- SUSPEND AND EXIT: Minimiert das Fenster, fährt die VM in den Suspend-Modus und schließt anschließend das Fenster. Die VM wird aus dem Suspend-Modus nicht automatisch herausgeholt und erst gestartet, wenn die Verknüpfung zur VM erneut geladen wird.
- SHUTDOWN GUEST AND EXIT: Gibt dem Benutzer die Möglichkeit, das Gastbetriebssystem herunterzufahren – das Fenster wird dabei geschlossen.

- DISCONNECT AND EXIT: Schließt das Fenster – die VM läuft weiter.

VMware-VMRC nutzt nicht das herkömmliche RDP-Protokoll. Es ist daher auch möglich, Zugriff auf die Oberfläche einer VM zu bekommen, die keine Netzwerkkarte hat oder sich in einem anderen Subnetz befindet.

## Remote Desktop Protocol

Über das Remote Desktop Protocol (RDP) auf einen entfernten Rechner zuzugreifen, ist keine Besonderheit mehr. Diese Technologie, die schon bei den mittlerweile veralteten Betriebssystemen von Microsoft Standard war, ist in Unternehmen heute sehr häufig anzutreffen. Warum sollte also darüber in diesem Buch geschrieben werden? Weil man damit einige Funktionen erreichen kann, die unter vSphere5 nicht laufen.

## Mehrere Monitore

Wie bereits ausführlich in Kapitel 4 beschrieben, kann man in den Einstellungen der virtuellen Maschine mehrere Monitore auswählen. Diese Option wird nur leider nicht für den Aufruf der VM über irgendeine Möglichkeit dargestellt.

Wenn Sie RDP verwenden, können Sie unabhängig davon, ob es sich um eine virtuelle oder physische Maschine handelt, den Parameter `/span` angeben. Rufen Sie also das Programm `mstsc.exe` mit dieser Option auf, und der Desktop des Zielrechners wird über alle angeschlossenen Bildschirme »gespannt«.

## USB in der VM

Bei einer virtuellen Maschine der Version 8 können Sie einen USB-Hostcontroller zur Hardwareliste hinzufügen. Innerhalb des Betriebssystems der VM steht dann ein USB-Adapter mit maximal 15 Anschlüssen zur Verfügung (siehe Abbildung 12-15). Dieser lässt sich übrigens auch im laufenden Betrieb hinzufügen und die Geräte sollten automatisch verbunden werden.



Abbildung 12-15: USB in der VM

Mittlerweile muss das USB-Gerät nicht mehr unbedingt mit dem Host verbunden sein, sondern das Durchreichen vom lokalen Arbeitsplatz über den vSphere Client in die VM ist ebenfalls möglich. Dafür wird am lokalen PC ein VMware USB Device installiert; angesteckte Geräte kann man über ein zusätzliches Icon in der Symbolleiste mit der VM

verbinden. Das funktioniert auch mit den meisten Dongles, Websticks, USB-Festplatten usw. Rufen Sie anschließend die Eigenschaften der VM auf, steht das verbundene USB-Gerät ebenfalls in der Liste.

Über eine Remote Desktop-Verbindung können Sie ebenfalls lokale USB-Sticks mit der Remote-Maschine verbinden. Wenn Sie die Remote Desktop-Verbindung aufgerufen haben, klicken Sie auf die Schaltfläche **OPTIONEN** und anschließend auf die Registerkarte **LOKALE RESSOURCEN**. Im unteren Bereich des Fensters klicken Sie auf die Schaltfläche **WEITERE**. Im folgenden Fenster, können Sie sowohl Laufwerke als auch Geräte, die später angeschlossen werden, an die entfernte Maschine durchreichen (siehe Abbildung 12-16).



Abbildung 12-16: USB-Geräte in der VM über RDP

USB-Dongles, Scanner, Drucker und andere Geräte können auch über einen USB-Device-Server angebunden werden – da gibt es z.B. den Digitus DN-13009, einen 4-Port-USB-Hub mit 100 MBit Ethernetanbindung, oder den »myUTN-50« von SEH mit 2 Ports; die Firma SILEX bietet sogar GBit-Verbindungen für USB im LAN an und AnywhereUSB bietet ebenfalls eine Netzwerklösung für USB an.

Das Programm *mstsc.exe* können Sie auch noch mit einer Reihe anderer Parameter aufrufen. Wählen Sie beispielsweise **START → AUSFÜHREN → MSTSC /?**, dann bekommen Sie einige Möglichkeiten angezeigt, die in Abbildung 12-17 aufgelistet sind. Die Parameter sind übrigens bei unterschiedlichen Versionen verschieden. So gibt es bei älteren Softwareständen den Befehl */admin* und bei den neueren */console*, die beide die gleiche Funktionalität haben: Damit kann ich die Remote-Verbindung so aufbauen, als säße ich direkt

am Rechner. Der Unterschied fällt meist erst auf, wenn zum Beispiel versucht wird, eine etwas kompliziertere Software zu installieren. Mit dem Parameter geht es, ohne nicht.

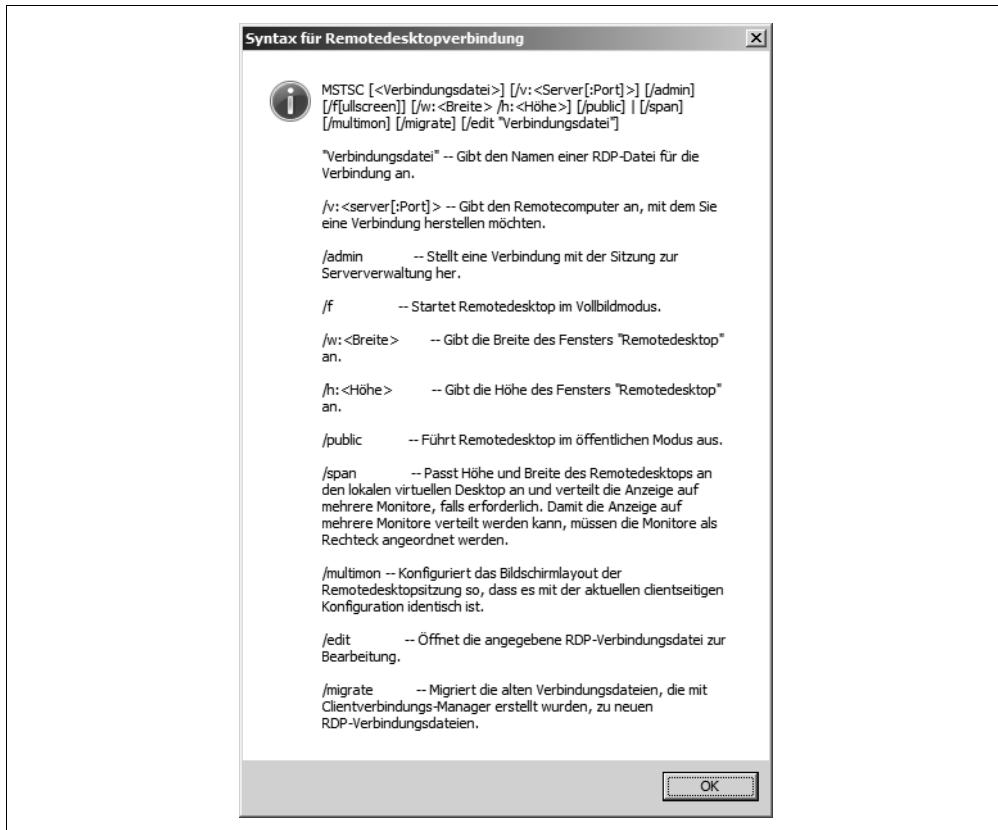


Abbildung 12-17: Informationen über Parameter von RDP

Eine neuere Version (7) für Windows XP und Vista ist auf der Microsoft-Website unter <http://www.microsoft.com/downloads/de-de/results.aspx?poId=&freetext=969084&DisplayLang=de> zum Download verfügbar.



---

# VMware Update Manager, Upgrade und Converter

Wenn Sie mit dem vCenter Server auch die Installation des Update Managers vorgenommen haben, hat dieser sicherlich schon Informationen aus dem Internet heruntergeladen, um potenzielle Patches und Updates anzeigen zu können, die sogenannten »Baselines« zugeordnet werden. Zu diesem Zeitpunkt können Sie aber außer auf der Festplatte des Servers keinerlei Einstellungsmöglichkeiten sehen. Das liegt daran, dass das Plugin für den vSphere Client noch nicht auf Ihrem Rechner installiert ist. Die Vorgehensweise dabei besprechen wir im zweiten Teil dieses Kapitels.

Der in vSphere integrierte vCenter Server Converter, den man aus den vorigen Versionen kennt, ist nicht mehr Bestandteil des Installationsmediums des vCenter Servers. Als Standalone-Variante kann man ihn in der Version 5.0 allerdings herunterladen und auf jedem Windows-Rechner nutzen.

## Konsolidieren

Eines der wichtigsten Themen bei der Virtualisierung in einer produktiven Umgebung ist die Übernahme bereits vorhandener physischer Rechner in die virtuelle Welt. Man spricht hier von einer *Konsolidierung*, weil meist mehrere Computer auf nur wenig Hardware zusammengefasst werden.

Da der Zugriff auf die Datenträger beim Booten des physischen und des virtuellen Servers meist unterschiedlich ist, kommt es in erster Linie auf die Anpassung des zukünftigen Gastbetriebssystems vor dem ersten Start in der virtuellen Welt an. Schlägt die Anpassung fehl, startet die VM später nicht.

Für die Virtualisierung von physischen Rechnern gibt es mehrere Möglichkeiten. Die einfachste Methode – die auch meistens funktioniert – ist der Import durch den VMware Converter, der unten besprochen wird. Hat man keine vSphere-Umgebung mit dem Management Server, kann man trotzdem den Converter Standalone von der VMware-Website herunterladen (nachdem man sich als User registriert hat).

Neben dem VMware Converter gibt es noch einige weitere Produkte, die ebenfalls für die Konvertierung genutzt werden können. Da muss als Erstes der *vConverter* von Vizion-core (jetzt Quest) genannt werden, weil er die zuverlässigste Alternative zum Produkt von VMware ist. Nach einer kurzen Registrierung kann das kostenlose Testprodukt über den zugesandten Link heruntergeladen und eingesetzt werden. Gerade bei nicht standardmäßigen Bootloadern oder mehreren Betriebssystemen auf einem Rechner ist dieses Produkt die richtige Wahl.

*Acronis Backup & Recovery* ist ebenfalls in der Lage, physische Maschinen in die virtuelle Welt zu holen. Dabei erstellt man ein Image des laufenden oder ausgeschalteten Rechners und spielt es in eine bereits vorhandene VM ein. Dieses Produkt kann auch den umgekehrten Weg gehen, also eine VM in eine physische Maschine exportieren. Der VMware Converter kann auch die entstandenen *.tib*-Dateien von Acronis in VMs konvertieren und anpassen.

## VMware Converter Standalone

Ob der Converter wie bei früheren Versionen als Plugin im vCenter Server oder als unabhängiges Produkt eingesetzt wird, spielt beim Import auf einen ESXi Server keine Rolle. Auch ist es egal, ob eine Windows- oder eine Linux-Maschine virtualisiert werden soll, ob Sie nur ein Backup oder Image von der zukünftigen VM haben oder ob es bereits eine laufende virtuelle Maschine auf einem anderen Produkt ist, z. B. Microsoft Virtual Server.

Folgende Importmöglichkeiten stehen zur Verfügung:

- ein laufender Rechner über das Netzwerk (administrativer Zugriff vorausgesetzt),
- ein ausgeschalteter physischer Rechner über die Boot-CD (Cold-Clone),
- ein Image von Acronis 9.1, 9.5, 10 oder 11 (*.tib*-Datei),
- ein Image von StorageCraft Shadow Protect (*.spf*-Datei) der Versionen 2.0, 2.5 oder 3.0 bis 3.2,
- ein Image von Norton Ghost 10.0, 12.0 oder 14.0,
- Parallels Desktop 2.5, 3.0 und 4.0 sowie Parallels Workstation 2.x (keine komprimierten Festplatten)
- ein Image von Symantec LiveState Recovery 3.0 oder 6.0 (nur *.sv2i*-Datei),
- ein Image von Symantec Backup Exec System Recovery 6.5, 7.0, 8.0 oder 8.5,
- ein Backup von VMware Consolidated Backup (VCB) und
- eine ausgeschaltete VM von allen VMware-Produkten, Microsofts Virtual PC und Server oder von Hyper-V.



Die Konvertierung eines Rechners mit EFI statt BIOS ist nicht möglich.

Der VMware Converter Standalone kümmert sich automatisch um das Alignment der Festplatte der virtuellen Maschine!

## Installation des Converters

Der vCenter Converter Standalone automatisiert und vereinfacht die Konvertierung physischer in virtuelle Maschinen, anderer virtueller Maschinen in ESXi VMs oder vorher gemachter Images in VMs. Eine Konvertierung zurück in das physische Format ist damit nicht möglich. Der Converter wird üblicherweise auf einem Rechner im Netzwerk installiert, der Zugriff auf die zu klonende Maschine und den Zielrechner hat, z. B. ESXi Server oder vCenter Server.



Sollte es doch einmal notwendig sein, eine virtuelle wieder in eine physische Maschine zu konvertieren, können Sie sich dabei wohl am ehesten auf *Acronis Backup & Recovery* verlassen. In den meisten bisherigen Fällen ging der Umzug zwischen verschiedenen Hardwareplattformen (virtuell oder physisch) ohne Probleme vonstatten.

Die Installation des Converter Standalone kann auf fast jeder Windows-Plattform durchgeführt werden:

- Windows XP 32 und 64 Bit mit SP3
- Windows Server 2003 32 und 64 Bit mit SP2
- Windows Vista 32 und 64 Bit mit SP2
- Windows 7 32 und 64 Bit
- Windows Server 2008 32 und 64 Bit mit SP2
- Windows Server 2008 R2 64 Bit

Alle diese Maschinen können als Converter-Client und als Converter-Server dienen und auch vom Converter selbst als physische oder virtuelle Maschine in die virtuelle Welt importiert werden. Es muss nicht unbedingt eine vSphere-Umgebung für die neue virtuelle Maschine angegeben werden – man kann auch eine andere Virtualisierungssoftware von VMware dafür nehmen.

Umwandeln kann der Converter zusätzlich fast alle Red-Hat-, SuSE- und Ubuntu-Maschinen, nur kann er dort nicht als Server oder Client installiert werden.

Der vCenter Converter Standalone kann von der VMware-Website (nach einmaliger Registrierung) kostenlos heruntergeladen und installiert werden (*VMware-converter-all-5.0.0-470252.exe*). Benutzen Sie für die Installation das benutzerdefinierte Setup und wählen Sie die Komponenten aus, die Sie benötigen (siehe Abbildung 13-1).

Wenn der Begrüßungsbildschirm angezeigt wird, klicken Sie auf WEITER.

Wählen Sie aus den folgenden Möglichkeiten das Passende aus:

- CONVERTER-SERVER: Dieser kann zentral auf einem Computer installiert werden, auf dem dann die eigentliche Arbeit verrichtet wird.

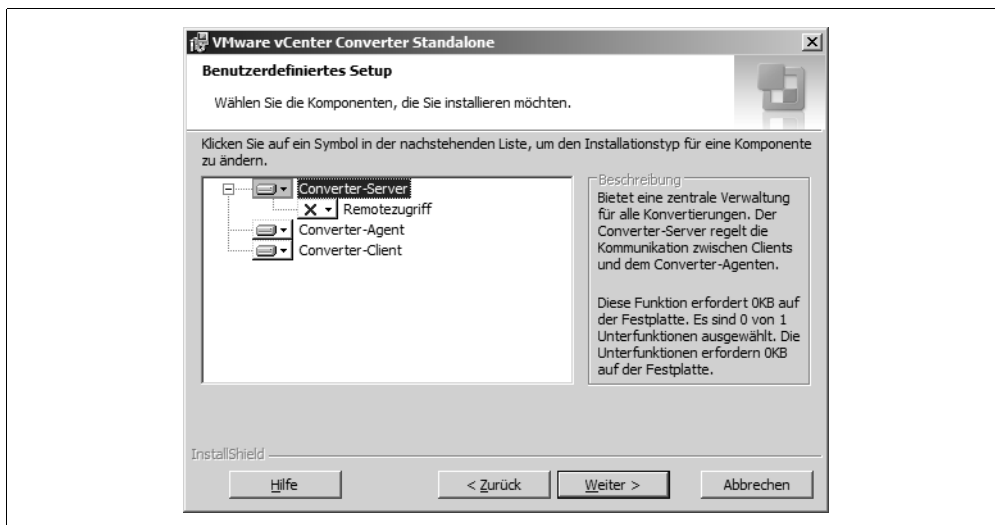


Abbildung 13-1: Installation des Converter Standalone

- **CONVERTER-SERVER REMOTEZUGRIFF:** Hiermit kann ein Zugriff von externen Rechnern auf den Server ermöglicht werden.
- **CONVERTER-AGENT:** Ist nur notwendig, wenn der lokale Rechner konvertiert werden soll.
- **CONVERTER-CLIENT:** Mit dem Client kann über eine grafische Oberfläche auf den Converter-Server zugegriffen werden. Dafür wird Port 9089 benötigt.

Sie brauchen die Portnummer für HTTP und HTTPS; standardmäßig verwendet vCenter Server dafür die Ports 80 und 443.

## Eine physische Maschine konvertieren

Die häufigste Anwendung für den Converter ist wohl das Migrieren eines eingeschalteten Rechners im laufenden Betrieb über das Netzwerk. Diese Vorgehensweise (»Hot-Clone«) hat den Vorteil, dass der Ausgangsrechner ohne Unterbrechung zur Verfügung steht und man den Vorgang ohne Probleme auch jede Nacht laufen lassen kann, um z. B. eine VM als Sicherheit bei einem Ausfall des physischen Rechners zu haben. Dabei werden folgende Phasen durchlaufen:

1. Der Computer, an dem die Aufgabe gestartet wird, nimmt über den Namen oder die IP-Adresse Kontakt zum Quellrechner auf (ADMIN\$ Freigabe).
2. Auf dem Quellrechner wird ein Agent installiert und mit administrativen Berechtigungen ausgeführt.
3. Der Agent überprüft die Quellmaschine und meldet die gesammelten Informationen über Betriebssystem und Hardware an den Converter.

4. Anhand der vorliegenden Informationen wird auf dem Zielrechner (ESXi Server) eine neue VM erstellt, die möglichst die gleiche Hardware (Festplattengröße, Anzahl CPUs und RAM usw.) hat.
5. Der Agent auf dem Ausgangs-PC macht einen Snapshot der beteiligten Volumes und übergibt die Daten dem ESXi Server. Dieser speichert die Daten in der *.vmdk*-Datei.
6. Die erforderlichen Treiber werden in die *.vmdk*-Datei kopiert, und das Betriebssystem wird entsprechend geimpft (Registry-Änderungen).
7. Auf dem Quellrechner wird der Agent deinstalliert.
8. Beim ersten Start wird die MAC-Adresse der Netzwerkkarte der VM angepasst.

Wie Sie in Abbildung 13-2 sehen, kann die Festplattengröße vor der Konvertierung noch angepasst werden. Zu große Volumes können verkleinert und zu kleine vergrößert werden. Das funktioniert auch bei bereits bestehenden virtuellen Maschinen, indem Sie die VM über den Converter in eine VM klonen. Weiterhin können Sie hier gegebenenfalls Partitionen in Laufwerke konvertieren und nicht benötigte Volumes aussparen. Brauchen Sie eine zusätzliche Partition, können Sie das ebenfalls jetzt oder nachträglich bei der VM erledigen.

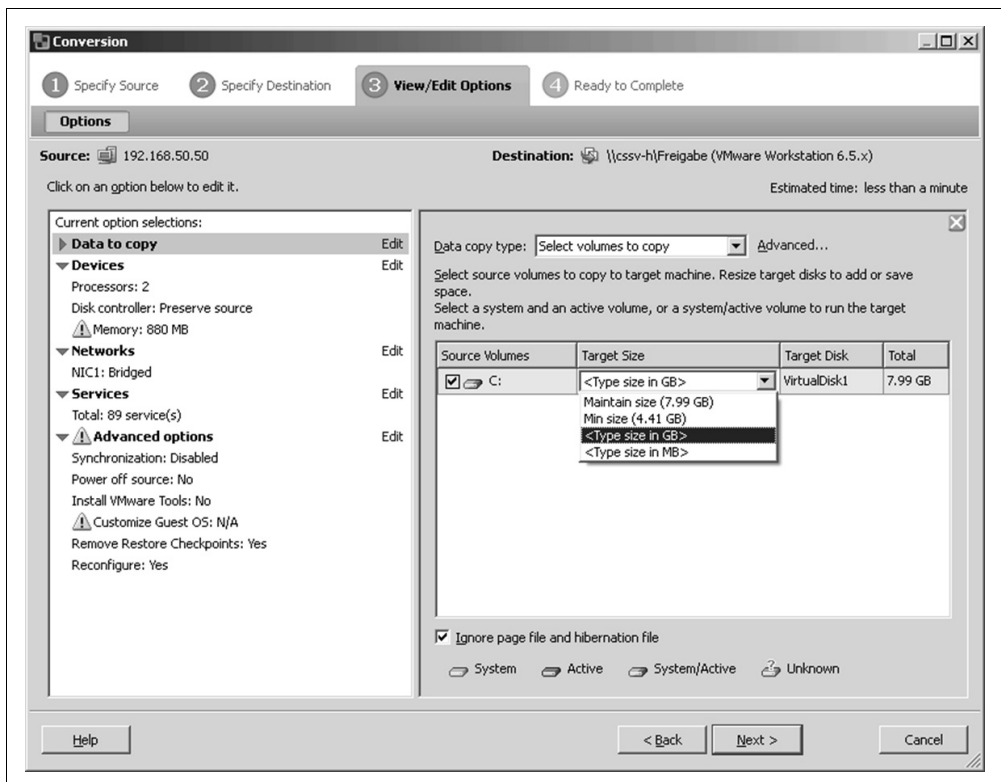


Abbildung 13-2: Converter-Festplattenanpassung

Weiterhin haben Sie die Möglichkeit,

- die Anzahl der Prozessoren zu ändern,
- die Menge an Arbeitsspeicher anzupassen,
- die Netzwerkkarte zu konfigurieren,
- laufende Dienste mit ihrer Startart anzupassen,
- eine Synchronisation nach dem Klonen anzustoßen,
- das Gastbetriebssystem in der VM benutzerdefiniert anzupassen (z.B. *sysprep* bei Windows) und
- Wiederherstellungspunkte bei Windows zu entfernen (empfohlen).



Wenn Sie in der fertigen VM einen Wiederherstellungspunkt von vor der Konvertierung auswählen, startet die Maschine wahrscheinlich nicht mehr.

Nachdem der Converter das Quellsystem in eine virtuelle Maschine migriert hat, sollten Sie noch ein paar weitere Arbeiten durchführen:

1. Vor dem Start der konvertierten VM schauen Sie sich zuerst die Einstellungen zur Hardware an. Entfernen Sie alles, was Sie in der VM nicht brauchen, z. B. serielle und parallele Schnittstellen, USB (funktioniert mittlerweile), Diskettenlaufwerke usw.
2. Ist die physische Maschine noch eingeschaltet, nehmen Sie in der VM den Link zur Netzwerkkarte weg, um doppelte Namen oder IP-Adressen im Netzwerk zu vermeiden. Am besten entfernen Sie die NIC ganz und fügen eine neue hinzu, die besser zur virtuellen Maschine passt (siehe Kapitel 4).
3. Führt die VM ohne Probleme hoch und laufen alle benötigten Anwendungen zu Ihrer Zufriedenheit, sollten Sie die VMware Tools installieren und gegebenenfalls die Auslagerungsdatei sowie Bildschirmauflösung und -farbtiefe usw. anpassen.
4. Nach dem Neustart sollten Sie die nicht mehr vorhandene Hardware entfernen. Gerade Windows merkt sich in der Registry alle jemals angeschlossenen Geräte und bekommt dadurch schon mal Probleme.

Geben Sie in einer DOS-Box Folgendes ein:

```
set devmgr_show_nonpresent_devices=1
devmgmt.msc
```

Schalten Sie anschließend unter ANSICHT die ausgeblendeten Geräte ein und deinstallieren Sie die nicht mehr vorhandenen (abgeblendet dargestellt) – mit Ausnahme des RAS-Adapters und des gesamten Zweigs NICHT-PNP-GERÄTE.

5. Beachten Sie, dass die Security-ID die gleiche ist wie bei der physischen Maschine. Meistens ist das gewollt, da die VM ja die Hardware ablösen soll.

6. Ist eine Anwendung an die MAC-Adresse der Maschine gebunden und lässt sich diese nicht durch eine Neueingabe im Treiber der NIC austricksen, können Sie diese in den Einstellungen der VM unter NETZWERKKARTE frei wählen.

Wenn Sie alles richtig gemacht haben, sollte Ihre VM nun die neue MAC-Adresse haben und damit auch starten können.

## Probleme bei der Konvertierung

Nicht immer geht die Migration einer physischen in eine virtuelle Maschine ohne Weiteres vonstatten. Bei der Arbeit mit dem VMware Converter werden über die Schaltfläche PROTOKOLLINFORMATIONEN die Speicherorte der Logdateien auf beiden beteiligten Rechnern angezeigt. Die Logdateien sind die erste Anlaufstelle, wenn es zu Komplikationen kommt. Die Lösungen zu Meldungen am Ende der Datei können auch bei VMware online abgefragt werden, unter <http://kb.vmware.com>.

Gerade unter Windows XP kann es zu Problemen beim Festplattenzugriff kommen. Microsoft hat im Artikel 314082 einen Workaround dafür festgehalten (siehe <http://support.microsoft.com/kb/314082/de>). Weitere Probleme mit dem Bootsektor können meist durch das Starten von CD in die Wiederherstellungskonsole behoben werden, indem auf der Kommandozeile die Befehle `fixmbr` und `fixboot` eingegeben werden. Ein weiteres mögliches Problem besteht in der falschen Sortierung der Festplatten und damit falschen Einträgen in *Boot.ini*. Das lässt sich meist durch den Befehl `bootcfg /rebuild` ebenfalls in der Wiederherstellungskonsole beheben.

Sollten beim importierten XP alle obigen Empfehlungen scheitern, importieren Sie nochmals und wählen beim Festplattenadapter IDE aus. Damit sollte die VM starten. Da eine IDE-Festplatte aber in der virtuellen Welt sehr langsam ist, sollten Sie diese dann umgehend ändern, z.B. in LSI Logic. Wie das geht, steht in Kapitel 18.

Bei Windows Vista ist die Vorgehensweise ähnlich: Starten Sie den Rechner von der CD und wählen Sie COMPUTERREPARATUROPTIONEN. Damit müsste alles automatisch repariert werden. Falls das nicht fruchtet, versuchen Sie es mit einer Windows 7-CD – meist klappt es damit.

Wenn Sie einen Domänencontroller virtualisieren wollen, müssen Sie dabei sehr vorsichtig sein. Beachten Sie, dass der importierte DC wie ein Klon ist – mit gleichem Namen und gegebenenfalls gleicher IP-Adresse. Sollten Fehler beim Migrieren oder hinterher auftreten, lesen Sie den KB-Artikel 1006996 von VMware. Dort wird eine Vorgehensweise erklärt, die bei meinen Kunden mehrfach problemlos funktionierte. Ich empfehle aber, eine neue VM zu erstellen und die FSMO-Rollen auf den neuen DC zu verschieben. Das funktioniert immer und ist eine saubere Vorgehensweise.

Einen Windows NT-Domänencontroller sollten Sie nicht konvertieren. Erstellen Sie besser eine VM als Backup-Domänencontroller, stufen Sie diesen anschließend hoch (nach

zwei bis drei Tagen), machen einen Snapshot und aktualisieren Sie diesen auf die neue Version.

Datenbankserver und Exchange-Server sollten ebenfalls vorsichtig behandelt werden. Beenden Sie vor dem Import die jeweiligen Dienste und versuchen Sie es erst dann.

Falls Sie den Rechner direkt auf einen ESXi Server migrieren wollen, beachten Sie Folgendes:

- Sie brauchen zur Anmeldung den User *root* und sein Passwort.
- Nehmen Sie lieber die IP-Adresse des ESXi Servers anstelle des DNS-Namens.
- Stellen Sie sicher, dass die Ports 443 und 902 zugänglich und nicht blockiert sind.
- Denken Sie bei VMFS-Versionen vor 5 an die Größe der Volumes: Bei 1 MByte Clustergröße können nur maximal 256 GByte große Dateien angelegt werden.
- Nutzen Sie einen eindeutigen Namen für Ihre VM, der noch nicht vergeben ist.

## Update Manager

Haben Sie bei der Installation des vCenter Servers ebenfalls gleich den Update Manager installiert, versucht dieser bereits im Hintergrund, Informationen über potenzielle Updates und Patches von VMware, Microsoft und Shavlik herunterzuladen. Weiterhin versucht er jede Stunde einmal Benachrichtigungen über zurückgezogene Updates und Patches von VMware zu bekommen. Die Meldungen darüber sehen Sie auch ohne installiertes Plugin am unteren Bildschirmrand bei Kürzlich bearbeitete Aufgaben. Einstellungen und Informationen zum Update Manager sehen Sie aber erst mit installiertem Plugin. Die Vorgehensweise dabei besprechen wir jetzt.

## vSphere Client-Plugin installieren

Klicken Sie auf der grafischen Oberfläche im Menü auf PLUG-INS → PLUG-INS VERWALTEN. Es öffnet sich ein neues Fenster, in dem Sie den Link (HERUNTERLADEN UND INSTALLIEREN) beim Update Manager auswählen können. Wenn der Fortschrittsbalken bei 100 % angelangt ist, können Sie eine Sprache für die Installation auswählen. Sollten Sie damit Probleme haben, finden Sie die ausführbare Datei auch auf dem vCenter Server unter *C:\Programme (x86)\VMware\Update Manager\docroot\vc\downloads\*. Falls die Probleme an der Namensauflösung liegen, sollten Sie besser dieses Problem zuerst beseitigen.

Akzeptieren Sie die Lizenzvereinbarung und klicken Sie auf WEITER. Die Installation braucht nur ein paar Sekunden, und anschließend bekommen Sie den Hinweis, dass ein Zertifikat erforderlich ist. Ansonsten warten Sie, bis das *Update Manager Plug-In* in der Liste nach oben gerutscht ist. Passiert weiterhin nichts, beenden sie den vSphere Client und melden sich neu an – dann sollte es funktionieren. Bekommen Sie aber eine Fehler-



meldung, kann es am Anmeldenamen liegen: Er darf ausschließlich aus ASCII-Zeichen bestehen.

Im Fenster des Plugin-Managers müsste kurze Zeit später die installierte Komponente im oberen Bereich der Liste auftauchen.

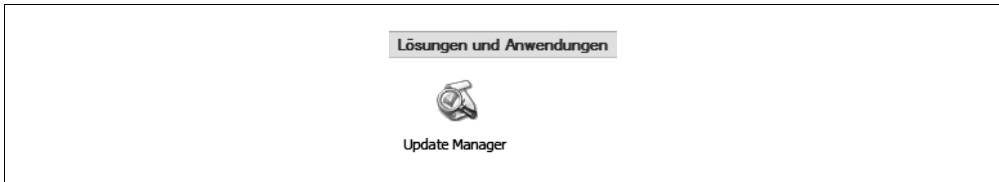


Abbildung 13-3: Symbol des Update Managers

Durch diese Clienterweiterung wird jeweils beim vCenter Server, dem Datencenter, dem Cluster, den Hosts und den vApps eine neue Registerkarte UPDATE MANAGER hinzugefügt. Bei der VM bekommen Sie jedoch nur den Hinweis, dass Sie nicht über die Bestandsliste *Hosts und Cluster*, sondern nur über *VMs und Vorlagen* darauf zugreifen können (seltsam!).

Im *Home*-Bereich wurde ein neuer Abschnitt LÖSUNGEN UND ANWENDUNGEN erstellt, über den Sie jetzt die Konfiguration des Update Managers vornehmen können (siehe Abbildung 13-3).

## Den Update Manager konfigurieren

Sie können den Update Manager als zentrale Instanz für Patches und Updates der Hosts und der virtuellen Maschinen ansehen. Sie müssen aber Ihre VMs nicht anders behandeln als Ihre physischen Rechner. Haben Sie also z. B. einen WSUS-Server, können Sie die VMs auch damit bestücken. Umgekehrt geht es übrigens nicht: Der Update Manager versorgt nur die virtuelle Welt. Bei den VMware Tools handelt es sich natürlich um eine Ausnahme, denn die bekommen Sie sonst nirgendwo.

Haben Sie das Symbol für den Update Manager angeklickt, erhalten Sie einen Abschnitt mit sieben Registerkarten, die teilweise wiederum unterteilt sind. Auf der ersten Karte BASELINES UND GRUPPEN wird zunächst zwischen Hosts und VMs unterschieden. Bei beiden gibt es PATCH-BASELINE und UPGRADE-BASELINE. Haben Sie nur ESXi Version 5 in Ihrer Zusammenstellung, dürfte zunächst lediglich die erste Möglichkeit PATCH-BASELINE interessant sein. Patches für ältere Server – also ESX und ESXi 4.x sowie ESX 3.x-Hosts – werden nur heruntergeladen, wenn Sie Ihrer Umgebung so einen Host hinzugefügt haben. In der Liste sehen Sie normalerweise zwei Zeilen für kritische und nicht kritische Patches und eine Anzahl möglicher Patches. Diese Zahl ist wieder ein Link, über den ein Fenster mit weiteren Informationen zu den Patches angezeigt wird (siehe Abbildung 13-4).

| Patch-Name                          | Anbieter     | Patch-ID            | Schweregrad | Kategorie  | Auswirkung            | Datum der Veröffentlichung |
|-------------------------------------|--------------|---------------------|-------------|------------|-----------------------|----------------------------|
| Updates VMX                         | VMware, Inc. | ESX400-200906401... | Kritisch    | Anderer    | Wartungsmodus (U...   | 09.07.09 10:00:00          |
| Updates ESX Scripts                 | VMware, Inc. | ESX400-200906402... | Kritisch    | Anderer    | Hostd-Neustart        | 09.07.09 10:00:00          |
| Updates CIM                         | VMware, Inc. | ESX400-200906404... | Kritisch    | Anderer    | Hostd-Neustart        | 09.07.09 10:00:00          |
| Updates krb5 and pam_krb5           | VMware, Inc. | ESX400-200906405... | Kritisch    | Sicherheit | Neu starten, Wartu... | 09.07.09 10:00:00          |
| Updates sudo                        | VMware, Inc. | ESX400-200906406... | Kritisch    | Sicherheit |                       | 09.07.09 10:00:00          |
| Updates curl                        | VMware, Inc. | ESX400-200906407... | Kritisch    | Sicherheit |                       | 09.07.09 10:00:00          |
| Updates SCSI Driver for QLogic FC   | VMware, Inc. | ESX400-200906408... | Kritisch    | Anderer    | Neu starten, Wartu... | 09.07.09 10:00:00          |
| Updates LSI storelib Library        | VMware, Inc. | ESX400-200906409... | Kritisch    | Anderer    | Hostd-Neustart        | 09.07.09 10:00:00          |
| Updates hostd                       | VMware, Inc. | ESX400-200906410... | Kritisch    | Anderer    | Hostd-Neustart        | 09.07.09 10:00:00          |
| Updates udev                        | VMware, Inc. | ESX400-200906411... | Kritisch    | Sicherheit |                       | 09.07.09 10:00:00          |
| Updates esxupdate                   | VMware, Inc. | ESX400-200906412... | Kritisch    | Anderer    | Hostd-Neustart        | 09.07.09 10:00:00          |
| Updates vmkernel iSCSI Driver       | VMware, Inc. | ESX400-200906413... | Kritisch    | Anderer    | Neu starten, Wartu... | 09.07.09 10:00:00          |
| Updates vmkernel64                  | VMware, Inc. | ESX400-200907401... | Kritisch    | Anderer    | Neu starten, Wartu... | 06.08.09 10:00:00          |
| Updates vmx and vmkernel64          | VMware, Inc. | ESX400-200909401... | Kritisch    | Anderer    | Neu starten, Wartu... | 24.09.09 10:00:00          |
| Updates VMware Tools                | VMware, Inc. | ESX400-200909402... | Kritisch    | Anderer    | Hostd-Neustart        | 24.09.09 10:00:00          |
| Updates bnx2x                       | VMware, Inc. | ESX400-200909403... | Kritisch    | Anderer    | Neu starten, Wartu... | 24.09.09 10:00:00          |
| Updates igbpe                       | VMware, Inc. | ESX400-200909404... | Kritisch    | Anderer    | Neu starten, Wartu... | 24.09.09 10:00:00          |
| Updates hpsa                        | VMware, Inc. | ESX400-200909406... | Kritisch    | Anderer    | Neu starten, Wartu... | 24.09.09 10:00:00          |
| Updates VMware ESX 4.0 Core and...  | VMware, Inc. | ESX400-200911201... | Kritisch    | Anderer    | Neu starten, Wartu... | 19.11.09 09:00:00          |
| Updates the ESX 4.0 Web Access C... | VMware, Inc. | ESX400-200911223... | Kritisch    | Sicherheit |                       | 19.11.09 09:00:00          |

Abbildung 13-4: Patch-Details

Für große Umgebungen ist das Gruppieren von Baselines gedacht. Sie können sich mit einem Assistenten auch eigene Grundlagenlinien erstellen und nach Ihren Wünschen konfigurieren.

Die eigentliche Konfiguration des Update Managers erfolgt auf der zweiten Registerkarte:

Bei NETZWERKKONNEKTIVITÄT können zunächst der Port für die Client- und Hostkommunikation sowie der zuständige Server festgelegt bzw. geändert werden.

Die PATCH-DOWNLOAD-EINSTELLUNGEN sollten Sie prüfen und die Häkchen nur dort setzen, wo es für Sie Sinn ergibt. Die Quellen, von denen die Updates geholt werden, können Sie über den Link PATCH-QUELLE HINZUFÜGEN erweitern. Ein GEMEINSAMES REPOSITORY ist für manche Firmen mit großem Sicherheitsbedürfnis eine Möglichkeit, Daten zwischen Firewalls bereitzustellen. Im unteren Teil des Fensters befinden sich die Proxy-Einstellungen, die Sie hier auch gleich testen können.

Den PATCH-DOWNLOAD-ZEITPLAN zum Herunterladen der Informationen können Sie hier nur einsehen. Möchten Sie ihn bearbeiten, verwenden Sie den Link DOWNLOAD-ZEITPLAN BEARBEITEN rechts oben oder gehen im *Home*-Bereich auf GEPLANTE AUFGABEN.

Der ZEITPLAN FÜR DAS PRÜFEN VON BENACHRICHTIGUNGEN ist ebenfalls eine vordefinierte Aufgabe, die Sie über GEPLANTE AUFGABEN finden können. Hier wird stündlich auf der Website von VMware nachgeschaut, ob es bei anderen Kunden zu Problemen mit Patches oder Updates gekommen ist. Wenn ja, wird der Patch gesperrt. Sie können Sich auch eine E-Mail zusenden lassen, wenn dieser Fall eintritt.

Unter EINSTELLUNGEN DER VM können Sie festlegen, ob vor Updates Snapshots gemacht und wie lange sie aufbewahrt werden, bevor sie übernommen werden.

Unter den ESX-HOST-/CLUSTEREINSTELLUNGEN kann ähnlich wie bei Diensten die Wiederholung mit Zeitverzögerung eingeräumt werden. In einem DRS-Cluster werden die VMs zunächst auf andere ESXi Server verteilt und dann der Host in den Wartungsmodus versetzt und schließlich upgedatet. Funktioniert das nicht sofort, wird der Vorgang standardmäßig dreimal wiederholt. Überlegen Sie sich, ob es nicht sinnvoll sein könnte, die Wechselmedien von den VMs zu trennen, damit diese ggf. verschoben werden können.

Unter CLUSTEREINSTELLUNGEN kann nach Bedarf oder tatsächlicher Umgebung noch eingestellt werden, dass z.B. DPM (Distributed Power Management) für den Updatevorgang deaktiviert wird. Je nachdem, wie viele Hosts Sie haben, kann das angebracht sein. Das Gleiche betrifft HA und FT. Ausgeschaltete oder angehaltene VMs müssen eigentlich nicht auf einen anderen Host übertragen werden. Der letzte Punkt betrifft das Updaten von Hosts, die über Auto Deploy erstellt wurden. Entscheiden Sie, ob Sie diese auch auf dem neuesten Stand haben oder lieber bei Bedarf neu installieren wollen.

Die Einstellungen unter VAPP sind selbsterklärend (auch in der deutschen Übersetzung).

Auf der Registerkarte EREIGNISSE erscheinen alle Vorgänge, die mit dem Update Manager zu tun haben, also auch das Prüfen eines Hosts auf Updates.

Die Anzeige auf der Karte BENACHRICHTIGUNGEN ist üblicherweise leer. Hier wird im Falle eines Falles ein Hinweis auf zurückgezogene Patches oder Updates angezeigt.

Das PATCH-REPOSITORY zeigt Informationen zu den bisher vorliegenden Informationen über Downloads an. Diese Liste kann natürlich nach jeder beliebigen Spalte sortiert werden.

ESXi-IMAGES ist die sechste oder vorletzte Karte in dem Register. Hier kann man ISO-Dateien zum Upgraden von Hosts zur Verfügung stellen. Über den Link ESXi-IMAGE IMPORTIEREN gelangen Sie in einen Browser zum Suchen der Vorlagen. Diese Images werden anschließend im Update Manager zur Verfügung gestellt, damit darüber ein Upgrade durchgeführt werden kann, z.B. von 4.1 auf 5.0. Lesen Sie dazu den letzten Teil in diesem Kapitel »Upgrade der Umgebung« durch.

Die letzte Registerkarte kann Updates für VA (Virtual Appliances) enthalten, denn auch für diese vorgefertigten VMs werden Aktualisierungen zur Verfügung gestellt, z.B. für den VMware Data Director Management und DB Server.

## Einen Host updaten

Wie sie einen alleinstehenden ESXi Host updaten, steht in Kapitel 9. Da es hier keinen Update Manager gibt, wird das über die Kommandozeile erledigt.

Klicken Sie auf den Host, den Sie auf den neuesten Stand bringen wollen. Navigieren Sie zum Register UPDATE MANAGER. Zuerst muss eine Baseline an den Host gehängt werden.

Klicken Sie dazu auf den Link ANHÄNGEN. Im folgenden Fenster wählen Sie die Baseline oder alle Baselines aus und klicken Sie auf ANHÄNGEN (siehe Abbildung 13-3).

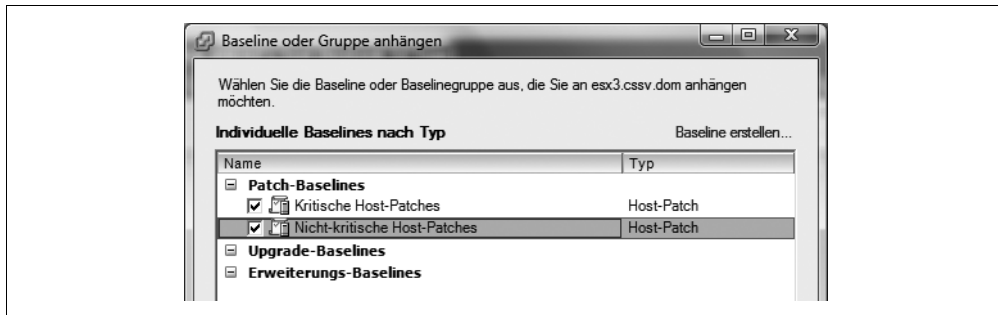


Abbildung 13-5: Baseline oder Gruppe anhängen

Welche von den Neuerungen vermutlich auf den Host zutreffen, erfahren Sie, wenn Sie auf den Link PRÜFEN klicken. Die Schaltfläche im unteren Teil des Fensters BEREITSTELLEN übernimmt anschließend die Aufgabe, dem Host die Neuerungen anzubieten. Über diesen Assistenten wird anschließend die zu überprüfende Anzahl von Patches angezeigt. Das BEREITSTELLEN kann einige Zeit dauern. Beachten Sie die Hinweise unter KÜRZLICH BEARBEITETE AUFGABEN.



Erst wenn einem Host Patches bereitgestellt werden, lädt der Update Manager diese Daten aus dem Internet. Je nach Internetverbindung kann das ein Weilchen dauern.

Sobald der Vorgang abgeschlossen ist, sehen Sie das Ergebnis in der Übersicht. Sollte ein großer roter Kreis angezeigt werden, gibt es Neuerungen, die Sie dem Host zuteilen sollten. Klicken Sie dafür auf STANDARDISIEREN (will sagen: auf den neuesten Stand bringen), bestätigen Sie die Auswahl zweimal mit WEITER und setzen Sie den Termin fest. Haben Sie SOFORT ausgewählt und auf BEENDEN geklickt, wird der Host in den Wartungsmodus gefahren, und die Updates werden installiert. Das lässt sich unter AUFGABEN UND EREIGNISSE detailliert betrachten.

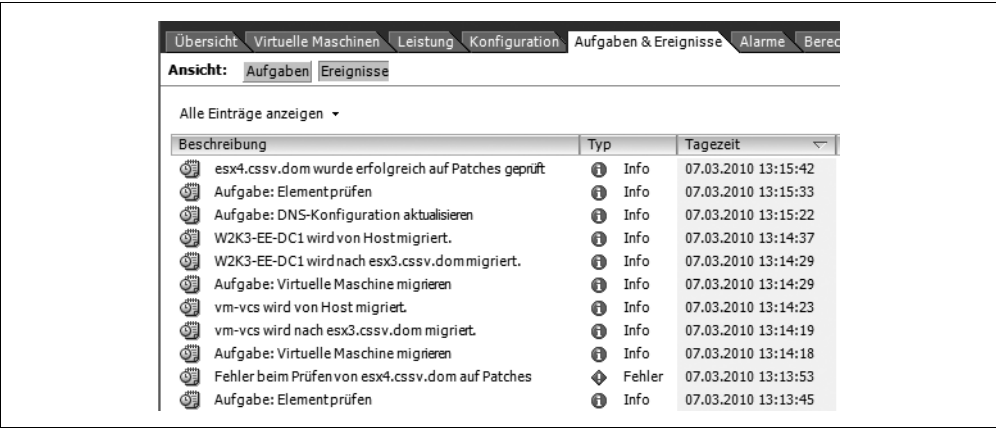


Sollte auf dem ESXi Server der vCenter Server laufen, kann der Vorgang eventuell fehlschlagen. Verschieben Sie ihn besser vorher mit vMotion auf einen anderen Host, weil der ESXi Server sonst gegebenenfalls nicht den Wartungsmodus einleiten kann und somit keine Updates bekommt.

Auch wenn für einen Patch das Neustarten des Hosts festgelegt ist, muss dieser eventuell gar nicht neu gestartet werden. Dabei können Sie sich auf den Update Manager verlassen.

Wenn alles installiert ist, wird der Host meistens neu gestartet. Das kann in seltenen Fällen auch mehrfach notwendig sein. Ist er fertig, kehrt er automatisch aus dem Wartungs-

modus zurück, und per DRS können wieder VMs aufgenommen werden. Bei den Ereignissen sollten Sie den erfolgreichen Abschluss der Aktion sehen können (siehe Abbildung 13-6).



| Übersicht Virtuelle Maschinen Leistung Konfiguration Aufgaben & Ereignisse Alarme Bere... |        |                     |  |
|-------------------------------------------------------------------------------------------|--------|---------------------|--|
| Ansicht: Aufgaben Ereignisse                                                              |        |                     |  |
| Alle Einträge anzeigen ▾                                                                  |        |                     |  |
| Beschreibung                                                                              | Typ    | Tagezeit            |  |
| esx4.cssv.dom wurde erfolgreich auf Patches geprüft                                       | Info   | 07.03.2010 13:15:42 |  |
| Aufgabe: Elementprüfen                                                                    | Info   | 07.03.2010 13:15:33 |  |
| Aufgabe: DNS-Konfiguration aktualisieren                                                  | Info   | 07.03.2010 13:15:22 |  |
| W2K3-EE-DC1 wird von Host migriert.                                                       | Info   | 07.03.2010 13:14:37 |  |
| W2K3-EE-DC1 wird nach esx3.cssv.dom migriert.                                             | Info   | 07.03.2010 13:14:29 |  |
| Aufgabe: Virtuelle Maschine migrieren                                                     | Info   | 07.03.2010 13:14:29 |  |
| vm-vcs wird von Host migriert.                                                            | Info   | 07.03.2010 13:14:23 |  |
| vm-vcs wird nach esx3.cssv.dom migriert.                                                  | Info   | 07.03.2010 13:14:19 |  |
| Aufgabe: Virtuelle Maschine migrieren                                                     | Info   | 07.03.2010 13:14:18 |  |
| Fehler beim Prüfen von esx4.cssv.dom auf Patches                                          | Fehler | 07.03.2010 13:13:53 |  |
| Aufgabe: Elementprüfen                                                                    | Info   | 07.03.2010 13:13:45 |  |

Abbildung 13-6: Ereignisse des Updates



Sollten Sie beim Prüfen auf Updates Fehlermeldungen bekommen, kann es an einer falschen DNS-Einstellung liegen (siehe Abbildung 13-6).

## Vorgehensweise beim Patchen

Die Erfahrungen der letzten Jahre haben gezeigt, dass das Aktualisieren der Hosts in einer vSphere-Umgebung fast immer ohne Probleme vonstatten geht. Trotzdem kann auch die beste Firma nicht alle Eventualitäten vorher durchprobieren. Meine Empfehlung lautet also: Wenn neue Patches für Ihre ESXi Server vorliegen, warten Sie noch ein paar Tage. Nehmen Sie sich dann zuerst einen der Hosts vor und bringen ihn auf den neuesten Stand. Erst wenn dieser Host ohne Probleme einige Zeit verbracht hat, nehmen Sie sich die anderen der Reihe nach vor.

Die ESXi Server können in einem Subnetz installiert und betrieben werden, das keine Verbindung zum eigentlichen LAN oder gar dem Internet hat. Auch wenn sicherheitskritische Updates vorliegen, brauchen Sie sich dann keine Gedanken zu machen. Der vCenter Server kann (außer bei der Appliance) mit zwei Netzwerkkarten in unterschiedlichen Subnetzen oder VLANs betrieben werden, und nur er braucht Zugriff auf das Management Network der Hosts. vMotion- oder Storage-Zugriff kann ebenfalls über VLANs oder separate Subnetze betrieben werden. Nur wenn Treiber oder Firmware von Geräten auf den neuesten Stand gebracht werden müssen, ist ein schnelles Eingreifen in so einer gesicherten Umgebung unabdingbar.

Sollte wirklich mal ein GAU passieren, haben Sie, wenn Sie wie eben beschrieben vorgegangen sind, höchstens einen ESXi Server, der nicht mehr korrekt funktioniert. Der lässt sich schnell wieder installieren und neu einrichten.

## Upgrade der Umgebung

Da die Verbreitung von vSphere 4 schon weit fortgeschritten ist, ist die Wahrscheinlichkeit eines Upgrades auf die aktuelle Version sehr hoch. Und wenn der Wartungsvertrag noch Bestand hat, können die Lizenzen meist kostenlos gegen eine Lizenz der neuen Version getauscht werden.

VMware wirbt mit einigen neuen Features und Funktionen sowie mit deutlich verbesserter Performance. Einige der Neuigkeiten habe ich in den vorangegangenen Kapiteln ja schon beschrieben, andere folgen in den nächsten Kapiteln. Hier nur in Kürze das Wichtigste:

- Den vCenter Server gibt es mit wenigen Funktionseinschränkungen auch als fertige VM im OVF-Format (siehe Kapitel 10).
- Der ESX Server wird in der neuen Version nicht mehr unterstützt, sondern nur noch der ESXi, der jetzt allgemein als »Hypervisor« bezeichnet wird (siehe Kapitel 3 und 5).
- Lokale ESXi-Platten können zu einem gemeinsamen Storage zusammengeschlossen werden (VSA, siehe Kapitel 11).
- Der vCenter Converter ist nicht mehr Bestandteil der vSphere-Umgebung, sondern nur noch als Standalone verfügbar (siehe dieses Kapitel).
- VMs können bis zu 32 virtuellen Prozessoren und 1 TByte RAM nutzen (siehe Kapitel 4).
- Die Lizenzierung wurde mit vRAM weiter eingeschränkt und teilweise verteuert (siehe Kapitel 10).
- vSphere Auto Deploy ermöglicht das Einrichten vieler neuer physischer Hostsysteme in kurzer Zeit (siehe Kapitel 11).
- Als neue Funktionen für Festplattenzugriffe sind Profile Driven Storage und Storage Distributed Resource Scheduler hinzugekommen (siehe Kapitel 18).

Wenn Sie eine komplette vSphere 4.x-Umgebung mit vCenter Server und externen Storages haben, können Sie zuerst den vSphere Client und dann den vCenter Server updaten. Als Nächstes nehmen Sie sich die Hosts vor. Haben Sie allerdings nur eine kleine Umgebung mit lokalen Festplatten auf Ihrem ESX Host, müssen Sie zunächst alle VMs auf einen anderen Storage verlagern oder im OVF-Format exportieren, bevor Sie eine Neuinstallation oder ein Upgrade versuchen.

Grundsätzlich ist der vSphere Client abwärtskompatibel: In Wirklichkeit landen also nur wenige zusätzliche Dateien auf der lokalen Festplatte, wenn Sie ihn erneuern. Mit einem neuen Client können Sie also auch noch auf die alte Umgebung zugreifen. Ähnlich gela-

gert ist es beim vCenter Server: In der Version 4.1 haben Sie Zugriff auf ESX Hosts der Version 4.1 und älter – aber nicht neuer. Bei der 5er-Version des Servers können Sie also auf die 5er-Hosts und die älteren zugreifen. Auch ein gemischter Modus ist kein Problem. Das Gleiche gilt für die virtuellen Maschinen: Eine ältere VM mit Hardwareversion 4 oder 7 läuft auch auf einem 5er-Host, der üblicherweise die aktuelle Version 8 der virtuellen Hardware nutzt.

Alle möglichen Updateszenarien hier detailliert aufzulisten, würde den Umfang des Buches sprengen, deshalb beschränke ich mich im Folgenden auf das Wesentliche.



Achten Sie vor dem Upgrade unbedingt auf die Kompatibilität Ihrer Hardware zur neuen Version und besorgen Sie sich rechtzeitig die neuen Lizenzschlüssel.

## Upgrade eines ESX Hosts

Liegt nur ein allein stehender ESX Server vor, können Sie diesen mit der neuen CD oder einem USB-Stick starten, nachdem alle VMs heruntergefahren wurden. Überlegen Sie sich, ob Sie –wie oben bereits erwähnt – Ihre VMs nicht doch lieber vorher sichern oder anderweitig kurzfristig auslagern wollen. Auch externe Storages sollten Sie vorher trennen, wenn nicht darauf die Bootpartition liegt. Beachten Sie die Hinweise bezüglich der BIOS-Einstellungen des Servers in Kapitel 3, zumal Sie hier meistens sowieso die Bootreihenfolge kurzfristig ändern müssen.

Meistens geht der Upgradeprozess ohne Probleme vonstatten und die bisherige VMFS-Partition wird dabei nicht angetastet. Meine Empfehlung lautet aber eindeutig: Neuinstallation ist in den meisten Fällen besser. Ein Upgrade auf die neue Version ist immer unumkehrbar.



Ein direktes Upgrade von Version 3.5 auf 5.0 ist nicht möglich – hier müssen Sie zunächst auf Version 4.x und anschließend auf Version 5 upgraden. Es gibt teilweise Probleme beim Upgrade von ESXi 4.0 Update 2: Installieren Sie Update 3 vor dem Upgrade auf 5 oder installieren Sie neu.

Booten Sie Ihren alten ESX Server mit der neuen Version, sollten Sie eine Meldung wie in Abbildung 13-7 sehen, die Ihnen maximal drei von vier Möglichkeiten bietet:

- **FORCE MIGRATE ESX, PRESERVE VMFS DATASTORE:** Hier wird das Upgrade von ESX erzwungen, weil Software oder Treiber erkannt wurden, die in der neuen Version nicht mehr unterstützt werden. Sonst lautet die Meldung auch nur Upgrade von ESXi und Behalten der VMFS-Partition.
- **INSTALL ESXi, PRESERVE VMFS DATASTORE:** ESXi wird installiert, aber nicht aktualisiert, und die Daten auf dem VMFS-Volume bleiben erhalten.

- **INSTALL ESXi, OVERWRITE VMFS DATASTORE:** ESXi wird installiert, aber nicht aktualisiert, und die Daten auf dem VMFS-Volumen werden überschrieben.

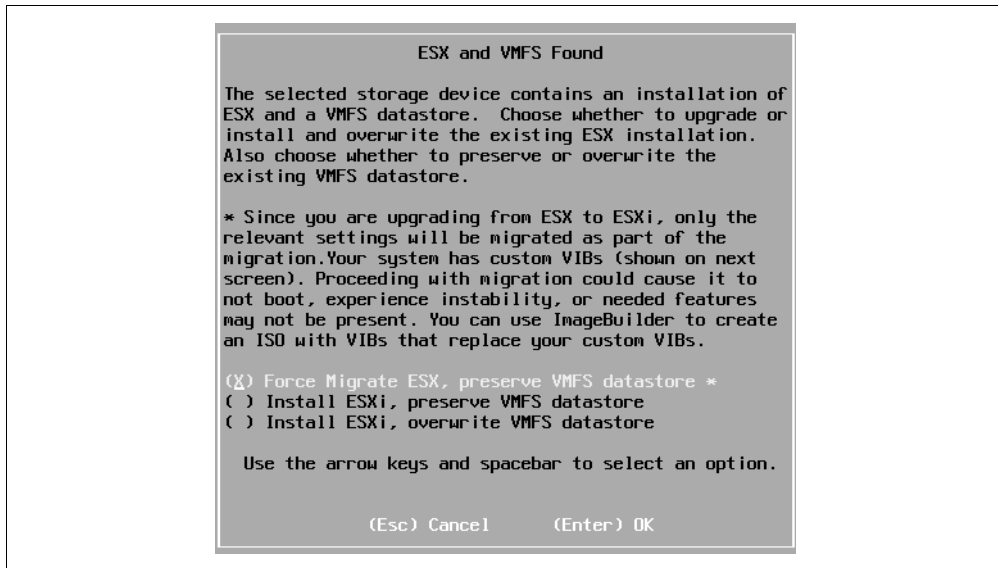


Abbildung 13-7: Meldung beim Upgrade eines Hosts

Nach einer recht kurzen Zeit ist der Vorgang erledigt und Sie können die Bootreihenfolge wieder umstellen, um den Host mit der neuen Version zu starten.

Bei einem Upgrade von ESX auf ESXi werden anschließend natürlich nicht alle bestehenden Funktionen aktualisiert, weil es z.B. unter der Variante mit dem »i« nicht alles das gibt, was der vorige ESX hatte. Auch werden z.B. manuelle Änderungen zur Authentifizierung im Ordner `/etc/pam.d/` auf Standardwerte zurückgesetzt und die Einstellungen zum SSH-Zugriff deaktiviert.

Überprüfen Sie anschließend über den vSphere Client die Netzwerkeinstellungen. Die ehemalige Servicekonsole mit der ihr zugewiesenen Netzwerkkarte wird meist richtig als Management Network übernommen. Die vSwitches mit 64 Ports werden in solche mit 128 Anschlüssen gewandelt. Schauen Sie nach, ob Sie das so wollen oder lieber manuell zurückändern möchten. Achten Sie auch darauf, ob eventuelle DHCP-Adressen noch denselben Wert haben. Da es beim neuen Hypervisor nur noch ein Standardgateway gibt, müssen Sie dieses eventuell anpassen. Beachten Sie dabei die Hinweise zur Netzwerktechnik in Kapitel 6 und zur Einstellung für HA in Kapitel 11. Bei Problemen mit HA ziehen Sie bitte auch Kapitel 18 zurate. Dort werden die meisten zusätzlich möglichen Optionen besprochen. Sollten Sie einen ausfallsicheren vSwitch mit passiven und aktiven Adaptern installiert haben (wie in Kapitel 6 empfohlen wurde), müssen Sie einen Teil der Konfiguration manuell wiederherstellen – das kann der Upgradeprozess nicht korrekt.



Kontrollieren Sie auch die Storage-Zugriffe (NFS-Einstellungen werden meistens übernommen, iSCSI Zugriffe nicht), Uhrzeit- und DNS-Einstellungen, die Startreihenfolge der VMs sowie ggf. die Authentifizierungsdienste. Hatten Sie vorher weitere manuelle Konfigurationen geändert – z. B. bei der Firewall oder den erweiterten Einstellungen –, sollten Sie auch die überprüfen. Kontrollieren Sie auch die angelegten User und deren Zugehörigkeiten zu Gruppen und Passwörter. Beim User *root* funktioniert die Migration üblicherweise problemlos – es sei denn, sein Passwort ist länger als acht Zeichen (siehe unten).

Ressourcenpools müssen nach einem Upgrade ebenfalls überprüft werden. Hatten Sie fast alle Ressourcen an VMs verteilt, kann es sein, dass die neuen Funktionen von ESXi 5 einen Start der beteiligten virtuellen Maschinen verhindern.

Bei einer Neuinstallation der 5er-Version wird das GPT-Partitionsprinzip angewendet, bei einem Upgrade bleibt es bei der herkömmlichen Art und wird nicht neu geschrieben. Auch bleibt die VMFS-Partition in der Version 3. Über den vSphere Client können Sie diese im laufenden Betrieb ohne Probleme auf die VMFS-Version 5 upgraden. Manuell erstellte zusätzliche Laufwerke sind nach dem Upgrade weg, die alten Daten ebenfalls. Das Gleiche passiert mit dem Bootlaufwerk, wenn es nicht zusätzlich eine VMFS-Partition enthält.

War Ihr Passwort für den User *root* länger als acht Zeichen, wird es abgeschnitten. Sie können es über die direkte Konsole wieder neu setzen. Achten Sie aber dabei auf die Tastatureinstellungen, die ggf. ebenfalls nicht übernommen wurden.

Nach dem Upgrade durch Neuinstallation (sonst nicht) haben Sie eine erneute Testphase von 60 Tagen. Vergessen Sie nicht, vor Ablauf dieser Frist die Lizenz einzugeben.

## Upgrade einer vSphere-Umgebung

Besitzen Sie eine komplette Umgebung mit mehreren ESX(i) Hosts und einem vCenter Server, dann können Sie den Update Manager auch für das Upgraden Ihrer Umgebung verwenden. Der Manager kann aber keinen vCenter Server oder die auf ihm laufenden zusätzlichen Dienste upgraden. Das manuelle Erneuern der Umgebung ist natürlich auch möglich.

Um eine komplette Umgebung auf den neuesten Stand zu bringen, empfehle ich, erst den vSphere Client, dann den vCenter Server und anschließend die Hosts upzugraden.

Den vSphere Client auf die neue Version zu hieven, ist recht simpel: Holen Sie sich die ausführbare Datei von der Seite von VMware und führen Sie sie aus. Alle Einstellungen werden üblicherweise von Version 4.1 übernommen, nicht von vorigen Versionen. Die ausführbare Datei finden Sie auch auf der CD oder dem ISO-Image des vCenter Servers.

Ein Upgrade des Virtual Infrastructure Servers ist nicht möglich, da dieser nur auf einem 32-Bit-Betriebssystem lief und der neue nur auf einem 64-Bit-OS. Liegt die Version 4.1 vor, ist ein Upgrade fast immer möglich, es muss nur ein in der neuen Version unterstütz-

tes Windows sein (kein Windows XP 64 Bit). Aber vielleicht entscheiden Sie sich ja auch für die vCenter Server Appliance auf Linux-Basis?

Ein Management Server der Versionen vor 4.1 muss also neu installiert werden. Die Daten der Datenbank können aber anschließend bei Bedarf auf den neuen migriert werden, egal ob eine externe oder die zum Lieferumfang gehörende Datenbank genutzt wurde.

Da der Upgradeprozess genauso vonstatten geht wie die Installation, die in Kapitel 10 detailliert beschrieben wurde, verzichte ich hier auf weitere Angaben. Der Assistent leitet Sie durch alle Optionen und gibt genug Hinweise für ein gutes Gelingen.



Beachten Sie aber, dass das Load-Balancing über DRS (Distributed Resource Scheduler) während dieser Zeit nicht funktioniert. HA läuft allein zwischen den ESX(i) Servern und wird durch den Upgradeprozess nicht behindert. Auch die VMs bekommen von dem Prozess nichts mit.

Haben Sie Guided Consolidation installiert, muss es vor dem Upgrade manuell deinstalliert werden.

Haben Sie den vCenter Server auf die neue Version aktualisiert, müssen Sie ggf. noch die weiteren Dienste wie den Update Manager ebenfalls aktualisieren. Nachdem Sie damit fertig sind, können Sie sich um die Hosts kümmern: Diese können nach dem obigen Schema »Upgrade eines ESX Hosts« oder mit dem neuen Update Manager auf die neue Version gebracht werden. Beachten Sie, dass auch Hosts der Version 3 und 4 in einem Cluster laufen können.



Vergessen Sie nicht, das neue Plugin für den Update Manager auf dem vSphere Client zu installieren.

Da Sie jetzt auch für den vCenter Server bei Neuinstallation 60 Tage lang den Evaluierungsmodus haben, können Sie z. B. einen Host mit Version 5.0 neu installieren und wie gewünscht konfigurieren und dann die in Kapitel 11 beschriebenen Hostprofile für die weiteren Server nutzen. Damit haben Sie sauber installierte ESXi Hosts und können bei Bedarf Ihre bisherige Konfiguration neu überdenken und in das Profil einfließen lassen. Haben Sie beim vCenter Server ein »Inplace Update« gemacht, müssen Sie die neue Lizenz einspielen, da die alte dann abgelaufen ist. Eventuell können Sie dann keine Hostprofile nutzen.

## ESX Upgrade mit Update Manger

Um einen ESX(i) Host der Version 4.x mit dem Update Manager 5.0 auf die neue Version zu aktualisieren, benötigen Sie zunächst das ISO-Image des ESXi 5.0 Servers. Dieses kann von der Website von VMware heruntergeladen werden und trägt den Namen *VMware-VMvisor-Installer-5.0.0-**<Build-Nummer>**.x86\_64.iso*.

1. Klicken Sie im vSphere Client (mit aktiviertem Update Manager-Plugin) unter HOME auf UPDATE MANAGER.
2. Wählen Sie die Registerkarte ESXi-IMAGES aus.
3. Oben rechts befindet sich der Link (in blau) ESXi-IMAGES IMPORTIEREN. Klicken Sie ihn an.
4. Über die Schaltfläche DURCHSUCHEN können Sie im folgenden Browser das ISO-Image auswählen und hochladen. Sie können jetzt schon eine neue Baseline erstellen oder im Anschluss (siehe Punkt 6).
5. Wenn das Image in der Liste der importierten Images erscheint, klicken Sie auf die Registerkarte BASELINES UND GRUPPEN.
6. Haben Sie schon beim Importieren eine Baseline für das Upgrade erstellt, sollte diese hier erscheinen – wenn nicht, klicken Sie links auf den blauen Link ERSTELLEN.
7. Vergeben Sie in dem Fenster einen aussagekräftigen Namen für die Upgrade-Baseline und klicken im unteren Teil den Kreis bei HOST-UGRADE an.
8. Wählen Sie im nächsten Fenster das importierte Image aus und klicken Sie auf WEITER und anschließend auf BEENDEN.

Die gerade erstellte Baseline können Sie nun einem alten ESX(i) Host anhängen, um diesen auf die aktuelle Version zu bringen. Gehen Sie dazu über HOME → HOSTS UND CLUSTER auf den ersten Host, den Sie aktualisieren wollen.

1. Wählen Sie die Registerkarte UPDATE MANAGER aus und klicken Sie auf den blauen Link ANHÄNGEN.
2. Wählen Sie die gerade erstellte Upgrade-Baseline aus und klicken Sie auf ANHÄNGEN.
3. In dem Fenster unter ANGEHÄNGTE BASELINES sollte sie jetzt zu sehen sein.  
Der Host wird beim Aktualisieren automatisch in den Wartungsmodus versetzt. Wenn Sie die auf ihm laufenden VMs manuell verschieben oder herunterfahren müssen, sollten Sie das jetzt zuerst tun und anschließend bei Punkt 4 weitermachen.
4. Beim ersten zu aktualisierenden Host sollten Sie zunächst den Link PRÜFEN verwenden. Wählen Sie beim Assistenten die Schaltfläche UPGRADES aus und deaktivieren Sie ggf. die Schaltfläche PATCHES UND ERWEITERUNGEN (siehe Abbildung 13-8).
5. Nachdem Sie im Fenster auf die Schaltfläche PRÜFEN geklickt haben, schließt es sich und der Host wird bezüglich des Upgrades geprüft.
6. Wenn im unteren Teil des Bildschirms unter KÜRZLICH BEARBEITETE AUFGABEN der Job erledigt ist, sollten Sie auf der Registerkarte UPDATE MANAGER die Ergebnisse sehen.
7. Nun können Sie auf die Schaltfläche STANDARDISIEREN (auf den neuesten Stand bringen) klicken. Füllen Sie in den folgenden Fenstern das Nötige aus bzw. klicken Sie das Gewünschte an. Überlegen Sie sich, ob der Vorgang sofort starten soll oder Sie eine geplante Aufgabe daraus machen möchten.

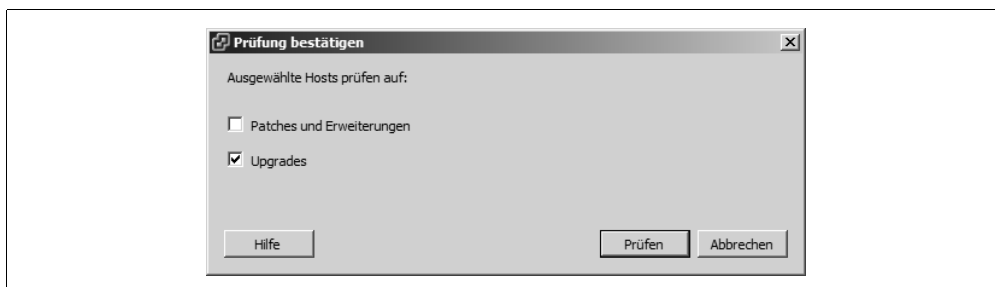


Abbildung 13-8: Prüfen auf Upgrades

8. Deaktivieren Sie ggf. die Funktionen in Ihrem Cluster, die eine Störung oder einen Alarm auslösen könnten (wie DPM, HA, FT usw.).
9. Klicken Sie auf BEENDEN.

Wenn die Standardisierung anfängt, wird der Server zunächst in den Wartungsmodus gefahren und ggf. alle VMs auf die anderen Hosts verschoben. Dann beginnt die Installation – der ESXi Server wird neu gestartet, überprüft die Aktualisierung und kommt automatisch aus dem Wartungsmodus heraus. Ggf. müssen Sie den neuen ESXi Server (über das Kontextmenü auf dem Host) mit dem vCenter Server neu verbinden.

Anschließend sollten Sie die bereits oben unter »Upgrade eines ESX Hosts« beschriebenen Funktionen und Einstellungen überprüfen.

Ist alles so, wie Sie es brauchen, können Sie den nächsten Server freiräumen, ihm die erstellte Upgrade-Baseline anhängen, prüfen und dann STANDARDISIEREN wählen. Haben Sie alle Hosts auf den neuesten Stand gebracht, können Sie die Storages aktualisieren und sich mit den neuen Funktionen vertraut machen. Denken Sie daran, Ihre Lizenzen rechtzeitig einzuspielen und die VMs bei Gelegenheit ebenfalls zu aktualisieren (siehe nächster Abschnitt).



Überprüfen Sie nach dem Upgrade die Ressourceneinstellungen der VMs. Gerade beim Arbeitsspeicher tauchen plötzlich etliche ungewollte Begrenzungen auf!

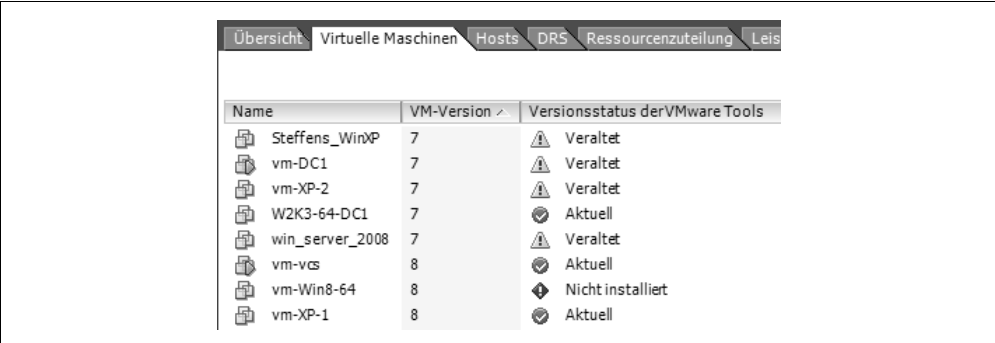
## Upgrade der VMs

Um die virtuellen Maschinen kompatibel mit dem neuen ESXi Server zu machen und alle neuen Funktionen nutzen zu können (z.B. mehr Prozessoren und Arbeitsspeicher), empfehlen VMware und auch ich, die VMs ebenfalls auf die aktuelle Hardwareversion 8 zu bringen. Eine ältere Hardwareversion als 8 ist kein kritischer Zustand – Sie können sich also Zeit damit lassen und es in Ruhe planen. Dabei gibt es wieder zwei Möglichkeiten: erstens, die VMs manuell nach und nach erneuern, und zweitens, die VMs über den Update Manager zu aktualisieren. Auf beide werde ich im Folgenden eingehen.

## Upgrade einer einzelnen VM

Es ist sehr wichtig, dass vor dem Upgrade der Hardwareversion die aktuellen VMware Tools in der virtuellen Maschine installiert wurden. Das können Sie überprüfen, indem Sie in der Bestandsliste auf eine VM klicken und auf der Registerkarte ÜBERSICHT der VM den Status der Tools ansehen. Mit dem ESXi 5.0 werden gleichzeitig neue VMware Tools zur Verfügung gestellt. Sind diese installiert, steht in der Anzeige WIRD AUSGEFÜHRT (AKTUELL). Ist das nicht der Fall, wird auf eine veraltete Version mit WIRD AUSGEFÜHRT (VERALTET) hingewiesen oder der Eintrag lautet LÄUFT NICHT (NICHT INSTALLIERT).

Um bei vielen VMs eine Übersicht über den Status der VMware Tools zu bekommen, können Sie im Cluster auf die Registerkarte VIRTUELLE MASCHINEN klicken und dort ggf. über das Kontextmenü auf einen Spaltenkopf die Spalten VM-VERSION und VERSIONSSTATUS DER VMWARE TOOLS einblenden (siehe Abbildung 13-9). Die Liste können Sie mit einem Klick auf den jeweiligen Spaltenkopf nach dem gewünschten Eintrag sortieren.



| Übersicht Virtuelle Maschinen Hosts DRS Ressourcenzuteilung Leis |            |                                 |
|------------------------------------------------------------------|------------|---------------------------------|
| Name                                                             | VM-Version | Versionsstatus der VMware Tools |
| Steffens_WinXP                                                   | 7          | Veraltet                        |
| vm-DC1                                                           | 7          | Veraltet                        |
| vm-XP-2                                                          | 7          | Veraltet                        |
| W2K3-64-DC1                                                      | 7          | Aktuell                         |
| win_server_2008                                                  | 7          | Veraltet                        |
| vm-vc8                                                           | 8          | Aktuell                         |
| vm-Win8-64                                                       | 8          | Nicht installiert               |
| vm-XP-1                                                          | 8          | Aktuell                         |

Abbildung 13-9: Status und Version der VMware Tools

Das Updaten der Tools und Treiber läuft genau ab wie die Erstinstallation, die in Kapitel 4 ausführlich behandelt wurde. Denken Sie daran, dass die VM nach der Aktualisierung neu gestartet werden muss. Führen Sie den Neustart aus und warten Sie, bis die neue Version der Tools neben der Uhr (bei Windows-Systemen) korrekt angezeigt wird. Fahren Sie den Rechner anschließend herunter und schalten Sie ihn aus.

Sollten Sie ein Linux-System mit den VMware Tools aktualisieren, werden neue Netzwerkmodule zur Verfügung gestellt. Diese können aber erst nach dem Neustart verwendet werden. Sie haben natürlich auch die Möglichkeit, die alten Netzwerkmodule von VMware manuell zu entladen und dann die aktuellen zu laden. Aber für das Upgraden der Hardware muss die Maschine trotzdem ausgeschaltet werden.

Klicken Sie mit der rechten Maustaste auf den ausgeschalteten Computer und wählen Sie aus dem Kontextmenü den Eintrag UPGRADE VIRTUELLER HARDWARE DURCHFÜHREN. Auf Host- oder Clusterebene können Sie auch mehrere VMs mit der Strg-Taste für das Upgrade auswählen.



Die Hardwareversion 8 wird nicht auf Hosts der Version 4.x unterstützt, die aktualisierte Version der VMware Tools aber sehr wohl.

## Hardware-Upgrade über den Update Manager

Mit dem Update Manager haben Sie die Möglichkeit, viele VMs mit der aktuellen Version der VMware Tools zu betanken und anschließend das Hardware-Upgrade durchzuführen zu lassen. Der Vorgang ähnelt dem Upgrade des ESX(i) Hosts, das oben in diesem Kapitel besprochen wurde – deshalb hier nur die Kurzform für die VMs:

1. Klicken Sie auf der Registerkarte BASELINES UND GRUPPEN beim Update Manager die Schaltfläche VMS/VAS an. Dort sind bereits drei vordefinierte Baselines für die virtuellen Maschinen und Appliances angelegt. Diese können Sie nicht verändern.
2. Im rechten Fenster kann eine Gruppe für die vordefinierten Baselines erstellt werden. Dazu wählen Sie rechts den Link ERSTELLEN aus.
3. Im folgenden Fenster wird zunächst ein Name für die Gruppe vergeben.
4. Anschließend sollten die Einträge für VM-HARDWARE-UPGRADES und UPGRADES VON VMWARE TOOLS ausgewählt werden.

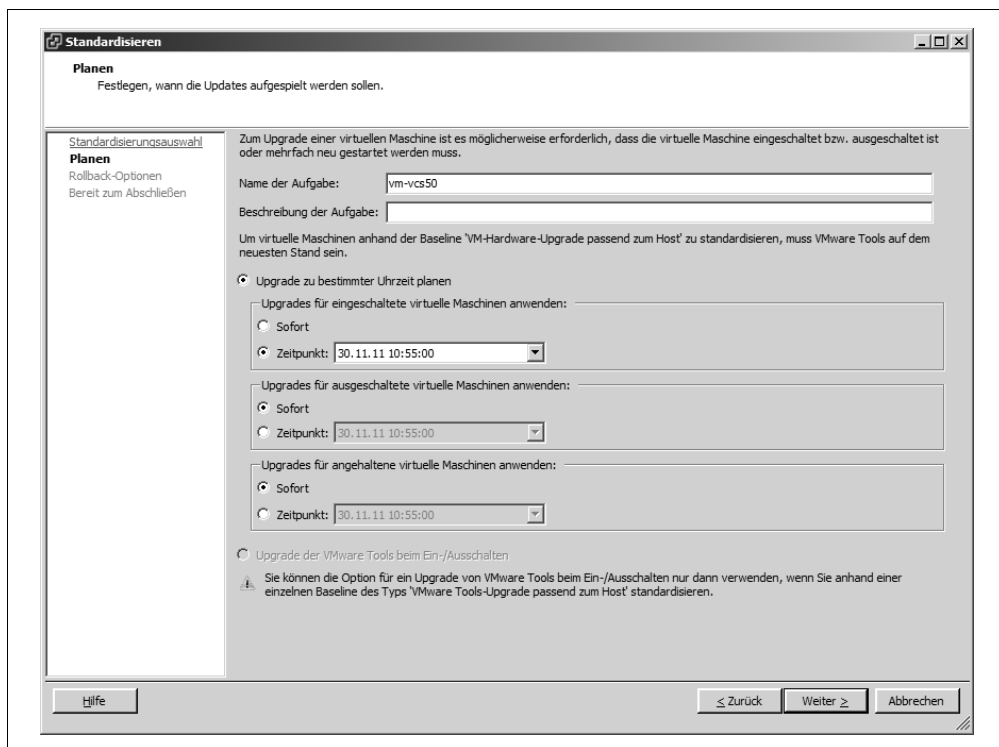


Abbildung 13-10: HW-Upgrade der VMs

5. Nachdem auf BEENDEN geklickt wurde, erscheint die Baseline-Gruppe im rechten Fenster.
6. Navigieren Sie über HOME zu VMS UND VORLAGEN und wählen Sie dort das Data-center aus.
7. Auf der Registerkarte UPDATE MANAGER kann die neue Baseline-Gruppe angehängt werden.
8. Im unteren Teil des Fensters erscheinen alle VMs, die anschließend überprüft und bei Bedarf auf den neuesten Stand gebracht werden können.

Sie haben mit diesem Werkzeug die Möglichkeit, eine einzelne oder viele VMs gleichzeitig upzudaten. Für dieses Vorhaben sollten Sie sich aber ein Zeitfenster aussuchen, indem die virtuellen Maschinen nicht zur Verfügung stehen müssen. Planen Sie deshalb sorgfältig. Eine einzelne Windows-VM muss bei diesem Vorgehen dreimal neu gestartet werden, Linux-Maschinen nur einmal.

Sie haben mit diesem Werkzeug die Möglichkeit, eine einzelne oder viele VMs gleichzeitig upzudaten, wie in Abbildung 13-10 gezeigt wird. Für dieses Vorhaben sollten Sie sich aber ein Zeitfenster aussuchen, in dem die virtuellen Maschinen nicht zur Verfügung stehen müssen. Planen Sie deshalb sorgfältig. Eine einzelne Windows VM muss bei diesem Vorgehen drei Mal neu gestartet werden, Linux Maschinen nur einmal.

## VMFS-Upgrade

Haben Sie Ihre komplette Umgebung auf die neue Version gehoben, können Sie als Letztes noch die Storages von VMFS 3 auf 5 aktualisieren. Das kann im laufenden Betrieb geschehen, d.h. Sie müssen weder die Festplatten leer räumen noch die virtuellen Maschinen herunterfahren.

Am Besten erledigen Sie das über HOME → DATENSPEICHER UND DATENSPEICHERCLUSTER, wählen sich einen Storage aus und klicken auf die Registerkarte KONFIGURATION und dann auf der rechten Seite des Fensters auf den blauen Link UPGRADE AUF VMFS-5. Die Überprüfung wird dann in einem extra Fenster angezeigt, wie Abbildung 13-11 zeigt.

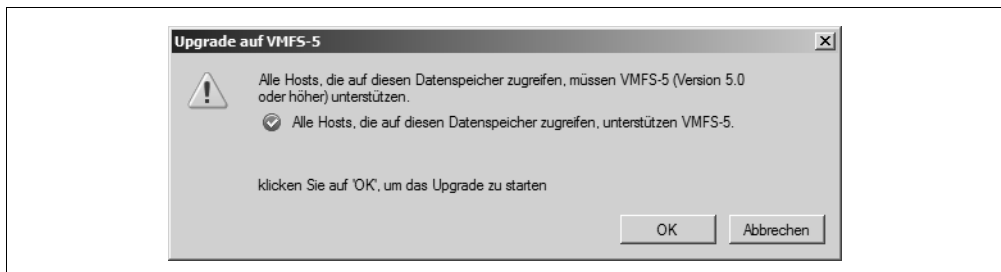


Abbildung 13-11: VMFS-Storage aktualisieren.

Jetzt fehlen nur noch die korrekte Konfiguration der Umgebung, die ich in Kapitel 15 ausführlich beschreibe und eine vernünftige Datensicherung (siehe Kapitel 16). Im nächsten Kapitel geht es um die Templates (Vorlagen von VMs) und zum Schluss nochmals um die Optimierung.



---

# Templates (Vorlagen für virtuelle Maschinen)

Mit Vorlagen, sogenannten Templates, kann man schnell neue virtuelle Maschinen erstellen und automatisch mit einer Anpassungsspezifikation multiplizieren. Dabei bekommen Sie über die Anpassung eine neue SID, einen neuen Namen und ggf. weitere individuelle Einstellungen übergeben. Auch wenn eine produktive VM durch Viren, Trojaner oder Ähnliches geschädigt ist, kann eine neue VM durch ein Template bereitgestellt und die Datensicherung zurückgespielt werden. Diese Funktion ist im vCenter Server für jede virtuelle Maschine bereits enthalten, Sie brauchen also keine weitere Software eines anderen Anbieters.

## Templates und ihr Nutzen

Templates sind Vorlagen von virtuellen Maschinen, aus denen man sehr zeitsparend neue VMs erstellen kann. Diese können nicht gestartet oder geändert werden – Sie müssen sie erst wieder in eine VM konvertieren, um z.B. ein Update oder einen Servicepack einzuspielen.

Bei so einer Vorlage sollte man sich große Mühe geben, um Fehler zu vermeiden, die sich dann auf jede daraus erstellte Maschine auswirken.

Vorgehensweise:

- Installation des Betriebssystems
- Installation aller notwendigen Treiber und VMware Tools
- Installation von Servicepacks, Patches und Hotfixes
- evtl. Löschen der Auslagerungsdatei, Defragmentierung der Festplatte und Setzen der Auslagerungsdatei auf einen festen Wert
- gegebenenfalls Installieren der Anwendungen
- Anonymisierung durch Sysprep oder NewSid

- Herunterfahren des Systems
- Konvertieren der VM in ein Template

Bei physischen Systemen kann man den Vorgang mit *Symantec Ghost* oder *Acronis Backup & Recovery* durchführen. Um individuelle Einstellungen für den Klon zu bekommen, kann bei Microsoft-Betriebssystemen das Tool *Sysprep* benutzt werden. Auch das ursprünglich aus dem Hause Sysinternals stammende *NewSID* (jetzt Microsoft) ist für solche Duplizierungen geeignet. Nachteilig bei diesem Verfahren ist die Hardwareabhängigkeit des Image: Nur bei identischer Hardware kann man sicher sein, dass der Rechner hinterher auch startet. Eine virtuelle Maschine sieht aber immer die gleiche Hardware, deshalb ist es in der virtuellen Welt ohne Probleme oder vorheriges Impfen mit allen erdenklichen Treibern möglich, VMs beliebig oft zu duplizieren.

Wenn Sie einen Snapshot einer VM erstellt haben, können Sie sogar im laufenden Betrieb die Festplattendatei der Maschine über den Datastore-Browser an einen anderen Ort kopieren und damit eine neue VM generieren – die oben erwähnten Tools sollten Sie anschließend jedoch zum Einsatz bringen.



Trennen Sie möglichst die System- und Datenpartition einer VM, um hier flexibler zu sein. Damit könnten Sie auch viele verschiedene Betriebssystemvorlagen besser nutzen. Dieser Vorgang lässt sich sogar noch mithilfe von geplanten Tasks automatisieren und z.B. nachts erledigen.

Auch für eine Disaster Recovery kann man vorgefertigte Disks oder ganze VM-Vorlagen nutzen, um schnell wieder den gewünschten Zustand der Maschine zu erhalten. Das ist bei physischen Systemen meistens nicht möglich.

Wenn Sie Microsoft-Betriebssysteme vor Windows Vista einsetzen (also bis einschließlich Server 2003), können Sie die Sysprep-Tools beim vCenter Server hinterlegen und die VMs damit anonymisieren. Nachdem Sysprep den Rechner heruntergefahren hat, können Sie daraus eine Vorlage erstellen.

Auch auf einem Linux-System können Sie derartige Vorgänge durchführen, wie Abbildung 14-1 zeigt. Die dazu notwendigen Dateien bringt der vCenter Server für die gängigsten Distributionen bereits mit. Falls Sie ein System einsetzen, das nicht unterstützt wird, achten Sie auf die Netzwerkeinstellungen (die MAC-Adresse ändert sich automatisch) und den Namen, der im Netzwerk vielleicht schon bekannt ist.

Damit ist die Erstellung schon abgeschlossen, und Ihnen steht ein funktionstüchtiges Template zur Verfügung. Die meisten manuellen Eingriffe nimmt Ihnen der VMware vCenter Server ab, bzw. er führt Sie mithilfe eines Assistenten durch die notwendigen Schritte. Ein weiterer Vorteil des vCenter Servers zeigt sich darin, dass Sie sich nicht um das Format der Festplattendateien kümmern müssen, was bei einem manuellen Eingriff sehr wohl der Fall sein kann.

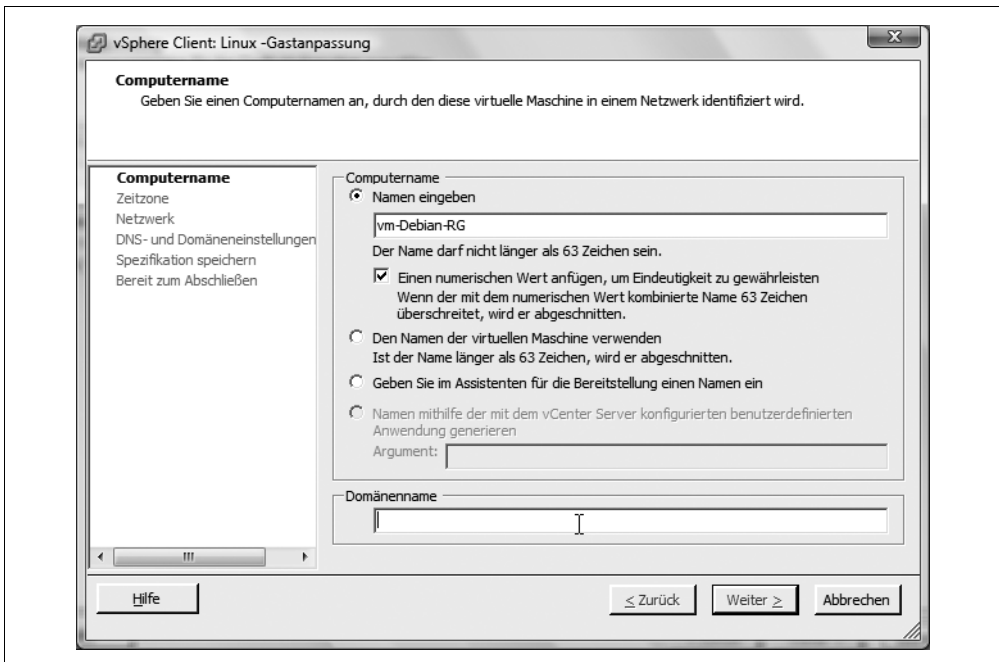


Abbildung 14-1: Linux-Gastanpassung

## Format der Festplattendateien

Unter VMware ESXi können Festplattendateien einer virtuellen Maschine nur auf VMFS-Partitionen und damit im monolithischen Format genutzt werden. So ein monolithisches Dateisystem ist für große Dateien und für mehrere konkurrierende Zugriffe optimiert und eignet sich daher ideal als Grundlage für schnelle virtuelle Maschinen. Die Festplatte liegt in einem Stück vor, und es existiert dafür eine Beschreibungsdatei, die Sie allerdings nur auf der Kommandozeile des ESXi Hosts sehen können. Über den Datastore-Browser werden diese Dateien als eine Einheit angezeigt. Beim Verschieben oder Kopieren einer Festplatte über diesen Browser werden automatisch beide Dateien verschoben oder kopiert.

Die Festplatten in diesem Format werden entweder mit der maximal möglichen Größe oder im Thin-Format dynamisch wachsend angelegt. Die Größenbegrenzung einer Festplattendatei unter VMware ESXi im monolithischen Format liegt zurzeit bei 2 TByte minus 512 Byte.

Wenn Sie sich so eine Festplatte an die Seite gelegt haben, brauchen Sie nur eine virtuelle Maschine ohne Festplatte zu erstellen, anschließend die beiden `.vmdk`-Dateien über den Datenspeicherbrowser oder die Kommandozeile mit `cp` oder `scp` in den Ordner zu kopie-

ren und die Festplatte der neuen VM hinzuzufügen. Verwenden Sie nicht die Original-festplattendatei, weil sie ja sonst keine Vorlage mehr wäre.

Viel einfacher geht es aber über den vCenter Server: Wie schon oben erwähnt, können Sie eine bereits fertige Linux- oder Windows-VM über die Sysprep-Dateien wie gewünscht klonen.

## Benutzerdefinierte Anpassung des Gast-OS

Wenn Sie eine neue virtuelle Maschine aus einem Template bereitstellen oder eine vorhandene virtuelle Maschine klonen, können Sie das neue Gastbetriebssystem benutzerdefiniert anpassen. Der Assistent zur benutzerdefinierten Anpassung des Gastbetriebssystems führt Sie durch die Konfigurationsoptionen.

Wenn Sie ein Windows-Gastbetriebssystem vor Windows Vista anpassen wollen, müssen Sie die erforderlichen Komponenten, also die Sysprep-Dateien, auf dem vCenter Server hinterlegen.



Nach dem Bereitstellen und benutzerdefinierten Anpassen nicht volumenlizenzierter Versionen von Windows XP oder Windows 2003 müssen Sie das Microsoft-Betriebssystem auf der neuen virtuellen Maschine möglicherweise erneut aktivieren.

## Ein Windows-Gastbetriebssystem anpassen

Der Prozess der benutzerdefinierten Anpassung unterscheidet sich je nach Gast-Betriebssystem, das auf der neuen virtuellen Maschine verwendet werden soll. Ob Sie ein Template bereitstellen oder eine virtuelle Maschine klonen wollen, ist dabei der gleiche Vorgang.

Microsoft bietet die Sysprep-Tools auf den Installations-CD-ROMs für Windows 2000, Windows XP und Windows 2003 an. Beachten Sie, dass es jeweils unterschiedliche Tools für jede Version und gegebenenfalls auch für 32 und 64 Bit gibt. Darüber hinaus kann Sysprep 1.1 für Windows 2000 von der Microsoft-Website bezogen werden.



Die Sysprep-Tools für Vista und Windows 7 mit 32 und 64 Bit und für Server 2008 32 und 64 Bit sowie für 2008 R2 befinden sich im Betriebssystem und müssen nicht extra auf dem vCenter Server installiert werden.

Während der benutzerdefinierten Anpassung sucht der vCenter Server nach dem Sysprep-Paket, das dem betreffenden Gastbetriebssystem entspricht. Wenn die Sysprep-Tools im entsprechenden Betriebssystemverzeichnis nicht gefunden werden, wird vom vCenter Server im unten angegebenen Verzeichnis gesucht. Findet der vCenter Server keine Sysprep-Tools, wird die benutzerdefinierte Anpassung der virtuellen Windows-Maschine nicht fortgesetzt.

## Installation der Sysprep-Tools von Microsoft

1. Laden Sie das Sysprep-Paket für Windows 2000 von dieser Webseite herunter:  
*<http://www.microsoft.com/downloads/details.aspx?FamilyID=0c4bfb06-2824-4d2b-abc1-0e2223133afb>*
2. Klicken Sie zum Fortfahren auf NEXT (WEITER).
3. Klicken Sie auf I AGREE TO ACCEPT THE TERMS AND CONDITIONS (Ich stimme den allgemeinen Bedingungen zu).
4. Klicken Sie auf DOWNLOAD.
5. Speichern Sie die Datei auf der lokalen Festplatte.
6. Führen Sie den Microsoft Installer *Q257813\_w2k\_spl\_x86\_en.exe* aus.
7. Extrahieren Sie die Dateien in das angegebene Verzeichnis, gegebenenfalls mit dem Parameter /x.

Die folgenden leeren Sysprep-Verzeichnisse wurden während des vCenter Installationsvorgangs auf einem Windows Server 2003 hier erstellt:

```
C:\<PROFILFÜRALLEBENUTZER>\Anwendungsdaten\VMware\VMware VirtualCenter\sysprep
... \1.1\
... \2k\
... \xp\
... \xp-64\
... \svr2003\
... \svr2003-64\
```

Dabei steht <PROFILFÜRALLEBENUTZER> normalerweise für *\Dokumente und Einstellungen\Alle Anwender\*. Unter Server 2008 findet man die Unterordner bei *C:\Program-Data\VMware\VMware VirtualCenter\sysprep\*.

8. Wählen Sie das entsprechende Unterverzeichnis aus.
9. Klicken Sie auf OK, um die Dateien zu erweitern.

Nachdem Sie die Dateien in das richtige Verzeichnis extrahiert haben, muss z.B. Folgendes angezeigt werden:

```
... \1.1\docs\
... \1.1\samples\
... \1.1\tools\
... \1.1\contents.txt
```

So installieren Sie die Sysprep-Tools von Microsoft von einer Windows-Betriebssystem-CD:

1. Legen Sie die Windows-Betriebssystem-CD in das CD-ROM-Laufwerk ein (meistens D:).
2. Suchen Sie im CD-Verzeichnis *\Support\Tools* nach der Datei *DEPLOY.CAB*.
3. Öffnen und erweitern Sie die Datei *DEPLOY.CAB* mithilfe eines Tools wie Windows Explorer oder Winzip o. Ä., das Microsoft-CAB-Dateien unterstützt.

4. Extrahieren Sie die Dateien in das entsprechende Verzeichnis für das Sysprep-Gastbetriebssystem.
5. Klicken Sie auf OK, um die Dateien zu erweitern.

Nach dem Extrahieren der Dateien aus *DEPLOY.CAB* wird Folgendes angezeigt:

```
...\\<Gast>\\deptool.chm
...\\<Gast>\\readme.txt
...\\<Gast>\\setupcl.exe
...\\<Gast>\\setupmgr.exe
...\\<Gast>\\setupmgx.dll
...\\<Gast>\\sysprep.exe
...\\<Gast>\\unattend.doc
```

Dabei ist <Gast> entweder 2k, xp oder svr2003, mit jeweils 32 oder 64 Bit.

6. Wiederholen Sie diesen Vorgang, um Sysprep-Dateien für jedes der Windows-Gastbetriebssysteme (Windows 2000, Windows XP oder Windows 2003) zu extrahieren, das mithilfe von vCenter Server benutzerdefiniert angepasst werden soll.

Sie können nun eine neue virtuelle Maschine mit einem unterstützten Windows-Gastbetriebssystem anpassen, wenn Sie eine vorhandene virtuelle Maschine klonen.

Folgende Angaben von benutzerspezifischen Daten sind möglich:

- Endbenutzer-Lizenzvertrag
- Produkt-ID
- Ländereinstellungen
- Benutzername
- Firmenbezeichnung
- Netzwerkkonfiguration
- Angaben, ob der Rechner zu einer Arbeitsgruppe oder Domäne gehört
- Auswahl einer Zeitzone



Mit dem Setup-Assistenten erstellte Konfigurationen können abgespeichert und öfter benutzt werden. Achten Sie darauf, das jeweilige Betriebssystem mit anzugeben.

## Integrierter Assistent

Sie können den Assistenten zur benutzerdefinierten Anpassung des Gastbetriebssystems nicht über ein Menü oder eine Symbolleisteoption starten, sondern nur indirekt über den Assistenten zum Bereitstellen von Templates oder den Assistenten zum Klonen einer virtuellen Maschine.

1. Starten Sie den Assistenten zur benutzerdefinierten Anpassung des Gastbetriebssystems (KLONEN ALS NEUE VIRTUELLE MASCHINE).

2. Geben Sie auf der Seite NAME UND SPEICHERORT den Namen und den Speicherort der virtuellen Maschine ein. Klicken Sie auf WEITER (siehe Abbildung 14-2).

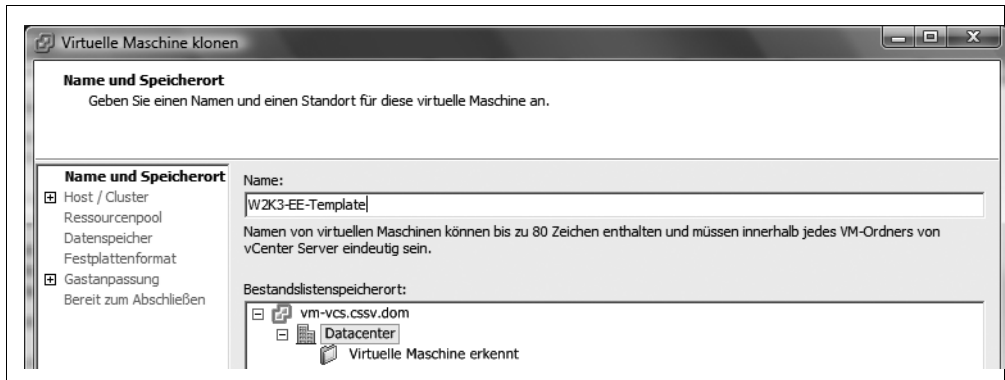


Abbildung 14-2: Assistent zur benutzerdefinierten Anpassung des Gastbetriebssystems

3. Nach der Wahl der Datenablage für die neue Maschine kann die Konfiguration des Anpassungsspezifikations-Assistenten gestartet werden. Sollten Sie das Bild aus Abbildung 14-3 sehen, haben Sie die Sysprep-Dateien nicht im richtigen Ordner platziert.

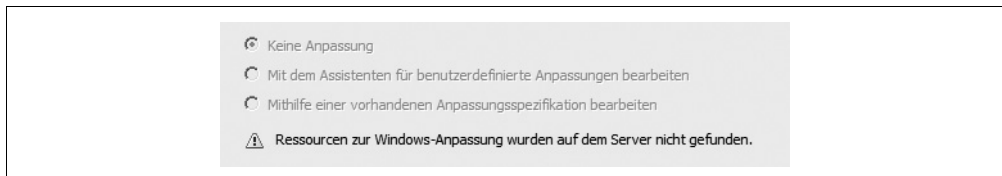


Abbildung 14-3: Keine Sysprep-Dateien für das ausgewählte OS vorhanden

4. Geben Sie auf der Seite REGISTRIERUNGSMITTELSINFORMATIONEN den Namen und das Unternehmen der virtuellen Maschine ein. Klicken Sie auf WEITER.

Diese Angaben sind rein informativ. Sie haben keinen Einfluss auf die Funktionen der virtuellen Maschine. Im Feld NAME (siehe Abbildung 14-4) können Sie den Namen einer Person, eines Anwenders oder einer Anwendergruppe eingeben.

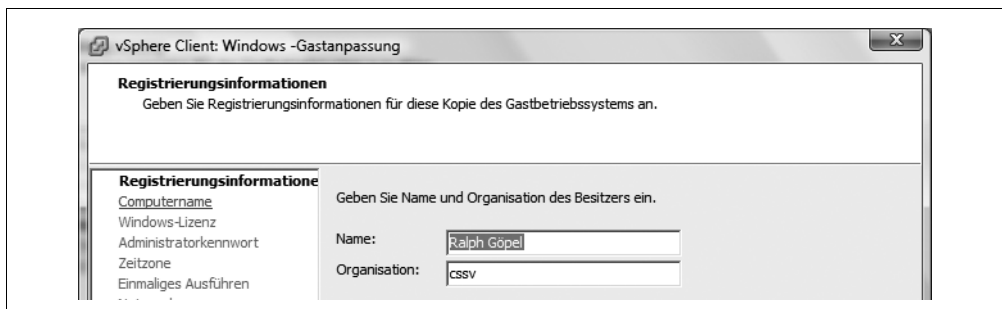


Abbildung 14-4: Individuelle Gastbetriebssystemeinstellungen

5. Geben Sie auf der Seite COMPUTER-NAME den Computernamen für die virtuelle Maschine an. Klicken Sie auf WEITER.

Der Computernamen ist der Name, der an eine bestimmte Instanz eines Gastbetriebssystems vergeben wird. Das Betriebssystem verwendet diesen Namen, um sich selbst im Netzwerk zu identifizieren. In Windows-Systemen wird er als »Computernamen« bezeichnet, in den meisten anderen Betriebssystemen heißt er »Hostname«. Dabei handelt es sich nicht um den Namen der virtuellen Maschine, der zuvor im Assistenten zum Bereitstellen von Templates oder im Assistenten zum Klonen einer virtuellen Maschine angegeben wurde. Sie können den Computernamen folgendermaßen angeben:

- *Indem Sie einen bestimmten Namen zuweisen:* Der Name darf alphanumerische Zeichen, Unterstriche (\_) und Bindestriche (-) enthalten. Er darf keine Punkte (.) oder Leerzeichen enthalten und nicht ausschließlich aus Ziffern bestehen. Um einen mit Sicherheit eindeutigen Namen zu erstellen und somit das Auftreten von Konflikten zu vermeiden, markieren Sie EINEN NUMERISCHEN WERT ANFÜGEN, UM EINDEUTIGKEIT ZU GEWÄHRLEISTEN.
  - *Indem Sie den Namen der virtuellen Maschine verwenden:* Der Computernamen, den VirtualCenter erstellt, ist identisch mit dem Namen der virtuellen Maschine, in der das Gastbetriebssystem ausgeführt wird.
  - *Indem Sie auf Eingabeaufforderungen für einen Namen reagieren:* Der vSphere Client übernimmt für den Assistenten zum Bereitstellen von virtuellen Maschinen eine Eingabeaufforderung für den Computernamen, nachdem Sie alle Schritte im Assistenten abgeschlossen haben.
  - *Indem Sie eine benutzerdefinierte Anwendung zum Erstellen eines Namens verwenden:* Der vSphere Client ruft eine benutzerdefinierte Anwendung auf, die auf dem vCenter Server gespeichert ist, um einen Namen zu erstellen. Wenn Sie diese Option auswählen, müssen Sie den absoluten Pfad der benutzerdefinierten Anwendung im zugehörigen Textfeld eingeben.
6. Geben Sie auf der Seite WINDOWS-LIZENZ den Windows-Lizenzschlüssel für das neue Gastbetriebssystem an (siehe Abbildung 14-5). Klicken Sie auf WEITER.
- Wenn Sie ein Windows Server-Betriebssystem benutzerdefiniert anpassen, markieren Sie den entsprechenden Lizenzmodus: PRO ARBEITSPLATZ oder PRO SERVER. Wenn Sie PRO SERVER auswählen, geben Sie die maximale Anzahl gleichzeitiger Verbindungen an, die der Server akzeptieren soll. Beachten Sie dabei die erworbenen Lizenzen.
7. Geben Sie auf der Seite ADMINISTRATORKENNWORT das Administrator Kennwort für die virtuelle Maschine ein und bestätigen Sie es durch nochmalige Eingabe. Klicken Sie auf WEITER.

Geben Sie kein Kennwort ein, fordert Sie der vSphere Client auf, zu bestätigen, dass Administratorbenutzer kein Kennwort eingeben müssen.



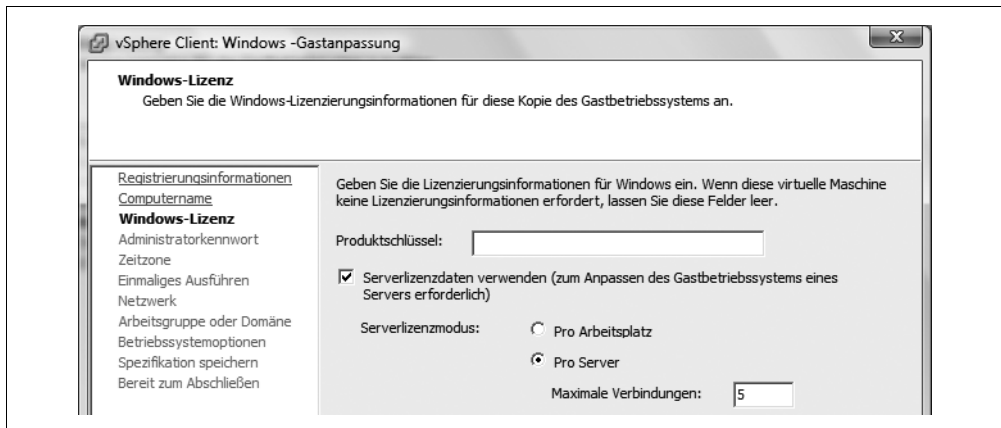


Abbildung 14-5: Eingabe der Produkt-ID und des Lizenzmodus



Wenn Sie ein neues Administratorkennwort angeben und das Template oder die virtuelle Maschine unter Windows, das oder die als Quelle funktioniert, bereits über eines verfügt, müssen Sie in Schritt 13 die Option **ALLE ANWENDERKONTEN LÖSCHEN** markieren. Andernfalls wird das alte Administratorkennwort nicht geändert (nicht immer vorhanden).

- Wenn Sie sich beim Booten der virtuellen Maschine automatisch als Administrator anmelden möchten, wählen Sie **AUTOMATISCH ALS ADMINISTRATOR ANMELDEN** und geben an, wie oft die automatische Anmeldung ausgeführt werden soll. Das ist hilfreich, wenn Sie wissen, dass Sie mehrere Neustarts durchführen werden, bevor sich andere Anwender normal auf der virtuellen Maschine anmelden können.
8. Geben Sie auf der Seite **ZEITZONE** die Zeitzone für die virtuelle Maschine an. Klicken Sie auf **WEITER**.
  9. Geben Sie auf der Seite **EINMALIGES AUSFÜHREN** sämtliche Befehle ein, die Sie im Rahmen des ersten Starts für die neue virtuelle Maschine ausführen möchten. Klicken Sie nach Eingabe eines jeden Befehls auf **HINZUFÜGEN**. Mit den Optionen **LÖSCHEN** und **VERSCHIEBEN** können Sie die Ausführungsreihenfolge für die Befehle erstellen. Wenn die Befehlsliste vollständig ist, klicken Sie auf **WEITER**.
  10. Werden alle Netzwerkschnittstellen der VM automatisch über einen DHCP-Server konfiguriert, markieren Sie auf der Seite **NETZWERK** die Option **NORMAL**. Klicken Sie auf **WEITER**.
  11. Wenn die automatische Konfiguration für Ihre Umgebung nicht geeignet ist, wählen Sie **BENUTZERDEFINIERT** aus, markieren die anzupassende Netzwerkschnittstellenkarte (NIC) und klicken auf **ANPASSEN**, um zusätzliche Spezifikationen vorzunehmen. Das Dialogfeld mit den Netzwerkeigenschaften wird geöffnet.

Nehmen Sie im Dialogfeld mit den NETZWERKEIGENSCHAFTEN die folgenden Schritte vor:

- Wählen Sie auf der Registerkarte ALLGEMEIN aus, ob Sie automatisch eine IP-Adresse über DHCP erhalten möchten, oder geben Sie die IP-Adressen manuell ein. Wählen Sie auch aus, ob Sie automatisch eine DNS-Serveradresse über DHCP erhalten möchten, oder geben Sie die DNS-Serveradressen manuell ein.
- Geben Sie auf der Registerkarte DNS die DNS-Verbindungen an, indem Sie DNS-Suffixe eingeben. Klicken Sie für jedes DNS-Suffix, das Sie eingeben, auf HINZUFÜGEN. Wenn Sie mehrere DNS-Verbindungen hinzufügen, können Sie die Reihenfolge, in der eine virtuelle Maschine die Verbindungen verwenden soll, mit NACH OBEN bzw. NACH UNTEN bestimmen.
- Geben Sie auf der WINS-Registerkarte die primäre und sekundäre WINS-Adresse an, indem Sie die IP-Adressen manuell in die Eingabefelder eingeben.
- Klicken Sie auf OK, um zum vorigen Dialogfeld zurückzukehren. Klicken Sie im Dialogfeld BENUTZERDEFINIERT ANPASSUNGEN DES NETZWERKS auf WEITER.

12. Führen Sie auf der Seite ARBEITSGRUPPE ODER DOMÄNE folgende Schritte durch:

- Wenn Sie einer Arbeitsgruppe beitreten möchten, wählen Sie ARBEITSGRUPPE aus, geben den Namen der Arbeitsgruppe ein und klicken auf WEITER.
- Möchten Sie einer Domäne beitreten, wählen Sie WINDOWS-SERVER-DOMÄNE aus, geben den Användernamen und das Kennwort eines Anwenders an, der Computer zur Windows-Domäne hinzufügen darf (meistens des Administrators), und klicken auf WEITER.

13. Wählen Sie auf der Seite BETRIEBSSYSTEMOPTIONEN die folgenden Optionen für das Gastbetriebssystem aus:

- NEUE SICHERHEITS-ID (SID) ERZEUGEN – Erzeugt eine neue Sicherheits-ID für die virtuelle Maschine (siehe Abbildung 14-6).

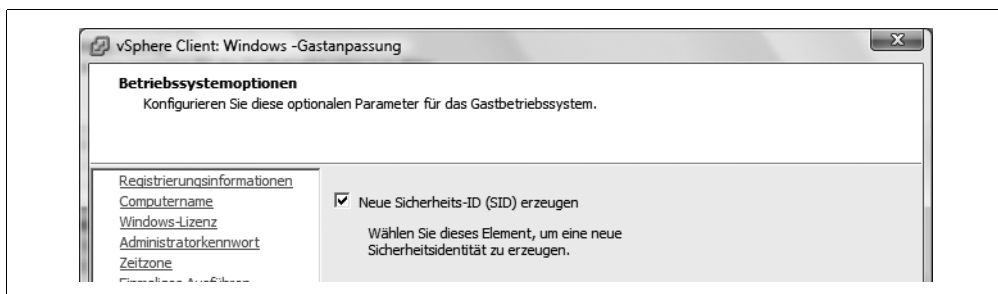


Abbildung 14-6: Neue Sicherheits-ID erzeugen

- ALLE ANWENDERKONTEN LÖSCHEN – Löscht alle alten Anwenderkonten, die im System gefunden werden. Wenn Sie in Schritt 5 ein neues Administratorkennwort angegeben haben und das Template oder die virtuelle Maschine unter Win-

dows, das bzw. die als Quelle fungiert, bereits über eines verfügt, müssen Sie jetzt die Option ALLE ANWENDERKONTEN LÖSCHEN markieren. Andernfalls wird das alte Administratorkennwort nicht geändert. Klicken Sie auf WEITER.



Der Punkt ALLE ANWENDERKONTEN LÖSCHEN ist nicht in allen Sysprep-Varianten vorhanden.

14. Optional: Führen Sie die folgenden Schritte aus, um auf der Seite SPEZIFIKATION SPEICHERN die benutzerdefinierten Optionen als XML-Datei zu speichern.

- Wählen Sie DIESE SPEZIFIKATIONEN DER BENUTZERSPEZIFISCHEN ANPASSUNG ZUR SPÄTEREN VERWENDUNG SPEICHERN aus.
- Geben Sie den Pfad und den Dateinamen für die Spezifikation an und klicken Sie auf WEITER.

Der vCenter Server speichert die benutzerdefinierten Konfigurationsparameter in einer XML-Datei. Später können Sie diese vordefinierten benutzerspezifischen Parameter importieren, wenn Sie ein Template bereitstellen oder eine vorhandene virtuelle Maschine klonen. Wenn die benutzerspezifischen Einstellungen in einer Datei gespeichert sind, werden das Administratorkennwort der virtuellen Maschine unter Windows und das Kennwort des Administrators der Domäne gegebenenfalls in verschlüsseltem Format in der XML-Datei gespeichert. Die gespeicherten Dateien für die benutzerdefinierte Anpassung sind wegen der Verschlüsselung für jeden vCenter Server und für jede Version von vSphere5 eindeutig. Sie müssen die Dateien für die benutzerdefinierte Anpassung für jeden vCenter Server neu erstellen. Die Verschlüsselung wird zwischen Upgrade-Versionen auf demselben vCenter Server beibehalten – das heißt, dass Sie nach dem Upgrade des vCenter Servers dieselben Dateien verwenden können.

15. Klicken Sie auf BEENDEN.

Das schließt den Assistenten zur benutzerdefinierten Anpassung des Gastbetriebssystems und kehrt zurück zum Assistenten zum Bereitstellen von Templates oder zum Assistenten zum Klonen einer virtuellen Maschine.

16. Klicken Sie auf BEENDEN, um die virtuelle Maschine aus einem Template bereitzustellen oder den Klon zu erstellen.



Wenn Sie den Klon das erste Mal starten, fährt die Maschine zunächst ganz normal hoch und der Anmeldebildschirm wird angezeigt. Erst nach einer kurzen Zeitspanne beginnt im Hintergrund die Arbeit, die VM wird neu gestartet, und die Gastanpassung wird durchgeführt. Haben Sie also Geduld und melden Sie sich nicht sofort an.



---

# vCenter Server – Konfiguration und Alarme

Die Konfiguration des vCenter Servers ist eine wichtige Angelegenheit, bei der einige Einstellungen zum Verhalten der gesamten Umgebung angepasst oder neu konfiguriert werden müssen. In diesem Kapitel gehe ich auf die Besonderheiten und die damit verbundenen Möglichkeiten ein. In verschiedenen Gruppen von Dialogfeldern mit Eigenschaften und Einstellungen können Sie Anpassungen vornehmen.

Logisch hängen die Alarme des Systems von den Einstellungen des vCenter Servers ab, z. B. wenn E-Mails verschickt werden sollen. Die Alarme werden im zweiten Teil dieses Kapitels behandelt.

## Einstellungen des vCenter Servers

Über HOME → vCENTER SERVER EINSTELLUNGEN gelangen Sie zur Konfiguration der vCenter-Umgebung, die zentral in einem Fenster angeboten wird.

Änderungen an diesen Einstellungen werden nur auf den aktuellen vCenter Server angewendet. Wenn Sie sich abmelden und bei einem anderen vCenter Server anmelden, gelten diese Einstellungen nicht für diesen Server, auch nicht für Server im verknüpften Modus.

Auf den im Dialogfeld angezeigten Registerkarten können Sie folgende Konfigurationen vornehmen:

- *Lizenzierung* – Wie bereits in Kapitel 10 beschrieben, können hier die Lizenzen eingetragen werden. Sollten Sie bei dem Versuch eine Fehlermeldung bekommen, kann das an genutzten Features liegen, die in Ihrer Lizenz nicht enthalten sind. Im Testmodus stehen Ihnen alle Optionen der Version Enterprise Plus zur Verfügung. Wenn Sie also z. B. vMotion getestet haben, es in Ihrer Lizenz aber nicht enthalten ist, müssen Sie alle Einstellungen diesbezüglich rückgängig machen, bevor Sie Ihre Lizenz eintragen können. Im unteren Teil des Fensters kann ein Lizenzserver für die alten 3er-Hosts eingetragen werden, falls das nötig ist. Der Lizenzserver der alten Version muss

dann entweder noch auf dem ehemaligen Virtual Center Server laufen oder Sie installieren den Lizenzdienst auf einem anderen Rechner. Das kann auch der aktuelle vCenter Server sein. Geben Sie anschließend hier die IP-Adresse des Computers mit dem LM-Tool ein.

- **Statistik** – Geben Sie die Erfassungsintervalle, die Aufbewahrungszeit für Statistikerfassung und die Statistikerfassungsstufe an. Die Auswirkungen der Statistikerfassung auf Ihre vCenter Datenbank hängen vom aktuellen vCenter und der Bestandslisten-größe ab. Wenn Sie die Anzahl der physischen Hosts und deren virtuelle Maschinen ändern, wird auch der geschätzte erforderliche Speicherplatz der Datenbank aktualisiert (siehe Abbildung 15-1). Damit reduzieren Sie nicht die Größe der Datenbank – das können Sie beim Eintrag *Datenbank* erledigen (siehe Seite 384 Datenbankaufbewahrungsrichtlinie unten). Bei den Statistikintervallen können drei Werte verändert werden. Das beeinflusst natürlich auch die Größe der Datenbank. Bei den Tagesstatistiken können Sie z.B. die Werte für den Intervall auf eine Minute einstellen und damit fünfmal mehr Daten abspeichern als üblich. Setzen Sie gleichzeitig die Anzahl der Tage auf fünf, werden 25-mal mehr Werte anfallen, und bei der Statistikebene können Sie diesen Wert nochmals mit vier multiplizieren, was dann zum 100-fachen Datenvolumen führt.

| Intervalldauer                                 | Speichern für | Statistikebene |
|------------------------------------------------|---------------|----------------|
| <input checked="" type="checkbox"/> 5 Minuten  | 1 Tage        | 1              |
| <input checked="" type="checkbox"/> 30 Minuten | 1 Woche       | 1              |
| <input checked="" type="checkbox"/> 2 Stunden  | 1 Monat       | 1              |
| <input checked="" type="checkbox"/> 1 Tag      | 1 Jahre       | 1              |

**Datenbankgröße**

Anhand der aktuellen Größe des vCenter und der Bestandsliste kann die Größe der vCenter-Datenbank geschätzt werden. Um eine Schätzung zu erhalten, geben Sie die in Ihrer Bestandsliste erwartete Anzahl an Hosts und virtuellen Maschinen ein.

Physische Hosts    Geschätzter erforderlicher Speicherplatz: **0,89 GB**  
 Virtuelle Maschinen

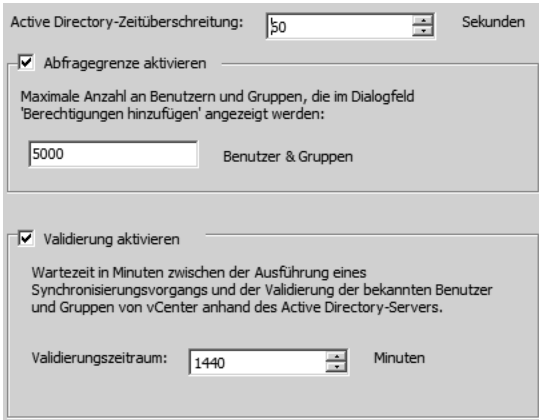
Klicken Sie auf 'Hilfe' für weitere Informationen über das Berechnen der Größe der vCenter-Datenbank.

Abbildung 15-1: Die geschätzte Datenbankgröße

- **Laufzeiteinstellungen** – Sehen Sie sich die Laufzeiteinstellungen für die vCenter Server-Installation an. Die eindeutige vCenter Server-ID liegt im Zahlenbereich von 0 bis 63. Eine Änderung ist nur notwendig, wenn Sie mehrere vCenter Server im verknüpften Modus haben und hier eine ID vom System doppelt vergeben wurde. Die ID des vCenter Server-Systems kennzeichnet diesen in einer gemeinsamen Umgebung eindeutig. Standardmäßig wird ein willkürlicher ID-Wert generiert. Die verwaltete IP-Adresse muss nicht eingetragen werden, selbst wenn der vCenter Server mit mehre-

ren Netzwerkkarten in unterschiedlichen Subnetzen liegt. Sollte es doch einmal zu Problemen kommen, gehört hier die IP hinein, die die Hosts sehen können. Benennen Sie den vCenter Server um, muss diese Änderung im letzten Feld eingetragen werden. Nehmen Sie dafür den FQDN (Fully Qualified Domain Name). Bei allen Änderungen auf dieser Seite muss der vCenter Server neu gestartet werden. Der bloße Neustart der Dienste reicht hier meist nicht aus.

- *Active Directory* – Sie können hier zunächst das Zeitlimit für Active Directory-Abfragen einstellen. Der Wert von 60 Sekunden reicht üblicherweise aus. Befindet sich der nächstgelegene Domänencontroller nicht im selben Netz wie der vCenter Server, kann dieser Wert nach oben auf maximal 180 Sekunden angepasst werden. Die maximale Anzahl von Anwendern und Gruppen, die im Dialogfeld *Berechtigungen hinzufügen* angezeigt werden können, wird im zweiten Block eingestellt. *Abfragegrenze aktivieren* gibt die maximale Anzahl von Anwendern und Anwendergruppen aus der markierten Domäne an, die von vCenter gespeichert werden. Geben Sie 0 (null) ein, um keine Obergrenze zu setzen. Die Häufigkeit, mit der die Synchronisierung und Validierung der dem vCenter Server bekannten Anwender und Anwendergruppen durchgeführt wird, lässt sich im *Validierungszeitraum* angeben. 1.440 Minuten entsprechen einem Tag und sind ein üblicher Wert. Hier wird in Sekunden angegeben, wie lange das Durchsuchen der markierten Domäne im vCenter Server höchstens dauern darf. Das Durchsuchen von sehr großen Domänen kann viel Zeit in Anspruch nehmen.



The screenshot shows the 'Active Directory' configuration window in vCenter. At the top, 'Active Directory-Zeitüberschreitung:' is set to 50 with a spin button and the unit 'Sekunden'. Below this, there are two sections. The first section, 'Abfragegrenze aktivieren', is checked and contains the text 'Maximale Anzahl an Benutzern und Gruppen, die im Dialogfeld 'Berechtigungen hinzufügen' angezeigt werden:' followed by a text box containing '5000' and the label 'Benutzer & Gruppen'. The second section, 'Validierung aktivieren', is also checked and contains the text 'Wartezeit in Minuten zwischen der Ausführung eines Synchronisierungsvorgangs und der Validierung der bekannten Benutzer und Gruppen von vCenter anhand des Active Directory-Servers.' followed by 'Validierungszeitraum:' and a spin box set to '1440' with the unit 'Minuten'.

Abbildung 15-2: Einstellungen zu Active Directory



Wenn Sie kein Microsoft Active Directory haben, kann es beim Abholen der Daten zu Zeitüberschreitungen kommen. Setzen Sie die Grenze bei *Benutzer & Gruppen* auf etwas über 1.000 fest, damit Sie überhaupt etwas bekommen (siehe Abbildung 15-2).

- *E-Mail* – Geben Sie den SMTP-Server und das E-Mail-Konto an, über die Sie Benachrichtigungen z.B. bei Alarmen oder neuen Updates (nur dort ist das möglich) erhalten wollen. Das funktioniert nur mit eigenen E-Mail-Servern, aber nicht mit POP3-Konten im Internet usw. Möchten Sie eine Mail z.B. bei Alarmen nach Hause bekommen, können Sie Ihren E-Mail-Server entsprechend einstellen.
- *SNMP* – Geben Sie die SNMP-Internetadressen der Empfänger und die Ports und Community-Zeichenfolgen an, wenn Sie das Simple Network Management-Protokoll für die vSphere-Umgebung nutzen wollen. Hiermit können dann aktiv SNMP-Traps geschickt werden. Eine Abfrage über SNMP ist standardmäßig möglich. Bis zu vier Empfänger können hier Nachrichten vom vCenter Server erhalten - üblicherweise bei Störungen oder Alarmen.
- *Web-Service (Ports)* – Ändern Sie die HTTP- und HTTPS-Ports für den Webservice nur, wenn es unbedingt notwendig ist. Eigentlich sollte die Einstellung schon bei der Installation des vCenter Servers gesetzt werden.
- *Zeitüberschreitungs-Einstellungen* – Geben Sie die Timeout-Einstellungen für die Verbindung des vSphere Clients für normale Vorgänge und lange Vorgänge an. Das normale Zeitlimit gibt an, wie lange (in Sekunden) der vSphere Client auf eine Antwort des vCenter Servers wartet, bis das Zeitlimit überschritten wird. Die Standardeinstellung sind 30 Sekunden. Das lange Zeitlimit, z.B. bei externen VPN-Verbindungen, gibt an, wie lange (in Sekunden) der vSphere Client hier auf eine Antwort des vCenter Servers wartet. Die Standardeinstellung sind 120 Sekunden.
- *Protokollierungsoptionen* – Geben Sie den Detaillierungsgrad und den Protokollumfang an, die während des normalen Betriebs vom vCenter erfasst werden sollen. Die sechste Einstellung gibt die erweiterte ausführliche Protokollierung an und wird für die Fehlerbeseitigung und Problemlösung verwendet. Achten Sie unbedingt auf die Größe der abgespeicherten Dateien, wenn Sie hier etwas geändert haben.
- *Datenbank* – Geben Sie die maximale Anzahl von Datenbankverbindungen an, die erstellt werden sollen (standardmäßig 50). Ändern Sie diesen Wert, muss der vCenter Server zur Übernahme neu gestartet werden.
- *Datenbankaufbewahrungsrichtlinie* – Hier kann die Größe der Datenbank erheblich beeinflusst werden. Die Aufgaben und Ereignisse können eine Menge Speicher benötigen. Die statistischen Leistungswerte der VMs und Hosts werden ebenfalls in der Datenbank gehalten. Achten Sie darauf, dass hier üblicherweise keine Löschungen vorgenommen werden (das Häkchen ist nicht gesetzt). Überlegen Sie sich, ob es etwas bringt, die Leistungsdaten von mehr als einem halben Jahr (ca. 180 Tage) aufzubewahren – wenn nicht, aktivieren Sie das Kästchen bei *Aufgaben beibehalten für* und das Kästchen bei *Ereignisse beibehalten für*.
- *SSL Einstellungen* – Sie können den vCenter Server so konfigurieren, dass er die SSL-Zertifikate von Hosts überprüft, zu denen er eine Verbindung herstellt (das ist der Stan-



dard). Bei dieser Option führen der vCenter Server, der vSphere Client und die WebAccess-Clients Überprüfungen für gültige SSL-Zertifikate durch, bevor eine Verbindung mit einem Host für Vorgänge wie das Hinzufügen eines Hosts oder das Erstellen einer Remote-Konsolenverbindung mit einer virtuellen Maschine erstellt wird.

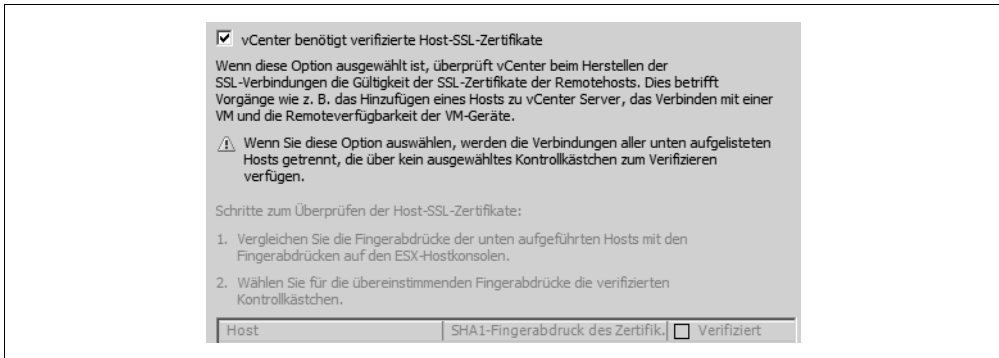


Abbildung 15-3: Host-SSL-Zertifikate

Falls Hosts vorhanden sind, die eine manuelle Validierung erfordern, vergleichen Sie die für die Hosts aufgelisteten Fingerabdrücke mit den Fingerabdrücken in der Hostkonsole und aktivieren Sie das Kontrollkästchen neben jedem übereinstimmenden Host.



Hosts, die nicht ausgewählt sind, werden getrennt, wenn Sie auf OK klicken, wie die Warnmeldung in Abbildung 15-3 zeigt.

- *Erweiterte Einstellungen* – Auf der Seite *Erweiterte Einstellungen* können Sie die vCenter Server-Konfigurationsdatei *vpxd.cfg* ändern. Sie können bestehende Einträge jedoch nicht bearbeiten oder löschen. VMware empfiehlt, dass Sie nur dann Änderungen an diesen Einstellungen vornehmen, wenn Sie vom technischen Support von VMware dazu aufgefordert werden oder die entsprechenden Anweisungen in der VMware-Dokumentation befolgen. Die meisten der hier angezeigten Felder sind mit den oben beschriebenen Einträgen gesetzt. Wenn Sie beispielsweise den ersten Eintrag in der Liste mit dem Namen *ads.checkIntervall* nehmen, ist das der 24-Stunden-Intervall für die Active Directory-Validierung.

## Alarme

Sowohl auf dem ESXi Server (nicht dem alleinstehenden) als auch dem vCenter Server gibt es nach der Installation einige vordefinierte Alarmfunktionen, die bei bestimmten Gegebenheiten ausgelöst werden. Diese konfigurierbaren Alarme werden bei eingestellten Ereignissen, bei erfüllten Bedingungen oder beim Erreichen eines bestimmten Status ausgelöst. Damit können Sie fast alle Komponenten Ihrer Umgebung überwachen:

- *ESXi Server*
- *virtuelle Maschinen*
- *vCenter Server*
- *Datenspeicher*
- *Netzwerke (auch verteilte Switches und Portgruppen)*
- *Cluster und Datencenter*
- *Lizenzierung (über vCenter Server)*
- *Update Manager (nur neue Updatemeldungen und Benachrichtigungen)*

Für jedes dieser Objekte gibt es eine oder mehrere eingerichtete Alarmfunktionen, die auch nur für diese Komponente ggf. eine Aktion auslösen. Zu den möglichen Aktionen gehört das Senden einer E-Mail, eines SNMP Trap, das Ausführen eines Skripts oder Befehls, die Anzeige auf der Oberfläche des vSphere Clients, das Starten oder Herunterfahren einer VM oder eines Hosts und weitere.

So gibt es zum Beispiel den vordefinierten Alarm für die Überwachung der CPU-Auslastung der virtuellen Maschine. Dieser ist von VMware so eingestellt, dass bei mehr als 75 % eine gelbe Warnmeldung und bei mehr als 90 % eine rote Alarmmeldung über den vSphere Client auf der Oberfläche angezeigt wird. Weitere mögliche Farben sind grün, wenn die CPU-Nutzung unter 75 % ist, und grau, wenn keine Auslastungsangaben zur Verfügung stehen. Die Meldung über einen grauen oder grünen Zustand wird aber üblicherweise nur in den Ereignismeldungen angezeigt. Alarme oder Warnungen werden immer dann ausgelöst, wenn sich der Status ändert, also von grün nach gelb, von gelb nach rot und wieder zurück, also von rot nach gelb oder von gelb nach grün.

Ändern können Sie alle Einstellungen nur dort, wo sie definiert wurden, und eigene Alarme können Sie überall erstellen, auch auf einer individuellen VM. Erstellen Sie einen neuen benutzerdefinierten Alarm, dann gilt dieser für alle Objekte an dieser Stelle und alle untergeordneten Objekte. Erstellen Sie also zum Beispiel einen Alarm auf dem vCenter Server für Hosts, gilt dieser für alle ESXi Server, die zu diesem vCenter gehören. Tun Sie dies aber auf einem ESXi Server, gilt der Alarm nur für diesen und nicht für die anderen Hosts.

Wollen Sie Meldungen nur für bestimmte VMs und nicht für alle bekommen, können Sie diese in einen Ordner verschieben und dort den Alarm setzen.

Grundsätzlich bestehen Alarmdefinitionen aus zwei Komponenten: einem Auslöser und einer abhängigen Aktion. Ein Auslöser ist dabei üblicherweise eine Bedingung, die zutreffen muss, damit die Aktion (z. B. eine E-Mail zu senden) ausgelöst wird. Teilweise muss die Bedingung auch erst für einen definierbaren Zeitraum vorliegen, damit die Aktion ausgelöst wird. Beispielsweise wird der Standardalarm für die Nutzung des Arbeitsspeichers der virtuellen Maschine erst nach fünf Minuten ausgelöst.

## Alarmmeldungen einstellen

Nach der Installation des ESXi oder vCenter Servers ist meist nur die Anzeige über den vSphere Client definiert. Um diese Meldungen per E-Mail oder SNMP Trap zusätzlich bekommen zu können, müssen Sie das vorher über den vSphere Client im vCenter Server konfigurieren (siehe oben) – diese Konfiguration ist beim ESXi Server nicht möglich. Weiterhin werden diese Vorkommnisse in den zugehörigen Logdateien und in der vCenter Server-Datenbank festgehalten. Ereignismeldungen sehen Sie auch unter dem jeweiligen Kartenreiter **EREIGNISSE**.

Wenn Sie E-Mails und/oder SNMP Traps gesendet bekommen wollen, gehen Sie über den vSphere Client zu **HOME → VCENTER SERVER EINSTELLUNGEN**, um das zu konfigurieren.

Beim Eintrag *E-Mail* geben Sie den SMTP-Server sowie das E-Mail-Konto an, über das Sie Benachrichtigungen z. B. bei Alarmen oder neuen Updates erhalten wollen.

Beim Eintrag *SNMP* geben Sie die SNMP Internetadressen der Empfänger, die Ports und Community-Zeichenfolgen an, wenn Sie das Simple Network Management-Protokoll für die vSphere-Umgebung nutzen wollen.

Änderungen an diesen Einstellungen werden nur auf den aktuellen vCenter Server angewendet. Wenn Sie sich abmelden und bei einem anderen vCenter Server anmelden, gelten diese Einstellungen nicht für diesen Server.

## Eigene Alarmmeldungen erstellen

Bei jedem Objekt, für das Alarme bereits vordefiniert sind oder für das Sie eigene Alarme erstellen können, haben Sie die eigene Registerkarte *Alarme*. In der Ansicht können Sie zwischen *ausgelöste Alarme* und *Definitionen* umschalten. Unter dem letzteren Punkt sehen Sie in der Liste auch, wo diese Alarme definiert wurden – und nur dort können sie auch verändert werden. Wurde ein benutzerdefinierter Alarm an diesem Punkt erstellt, so steht in der Spalte *Definiert in* »Diesem Objekt«.

Meist möchte man Alarme für eine virtuelle Maschine oder einen ESXi Server neu erstellen.

Beispiel:

In diesem Beispiel sollen eine Alarmmeldung über den vSphere Client angezeigt und zusätzlich die gerade heruntergefahrte oder ausgeschaltete VM sofort neu gestartet werden, weil sie wichtige Aufgaben zu erledigen hat und von unwissenden Benutzern häufiger heruntergefahren wird.

1. Klicken Sie auf die VM, die niemals aus sein darf.
2. Wählen Sie den Kartenreiter **ALARME** und anschließend die Schaltfläche **DEFINITIONEN**.
3. Über das Menü oder das Kontextmenü können Sie hier einen neuen Alarm erstellen. Es öffnet sich das Fenster **ALARMEINSTELLUNGEN**.

4. Geben Sie einen aussagekräftigen Namen ein, z.B. »vm-XP-3 ist aus«, und optional auch eine Beschreibung dazu. Da hier nur ein Alarm auf eine VM erstellt werden kann, steht im Drop-down-Fenster ÜBERWACHEN nur ein Eintrag.
5. Wählen Sie das zweite Optionsfeld aus, um ein Ereignis (Einschalten, Ausschalten etc.) zu überwachen, und klicken Sie auf den Kartenreiter AUSLÖSER.
6. Fügen Sie hier als Ereignis »VM ausgeschaltet« hinzu. Unter dem Link ERWEITERT können Sie noch weitere Bedingungen dafür auswählen, was aber für unser Beispiel nicht notwendig ist.
7. Ein Bericht kann für diesen Alarm auf dem nächsten Kartenreiter nicht ausgewählt werden, klicken Sie deshalb auf AKTIONEN.
8. Über die Schaltfläche HINZUFÜGEN können nun die Aktionen für den Alarm ausgewählt werden. Wählen Sie aus dem Drop-down-Feld VIRTUELLE MASCHINE EINSCHALTEN aus. Damit wird beim Alarm die VM sofort neu gestartet.



Ein einmal aufgetretener Alarm bleibt je nach Typ so lange bei dem Objekt stehen, bis Sie ihn manuell über die rechte Maustaste (Kontextmenü) bestätigen und auf grün setzen (siehe Abbildung 15-4).

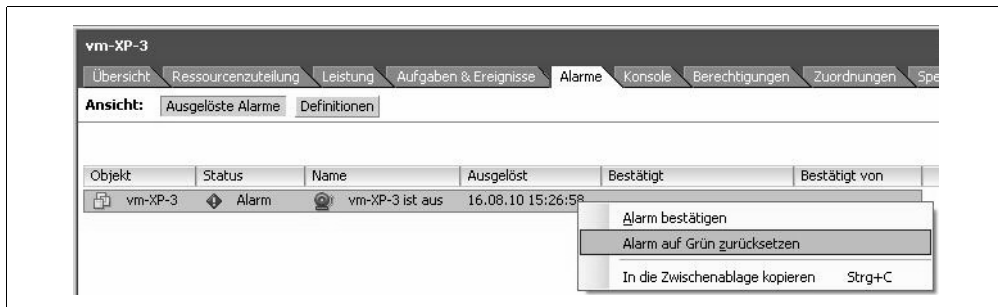


Abbildung 15-4: Alarm bestätigen und auf grün setzen

Bei anderen Alarmtypen wird eine Verzögerung von meist fünf Minuten eingestellt, nach der der Alarm automatisch verschwindet, wenn die Bedingung nicht mehr zutrifft, z.B. bei der CPU-Nutzung einer VM.

Für das Erstellen, Ändern, Löschen, Bestätigen und Deaktivieren von Alarmaktionen und das Festlegen des Alarmstatus sind besondere Berechtigungen notwendig. Diese können über eine Rolle einer Gruppe oder einem Benutzer zugeordnet werden. So können Sie beispielsweise einer Gruppe das Recht geben, eine Alarmaktion zu bestätigen, aber nicht, sie auf grün zu setzen. Anschließend sehen Sie als Administrator weiterhin den Auslöser und wer diesen Alarm bestätigt hat.

## Alarm mit mehreren Bedingungen

Es besteht die Möglichkeit, mehrere Bedingungen für das Auslösen eines Alarms oder einer Warnmeldung zu erstellen. Sie können beispielsweise eine Alarmdefinition erstellen, die nur eine Meldung ausgibt, wenn die CPU-Last und der verbrauchte Arbeitsspeicher einer VM einen bestimmten Wert überschreiten oder auch wenn nur eine der Bedingungen zutrifft. Überprüfen Sie aber, ob es nicht schon einen vordefinierten Alarm für den Zustand gibt, sonst bekommen Sie ggf. zu viele Meldungen.

Es sind sogar unsinnige und widersprüchliche Bedingungen möglich, wie Sie in Abbildung 15-5 sehen können. Einen Alarm wie in der Abbildung erstellt man natürlich nur, wenn man z.B. die E-Mail-Funktion überprüfen möchte – aber nicht als echte Funktion in einer produktiven Umgebung.

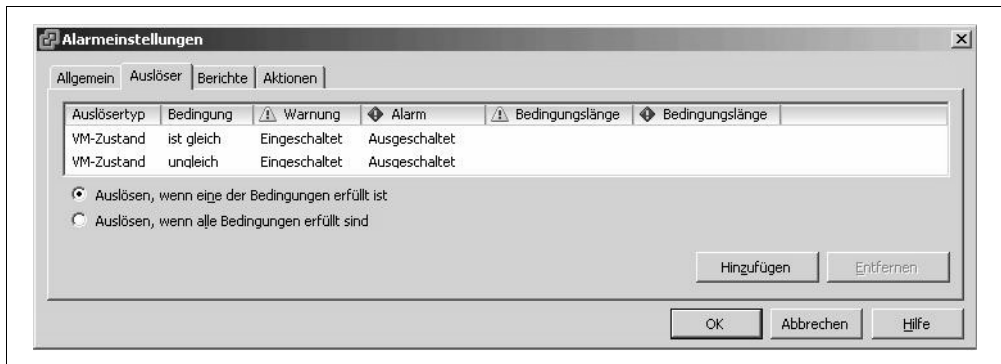


Abbildung 15-5: Widersprüchliche Alarmmeldungen



Vordefinierte Alarmlern lassen sich nicht auf unterer Ebene entfernen oder deaktivieren, und Sie können die Vererbung auf untergeordnete Objekte nicht einschränken.

## Zeitbedingungen bei Alarmen

Für einige Auslösertypen können Zeitangaben dafür mit angegeben werden, wie lang der Zustand anhalten muss, bevor eine Aktion ausgelöst wird. Bei einigen vordefinierten Alarmen ist das bereits konfiguriert, und bei anderen Auslösertypen ist es nicht möglich und meist auch nicht sinnvoll.

So sind bei der CPU-Nutzung der VM jeweils fünf Minuten vorgesehen, bevor eine Warnung oder ein Alarm ausgelöst wird. Wird eine virtuelle Maschine neu gestartet, verbraucht sie üblicherweise mehr CPU-Last als hinterher im Betrieb. Wären hier keine Zeiten angegeben, würde bei jedem Start einer Maschine auch eine Meldung kommen.

In den Feldern zur Bedingungs­länge können Sie zwischen 0 und 60 Minuten wählen. Die manuelle Eingabe der Zeit ist hier nicht möglich. Grundsätzlich sind Zeitangaben bei Netzwerk, vCenter Server, Datencenter, Cluster und Storage Alarmen nicht möglich, weil hier nur Ereignisse auftreten können, die sofort gemeldet werden. Lediglich beim Host oder der VM können zu einer Bedingung oder einem Status Zeiten ausgewählt werden – aber eben nicht bei jedem Auslösertyp.

## Schwellenwerte bei Alarmen

Für einige Alarme können über den Kartenreiter **BERICHTE** ein Schwellenwert und eine Häufigkeit für die jeweilige Aktion angegeben werden. Das ist angebracht, wenn Sie eine Maschine überwachen wollen, deren CPU-Nutzung kurzfristig über die eingestellte Marke kommt. Haben Sie beispielsweise 75 % CPU-Nutzung für eine Meldung festgelegt und möchten wissen, wann die VM die 80 % überschreitet, können Sie den ausgelösten Alarm wiederholen, wenn die CPU-Nutzung 5 % über den eingestellten Wert kommt.

Weiterhin können Sie die Häufigkeit der Meldungen festlegen. Bei den meisten vordefinierten Alarmen wird eine Aktion alle fünf Minuten ausgelöst – das kann bei einigen Meldungen sinnvoll, aber bei anderen auch nervig sein.



Bei der CPU-Nutzung einer VM wird die Anzahl der zugewiesenen CPUs berücksichtigt. Sie errechnet sich aus der Summe der MHz geteilt durch die Anzahl der vCPUs multipliziert mit der Taktrate der physischen CPUs multipliziert mit 100.

Beispiel:

Ein Host hat einen 3,0-GHz-Prozessor mit vier Kernen. Somit liegt seine maximale Gesamtfrequenz bei 12 GHz. Einer VM gebe ich zwei vCPUs, deren Auslastung bei 50 bzw. 75 % liegt. Das macht zusammen  $(50 + 75) / 2 = 60$  % Auslastung und entspricht  $(3,0 \text{ GHz} + 3,0 \text{ GHz}) * 60 \% = 3,6 \text{ GHz}$ . Also: CPU-Nutzung der VM =  $3,6 \text{ GHz} / (2 \text{ vCPUs} * 3,0 \text{ GHz}) * 100 = 60 \%$ .

Bei der Berechnung der prozentualen Host-CPU-Auslastung sieht es genauso aus. In unserem Beispiel wären das die CPU-Nutzung geteilt durch die Anzahl der CPUs multipliziert mit der Taktrate multipliziert mit hundert:  $4,6 \text{ GHz} / (4 * 3,0 \text{ GHz}) * 100 = 38,33 \%$ .

## Befehle und Skripten als Alarmaktion

Beim ESXi Server und der virtuellen Maschine haben Sie die Möglichkeit, Anwendungen oder Stapelverarbeitungsdateien als Alarmaktion festzulegen. Beachten Sie dabei, dass diese Aktionen über den vCenter Server-Dienst ausgeführt werden. Das heißt, dass das Skript oder der Befehl mit Systemberechtigungen läuft. Mit ein wenig Hintergrundkenntnissen kann man das aber umgehen. Eine schlechte Idee wäre es, dem VirtualCenter Server-Dienst deshalb nur mit Userrechten zu starten.

Wenn Sie Skripten für die Remote-Konsole erstellen möchten, geht das nicht direkt, da als Alarmskript nur eine Stapelverarbeitungsdatei (\*.bat) verwendet werden kann. Über eine »Umleitung.bat« können Sie aber Ihre (Power-)RCLI-Skripten aufrufen.



Das Skript wird bei Windows über *cmd.exe* ausgeführt. Diese Datei befindet sich üblicherweise unter *C:\Windows\System32\*. Sollten Sie einen anderen Pfad für Ihre Dateien bevorzugen (so wie ich), müssen Sie mit vollständigen Pfadangaben arbeiten (siehe Beispiel).

Beispiel:

In diesem Beispiel möchte ich Ihnen zeigen, wie man Informationen über einen ausgelösten Alarm auf dem vCenter Server in eine Datei ablegen kann. Ich nutze hier eine Batchdatei, die die Angaben über Parameter erhält und diese in eine Textdatei schreibt. Für diesen Test habe ich eine VM mit Windows XP genommen, Sie können aber auch jede andere VM und auch einen ESX(i) Server dafür nehmen. Was diesen Alarm auslöst, spielt dabei keine Rolle, Sie sollten jedoch für einen ersten Test eine Möglichkeit nutzen, die ohne großes Zutun einen Alarm auslöst.

Erstellen Sie einen benutzerdefinierten Alarm und wählen Sie auf der letzten Registerkarte AKTIONEN die Aktion BEFEHL AUSFÜHREN. In der Spalte KONFIGURATION geben sie jetzt Ihre Stapelverarbeitungsdatei mit (maximal neun) Parametern an (siehe Tabelle), also z.B. *C:\Test\Test.bat Para1 Para2...*

Die Dateien, also die Batch- und die Textdatei, befinden sich hinterher im Ordner *C:\Test*.

Parameter für die Batchdatei:

| Parameter           | Beschreibung                                |
|---------------------|---------------------------------------------|
| {eventDescription}  | Ereignisbeschreibung für den Statuswechsel  |
| {targetName}        | Zielname bzw. Objekt, das den Alarm auslöst |
| {alarmName}         | Name des Alarms (den Sie gewählt haben)     |
| {triggeringSummary} | Werte des Alarmauslösers                    |
| {declaringSummary}  | Werte der Alarmdeklaration                  |
| {oldStatus}         | Status vor der Auslösung des Alarms         |
| {newStatus}         | Status nach der Auslösung des Alarms        |
| {target}            | Zielobjekt, z.B. Ihre VM                    |

Aufruf der Batchdatei:

```
C:\Test\Test.bat "{eventDescription}" "{targetName}" "{alarmName}" "{triggeringSummary}"
"{declaringSummary}" "{oldStatus}" "{newStatus}" "{target}"
```

Text (Inhalt) der Batchdatei:

```
@echo off
echo Ereignisbeschreibung für den Statuswechsel : %1>>C:\Test\Alles.txt
echo Zielname bzw. Objekt, das den Alarm auslöst : %2>>C:\Test\Alles.txt
echo Name des Alarms (den Sie gewählt haben) : %3>>C:\Test\Alles.txt
echo Werte des Alarmauslösers : %4>>C:\Test\Alles.txt
echo Werte der Alarmdeklaration : %5>>C:\Test\Alles.txt
echo Status vor der Auslösung des Alarms : %6>>C:\Test\Alles.txt
echo Status nach der Auslösung des Alarms : %7>>C:\Test\Alles.txt
echo Zielobjekt, z. B. Ihre VM : %8>>C:\Test\Alles.txt
echo frei : %9>>C:\Test\Alles.txt
```

Bei der Batchdatei wird der erste Parameter mit dem Platzhalter %1 übernommen, der zweite mit %2 und so weiter. Beachten Sie, dass in meinem Beispiel bei %1 nur eine spitze Klammer nach rechts zeigt. Damit wird eine eventuell vorhandene Datei überschrieben.

```
Ausgabe der Batchdatei (C:\Test\Alles.txt)
Ereignisbeschreibung für den Statuswechsel : "Alarm 'Name des Alarms' auf vm-XP-
3 wurde von Grau in Rot ge"ndert"
Zielname bzw. Objekt, das den Alarm auslöst: "vm-XP-3"
Name des Alarms (den Sie gewählt haben) : "Name des Alarms"
Werte des Alarmauslösers : "Status = Ausgeschaltet"
Werte der Alarmdeklaration :
"([Status Gelb ist gleich poweredOn; Status Rot ist gleich poweredOff])"
Status vor der Auslösung des Alarms : "Grau"
Status nach der Auslösung des Alarms : "Rot"
Zielobjekt, z. B. Ihre VM : "VirtualMachine:vm-61"
frei :
```

Während der Laufzeit der Batchdatei sind über den Empfänger, also *vpxd.exe* auf dem vCenter Server, einige Umgebungsvariablen gesetzt. Setzt man also in die Batchdatei eine Pause, kann man sich diese Variablen mit Inhalt über den Befehl *set* ansehen. Natürlich könnte man auch die Stapelverarbeitungsdatei bei dem Alarm ohne jegliche Parameter aufrufen und in der Batchdatei nur eine Zeile einfügen:

```
set >>C:\Test\Alles.txt
```

Nur sieht die Ausgabe dann nicht so schön aus und es werden hier alle Umgebungsvariablen angezeigt. Sie können diese Umgebungsvariablen innerhalb der Batchdatei natürlich auch über die %-Zeichen abfragen, also z.B. so:

```
echo %VMWARE_ALARM_TARGET_ID%>>C:\Test\Alles.txt
```

Weitere mögliche Variablen sind in der deutschsprachigen PDF-Datei *Datacenter\_Administration\_Guide* ab Seite 174 zu finden. Beachten Sie dabei, dass nicht immer alle Variablen vorhanden sind. Einige sind nur bei Ereignissen, andere bei Statusänderungen und wieder andere nur bei bestimmten Bedingungen vorhanden. Über den Befehl *set* bekommen Sie aber immer alle möglichen angezeigt.



## Deaktivieren von Alarmen

Sie können einen Alarm an der Stelle, wo er definiert wurde, löschen oder deaktivieren. Haben Sie einen Alarm deaktiviert, wird das über ein geändertes Icon beim Alarm angezeigt. Die sonst übliche rote Klingel bekommt dann zusätzlich einen hellroten Kreis mit einem weißen X darin. So können Sie unkompliziert deaktivierte Alarme identifizieren.

Um einen Alarm für nur ein Objekt zu deaktivieren, also z. B. für einen Storage, gehen Sie wie folgt vor:

1. Klicken Sie auf HOME und dann auf DATENSPEICHER UND DATENSPEICHER-CLUSTER.
2. Wählen Sie den Storage aus, für den Sie den Alarm aussetzen wollen.
3. Klicken Sie mit der rechten Maustaste auf diesen Storage und wählen aus dem Kontextmenü ALARM → ALARMAKTIONEN DEAKTIVIEREN (siehe Abbildung 15-6).

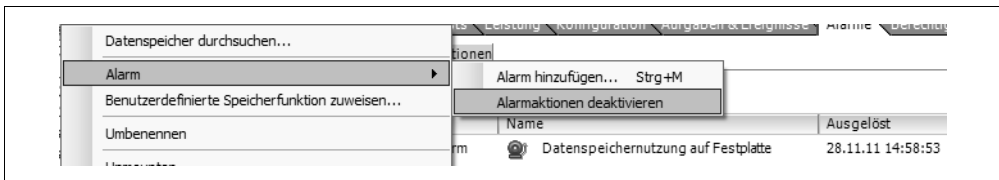


Abbildung 15-6: Alarmmeldungen für einzelnes Objekt deaktivieren

Um diesen Alarm wieder aktiv zu schalten, gehen Sie genau wie oben beschrieben vor. Im Kontextmenü wird bei einem deaktivierten Alarm die Option ALARM → ALARMAKTIONEN AKTIVIEREN angeboten. Die Änderungen werden dabei allerdings nicht sofort wieder angezeigt – es dauert ein Weilchen, bis ein erneuter Alarm ausgelöst wird.



# **Datensicherung und -wiederherstellung**

Backup und Recovery sind mit die wichtigsten Aufgaben, die bei einer produktiven Umgebung anfallen. Dabei spielt es keine Rolle, ob es sich um die virtuelle Welt handelt oder ob physische Systeme gesichert werden müssen. Auch eine Probewiederherstellung sollte zu den regelmäßigen Aufgaben eines jeden Administrators gehören.

Leider zeigt sich in der Praxis, dass dieses wichtige Thema im produktiven Bereich nur allzu oft vernachlässigt wird. Einige Betriebe sind sogar gesetzlich dazu verpflichtet, Sicherungen einzurichten und bei Anfrage auch nachzuweisen – aber dieser Umstand ist vielen EDV-Mitarbeitern unbekannt. Außerdem müssen einige Daten noch nach zehn oder gar dreißig Jahren auf Verlangen abrufbar sein.

Im Falle eines Falles muss man sich auf ein Backup verlassen können. Und man sollte auch regelmäßig durch ein Recovery überprüfen, ob man es kann. Nur wer das oft übt, wird im Katastrophenfall oder in Stresssituationen richtig handeln und einen größeren Datenverlust zu verhindern wissen.

## **Backup-Unterschiede zwischen den Welten**

Wenn Sie Ihre physischen Maschinen mit Agenten im Betriebssystem bisher auf Band oder Platte gesichert haben, können Sie das zunächst weiter so machen. In der virtuellen Welt gibt es aber andere Möglichkeiten, die einem die Wiederherstellung eines Rechners deutlich erleichtern. Die bloßen Daten eines Rechners kann man erst wieder in eine fertig aufgesetzte Maschine mit installiertem Backup-Agenten zurückspielen (siehe Kapitel 14). Welche Hardware vorher in der virtuellen Maschine war, lässt sich nachträglich nicht immer zweifelsfrei bestimmen. Bei einer VM können aber alle beteiligten Dateien auf ein VMFS-Volumen zurückkopiert werden, und die Maschine ist sofort wieder einsatzbereit – ohne Umwege über eine Neuinstallation des Betriebssystems und Installation einer Backupsoftware.

Gerade in letzter Zeit haben viele Hersteller recht gute Produkte für die Sicherung und Wiederherstellung virtueller Maschinen entworfen. Dabei gibt es einige kostenlose Pro-

dukte und auch Kaufversionen mit den unterschiedlichsten Ansätzen. Erfahrungen können Sie meist auch über voll funktionierende, zeitlich begrenzte Versionen machen und sich dann für ein Produkt entscheiden. Schauen Sie sich z.B. die Möglichkeiten an, die die Firmen Quest Software (ehemals Vizioncore, [www.quest.com/virtualization](http://www.quest.com/virtualization)), Veeam ([www.veeam.com/de](http://www.veeam.com/de)), arkeia software ([www.arkeia.com/de/products](http://www.arkeia.com/de/products)) und Acronis ([www.acronis.de](http://www.acronis.de)) bieten.

Die Ansätze der einzelnen Produkte sind zwar zum Teil sehr unterschiedlich, wichtig ist aber nur, dass Sie eine Software finden, mit der Sie einfach, schnell und unkompliziert diese Aufgabe erledigen können.

## Sicherung des Hosts

Die Meinungen beim Backup eines ESXi Servers gehen weit auseinander. Muss der Host überhaupt gesichert werden, oder setzt man ihn einfach neu auf? Beides ist möglich!

Da beim neuen installierbaren Hypervisor von VMware (ESXi) kein Betriebssystem mehr als Grundlage vorhanden ist, schlagen die üblichen Backupmethoden wie bei Linux fehl. Welche Möglichkeiten gibt es dann überhaupt? Mit dem Befehl `vicfg-cfgbackup.pl` über RCLI o. Ä. können die wichtigsten Konfigurationsdateien des Hosts gesichert und wieder zurückgespielt werden. Bei der kostenlosen Version schlägt das Zurückspielen aber fehl, weil der Host sich nach dem Einspielen der Lizenz im schreibgeschützten Modus befindet. Setzt man einen neuen ESXi auf, trägt man die Lizenz einfach erst nach dem Zurückspielen der Sicherung ein. Natürlich kann die Konfiguration aber auch händisch nach einer Neuinstallation wieder eingepflegt werden. Probleme gibt es dann aber ggf. bei der neuen Identität, die den Zugriff auf einen externen Storage z.B. wegen eines anderen IQN (iSCSI Qualified Name) verhindern kann.

Eine weitere Möglichkeit besteht darin, den Befehl `vm-support` aufzurufen. Dieser sammelt unter anderem auch die komplette Konfiguration. Die anschließend erstellte gepackte Datei kopiert man sich auf einen beliebigen Datenträger. Muss der Host neu installiert werden, entfernt man aus dem Paket die nicht benötigten Verzeichnisse wie z. B. `/proc` und `/vmfs` und kopiert die restlichen Daten in die Originalverzeichnisse zurück. Wenn man anschließend den Server neu startet, ist die komplette Konfiguration wiederhergestellt.

Hat man ein Fibre-Channel- oder iSCSI-SAN, kann man die Installation des Hosts auch dort vornehmen. Über zusätzliche Funktionen des Storage können natürlich auch diese Daten gesichert werden. Einen neuen Server lässt man einfach vom SAN booten und braucht sich keinerlei weitere Gedanken über das Backup zu machen.

## Sicherung der VMs

Wie schon eingangs erwähnt, kann man bei der Sicherung von virtuellen Maschinen genauso verfahren wie bei physischen Systemen. Besser ist es jedoch, wenn eine Backupsoftware die Dateien der VM von der VMFS-Partition sichert. Dazu gehören die Festplat-

tendateien (\*.vmdk und \*-flat.vmdk), die Konfigurationsdateien (\*.vmx und \*.vmxf) sowie ggf. das BIOS (\*.nvram, nur notwendig, wenn BIOS-Einstellungen geändert wurden). Haben Sie aktive Snapshots, müssen Sie diese ebenfalls berücksichtigen und zusätzlich die Snapshotdatei (\*.vmsd) sichern. Auf jeden Fall ist es besser, wenn Sie die Snapshots vor der Sicherung entfernen bzw. übernehmen (siehe Kapitel 8).

Die meisten Softwarelösungen für diese Aufgabe machen vor dem Backup einen Snapshot der Maschine, weil dann die Festplattendatei ohne Probleme kopiert werden kann. Ist der Vorgang abgeschlossen, wird der dann aktuelle Zustand übernommen.



Achten Sie unbedingt auf die korrekte Rücknahme der Snapshots. Bei Problemen kann das jeweilige Volume schnell voll laufen. Schuld daran ist manchmal die VSS-Komponente in den VMware Tools. Ändern Sie die Einstellungen der Tools und wählen Sie VSS ab (siehe Kapitel 4).

## VMware Consolidated Backup

Am 24. Februar 2010 teilte VMware mit, dass der Support für *Consolidated Backup* demnächst eingestellt wird. Das neue Produkt *Data Recovery* wird es jetzt vollständig ablösen.

## VMware Data Recovery

VMware Data Recovery (VDR) ist ein einfach zu bedienendes Tool, das Backups von den Festplatten und Konfigurationsdateien der virtuellen Maschinen mithilfe von Snapshots erstellt, ohne angemeldete Benutzer oder Daten und Dienste zu behindern. Mit dieser Backuplösung behalten Sie den Überblick und können einstellen, wie viele Ihrer Sicherungen aufbewahrt werden sollen und nach welcher Zeit ältere überschrieben werden.



Dieses Tool macht nur Backups von virtuellen Maschinen, nicht vom Host. Zur Sicherung des ESXi Servers müssen Sie auf eine andere Lösung ausweichen (siehe oben).

Um den Sicherungsbedarf möglichst klein zu halten und unnötige Dopplung von Daten zu verhindern, unterstützt Data Recovery von sich aus einen deduplizierten Speicher. Dieser enthält keinerlei Redundanzen – das heißt, dass vor der Sicherung der Daten auf dem Storage nach identischen Blöcken geschaut wird. Sind solche bereits von dieser oder einer anderen Maschine vorhanden, werden sie nicht noch einmal abgespeichert.

Das Programm wurde unter VMware vStorage API erstellt und wird bei der Zwei-Wege-Installation in den vCenter Server integriert. Die Sicherungsjobs werden über GEPLANTE TASKS in einem definierbaren Zeitfenster ausgeführt.

Da dieses Programm vollständig in den vCenter Server integriert ist, entfällt die Berücksichtigung von vMotion oder DRS (*Distributed Resource Scheduler*) von Maschinen, die verschoben wurden.

Die Zwei-Wege-Installation besteht aus einem unter Windows zu installierenden MSI-Paket (das *Client Plugin*) und einer Virtual Appliance (einer fertigen virtuellen Maschine), die als OVF-Datei (offenes Virtualisierungsformat) mitgeliefert wird, um das Management und das Wiederherstellen aus den Backups zu ermöglichen (siehe Abbildung 16-1). Das Data Recovery-Plugin wird über den VMware vSphere Client gesteuert.



Abbildung 16-1: Data Recovery als OVF-Vorlage bereitstellen

Sicherungen können auf jeder Festplatte abgelegt werden, die vom ESXi Server erkannt und unterstützt wird. Sie können *Storage Area Networks* (SANs), *Network Attached Storage*-Geräte (NAS über NFS) oder Windows-Freigaben (CIFS, *Common Internet File System*) als SAMBA-Komponente (unter Linux und Unix für das SMB-Protokoll von Microsoft benutzt) nutzen. Die Deduplizierung auf dem Storage geschieht im Hintergrund automatisch, und für die VMs werden die Volumenschattenkopien (VSS, *Volume Shadow Copy Service*) unterstützt, die das Sichern für einige Windows-Betriebssysteme vereinfachen.

## Sicherung der virtuellen Maschinen

Vor der Sicherung erstellt Data Recovery einen Snapshot der virtuellen Maschine, der nach Abschluss wieder in die Ausgangsfestplatte der VM integriert wird. Data Recovery kann gleichzeitig ein Maximum von acht virtuellen Maschinen sichern. Um mehrere Sicherungen gleichzeitig ausführen zu können, darf die CPU-Auslastung nicht höher als 90 % sein. Aus Gründen der Arbeitsspeicherauslastung unterstützt Data Recovery nicht mehr als zwei Backupziele gleichzeitig, also verschiedene Storages, auf denen gesichert wird. Wenn mehr als zwei Backupspeicher benutzt werden sollen, können Sie diese zu unterschiedlichen Zeiten ansprechen oder eine weitere Appliance installieren.

Die Sicherungen wenden die Verfolgungsfunktionalität für geänderte Blöcke auf den ESXi Hosts an. Diese überprüft für jede zu sichernde virtuelle Festplatte die vorherige

Sicherung. Anhand dieser Funktionalität werden nur die Änderungen seit der letzten Sicherung eingeholt. Der von Redundanzen bereinigte Storage enthält eine vollständige virtuelle Sicherung auf Basis des letzten Sicherungs-Image und übernimmt darin die Änderungen. Wenn eine virtuelle Maschine doppelte Teile enthält, werden die doppelten Informationen also nur einmal gespeichert.



Diese Optimierungen gelten nicht für virtuelle Maschinen, die mit VMware-Produkten vor vSphere 4.0 erstellt wurden. Beispielsweise werden Änderungstokens nicht für virtuelle Maschinen verwendet, die mit Virtual Infrastructure 3.5 oder früher erstellt wurden. Deshalb dauert das Sichern virtueller Maschinen länger, die mit früheren VMware-Versionen erstellt wurden.

Die Deduplizierung kann für eine bedeutende Platzersparnis sorgen. Es gibt oft viele identische Systemdateien bei virtuellen Maschinen, die unter demselben Betriebssystem ausgeführt werden. Um die Deduplizierung zu maximieren, sichern Sie ähnliche virtuelle Maschinen im selben Ziel. Die virtuellen Maschinen müssen nicht mit demselben Job gesichert werden.

Data Recovery ist Bestandteil folgender Editionen:

- Essential Plus
- Standard
- Enterprise
- Enterprise Plus

Jede installierte Backup-Appliance von Data Recovery kann maximal bis zu 100 virtuelle Maschinen schützen.

Haben Sie mehr VMs, die gesichert werden sollen, müssen Sie mehrere Instanzen von Data Recovery installieren. Durch die Installation zusätzlicher Appliances ist es möglich, mehr als 100 virtuelle Maschinen zu sichern. Allerdings haben die einzelnen Backup-Appliances keinen Zugriff auf die Informationen zu den Sicherungsaufgaben der jeweils anderen Appliances. Das kann zu unbeabsichtigten Konfigurationen führen. Beispielsweise können zwei Backup-Appliances zu Data Recovery so konfiguriert sein, dass sie einen Ordner mit 200 virtuellen Maschinen schützen, aber es ist sehr wahrscheinlich, dass einige dieser virtuellen Maschinen doppelt und andere gar nicht gesichert werden. Stellen Sie also sicher, dass Sie Ihre Jobs dann so planen, dass jeweils die anderen VMs gesichert werden.

Da Data Recovery VSS verwendet, kann es Snapshots erstellen und dabei die Anwendungskonsistenz sicherstellen. Das bedeutet, dass Anwendungen wichtige Daten, die sich gerade im Arbeitsspeicher befinden, auf die Festplatte schreiben, wodurch sichergestellt wird, dass eine spätere Wiederherstellung dieser virtuellen Maschine die Anwendung in einem konsistenten Status wiederherstellen kann.

## Vorteile des Deduplizierungsspeichers

Die von VMware Data Recovery verwendete Deduplizierungsspeicher-Technologie wurde von VMware selbst entwickelt und ist in die Anwendung integriert. Diese Technologie wertet auf dem Sicherungsspeicher vorhandene Blöcke aus, die in Wiederherstellungspunkten gespeichert werden, und überprüft, ob identische Abschnitte bereits vorhanden sind.

Speichern Sie gleiche Maschinen möglichst auf demselben Volume, damit mehrere Sicherungsaufgaben über die Deduplizierungsspeicher-Technologie besser zusammengefasst und die Deduplizierungsraten maximiert werden. Sie müssen aber nicht alle gleichartigen VMs in derselben Sicherungsaufgabe zusammenfassen – die Deduplizierung funktioniert davon unabhängig.

Die Deduplizierung wird für alle gespeicherten virtuellen Maschinen ausgewertet, selbst wenn einige momentan nicht gesichert sind. Es können Speicherplätze für die Sicherungen von bis zu 1 TByte angegeben werden, und jede Backup-Appliance, die Sie dem System hinzufügen, ist für den Einsatz von zwei Deduplizierungsspeichern ausgelegt.

Grundsätzlich gibt es bei Data Recovery keine Grenze hinsichtlich der Größe oder Anzahl der Deduplizierungsspeicher, wenn aber mehr als zwei Speicherziele verwendet werden oder die Größe eines Speichers 1 TByte überschreitet, kann das die Leistung beeinträchtigen. Die minimale Speichergröße beträgt 10 GByte.



Achten Sie darauf, dass ein einzelnes Netzwerkvolume möglichst nicht größer als 500 MByte ist. Die regelmäßigen Überprüfungen des Volume dauern sonst unverhältnismäßig lange und können die anstehende Datensicherung negativ beeinflussen.

Die Menge des benötigten Speichers variiert je nach der Menge an Festplattenspeicher, den die Deduplizierung durch die Ausführung von ähnlichen virtuellen Maschinen sparen kann.

## Systemanforderungen

Für Data Recovery benötigen Sie den vCenter Server und den vSphere Client. Virtuelle Maschinen müssen auf einem ESX 4.0 Server oder höher laufen, ältere ESX Server werden nicht unterstützt.

Je verschiedenartiger die Gruppe der zu schützenden virtuellen Maschinen ist, desto mehr Speicherplatz wird für jede virtuelle Maschine beansprucht. Die benötigte Menge an Speicherplatz wird auch durch die Häufigkeit und Aufbewahrungsdauer der Backups und die Anzahl an zu sichernden virtuellen Maschinen bestimmt. Sie sollten sich also vor der Erstellung der Sicherungsjobs einen Plan davon machen, welche VMs Sie wo ablegen möchten.



## Das Client-Plugin installieren

Damit Sie auf diese Backup-Lösung zugreifen können, müssen Sie – ähnlich wie beim Converter und beim Update Manager – ein Plugin installieren. Leider ist dieses nicht auf dem gleichen Weg wie die beiden anderen Verfahren erreichbar. Sie bekommen es üblicherweise als Microsoft-.*msi*-Datei geliefert, die auf dem Client installiert wird, über den Sie auf das System zugreifen wollen. Achten Sie auf die benötigten Ports 22024 und 22044 für den Client und die Backup-Appliance, wenn irgendwo zwischen Ihrem Rechner und dem ESXi Server eine Firewall sein sollte.

### Vorgehensweise

1. Beenden Sie ggf. Ihre Sitzung mit dem vSphere Client und führen Sie anschließend das Plugin-Installationsprogramm *VMwareDataRecoveryPlugin.msi* aus (siehe Abbildung 16-2).

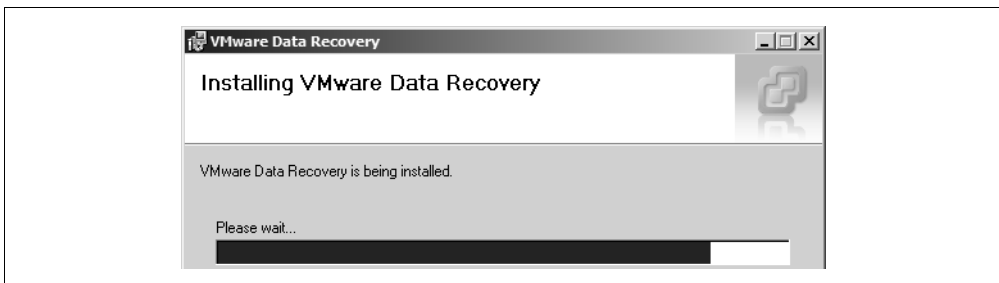


Abbildung 16-2: MSI-Paket installieren

2. Befolgen Sie die Anweisungen des Installationsassistenten.
3. Starten Sie den vSphere Client und melden Sie sich beim vCenter Server an.
4. Wählen Sie über das Menü PLUG-INS → PLUG-INS VERWALTEN und schauen Sie nach, ob das Data Recovery-Plugin aktiviert ist.

Sie können das Client-Plugin nun zum Verwalten von Data Recovery verwenden. Wenn das Data Recovery-Plugin nicht im vSphere Client verfügbar ist, starten Sie den Client neu.

## Installieren der Backup-Appliance

Die Backup-Appliance ist eine vorkonfigurierte virtuelle Maschine, die Sie dem System einfach hinzufügen können. Da es sich um eine OVF-Vorlage handelt, sind schon fast alle Parameter so eingestellt, dass sie ohne große Veränderungen in den meisten Umgebungen läuft.

## Vorgehensweise

1. Wählen Sie über den vSphere Client den Menüpunkt DATEI → OVF-VORLAGE BEREITSTELLEN.
2. Klicken Sie auf AUS DATEI BEREITSTELLEN und wählen Sie die Datei *VmwareDataRecovery.ovf* auf dem Datenträger aus.
3. Optional können Sie jetzt die Informationen zur OVF-Datei lesen.
4. Wenn Sie mit den Bedingungen der EULA einverstanden sind, wählen Sie die entsprechende Option, sonst können Sie den Vorgang nicht fortsetzen.
5. Suchen Sie sich einen Speicherort für die virtuelle Maschine in der vSphere-Bestandsliste aus. Sie können die Backup-Appliance auch umbenennen.
6. Wählen Sie den Host oder Cluster aus, auf dem die Maschine zunächst laufen soll.
7. Nehmen Sie einen geeigneten Datenspeicher, in dem die Dateien der virtuellen Maschine abgelegt werden sollen. Die Festplatte benötigt 5 GByte Platz, der RAM nochmals 2 GByte.
8. Überprüfen Sie die Einstellungen für die Bereitstellung und klicken Sie auf BEENDEN.

Die virtuelle Maschine, also die Backup-Appliance, wird nun in Ihre Umgebung eingefügt (siehe Abbildung 16-3).

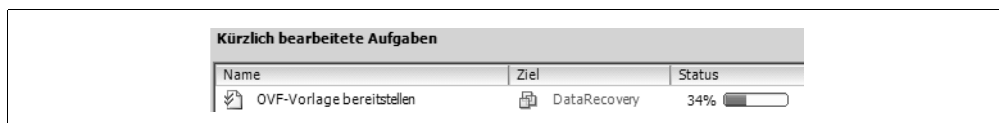


Abbildung 16-3: OVF-Vorlage wird importiert.

## Festplatte zur Backup-Appliance hinzufügen

Wenn Sie auf dem Storage, auf dem die VMs laufen, noch genügend Platz haben, können Sie der Backup-Appliance für die Datensicherung eine weitere Festplatte hinzufügen. Wie bereits oben erwähnt, können Sie auch Netzwerkspeicher dafür verwenden – sogar die Microsoft-Dateifreigabe. Vielleicht möchten Sie ja auch einen Windows-PC mit *Starwind* ausrüsten, um den iSCSI-Speicher nutzen zu können.

Der Backup-Appliance hinzugefügte Festplatten bieten eine schnellere Sicherung, verglichen mit anderen Zielen wie CIFS-Freigaben, die über das Netzwerk gehen.



Wenn Sie eine Festplatte hinzufügen wollen, müssen die Backup-Appliance und das Data Recovery-Plugin für den vSphere Client bereits installiert sein.

Hier der Vollständigkeit halber nochmals die Vorgehensweise beim Hinzufügen einer Festplatte:

1. Starten Sie den vSphere Client und melden Sie sich beim vCenter Server an.
2. Wählen Sie gegebenenfalls BESTANDSLISTE → VMS UND VORLAGEN.
3. Klicken Sie in der BESTANDSLISTE mit der rechten Maustaste auf die virtuelle Maschine, die als Backup-Appliance dient, und wählen Sie EINSTELLUNGEN BEARBEITEN.
4. Klicken Sie auf der Registerkarte HARDWARE auf HINZUFÜGEN.
5. Wählen Sie FESTPLATTE und klicken Sie auf WEITER.
6. Wählen Sie NEUE VIRTUELLE FESTPLATTE ERSTELLEN und klicken Sie auf WEITER.
7. Geben Sie die Festplattengröße und gegebenenfalls weitere Optionen an und klicken Sie auf WEITER.
8. Klicken Sie auf BEENDEN, um die Festplatte zu erstellen.
9. Sie können bei Bedarf noch weitere Änderungen vor dem ersten Starten vornehmen:
  - Die Grafikkarte auf *automatisch erkennen* einstellen
  - Bei CD-/DVD-Laufwerk den Gerätetyp auf *Clientgerät* ändern
  - Den zweiten Netzwerkadapter entfernen
  - Die Anzahl der CPUs und des RAMs für Ihre Umgebung anpassen (siehe oben)

Die Festplatte wird zur Backup-Appliance hinzugefügt und kann anschließend als Ziel für Sicherungen verwendet werden. Wenn die Backup-Appliance eingeschaltet ist, während die Festplatte hinzugefügt wird, wird diese erst beim Neustart erkannt. Sollte die VM also eingeschaltet sein, starten Sie sie neu, um das Hinzufügen der Festplatte sicherzustellen.

## Data Recovery konfigurieren

Was jetzt noch zu tun ist:

- Die Backup-Appliance muss eingeschaltet werden.
- Die Backup-Appliance muss auf dem vCenter Server eingerichtet werden.
- Data Recovery muss konfiguriert werden.
- Sicherungsaufgaben müssen erstellt werden.
- Es können weitere benötigte Ressourcen hinzugefügt werden, z. B. Speicher auf Netzwerkfreigaben.
- Vergessen Sie nicht das Formatieren von angeschlossenen (gemounteten) Volumes.

## Die Backup-Appliance einschalten

Sie müssen zum Durchzuführen und Planen von Sicherungen die VM-Backup-Appliance eingeschaltet haben.

1. Wählen Sie im vSphere Client BESTANDSLISTE → VMS UND VORLAGEN.
2. Klicken Sie mit der rechten Maustaste in der Bestandsliste auf die virtuelle Maschine, die als Backup-Appliance verwendet werden soll, und wählen Sie EINSCHALTEN.
3. Klicken Sie nach dem Einschalten der virtuellen Maschine mit der rechten Maustaste auf die Backup-Appliance-VM und wählen Sie KONSOLE ÖFFNEN. Das Konsolenfenster für die Backup-Appliance erscheint (siehe Abbildung 16-4).

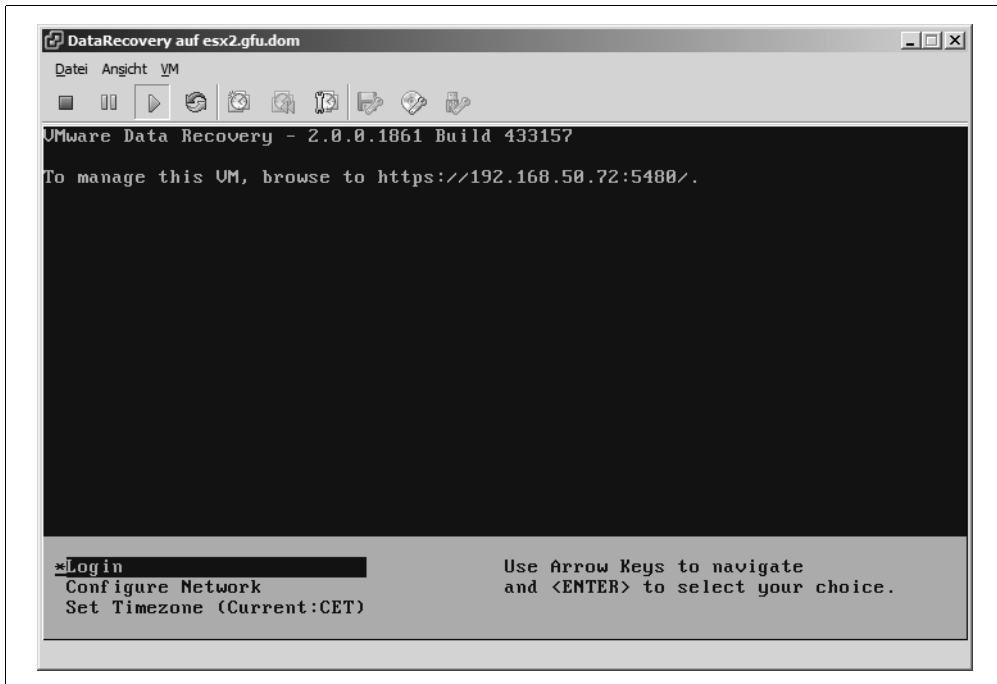


Abbildung 16-4: Konsole der Backup-Appliance

4. Falls Sie kein DHCP haben, konfigurieren Sie das Netzwerk und geben Sie die Informationen auf der dann folgenden Kommandozeile an.
5. (Optional:) Geben Sie den Benutzernamen und die Anmeldedaten für dieses System an. Wenn Sie sich zum ersten Mal bei dieser Backup-Appliance anmelden, ist der Standardbenutzername *root* und das Standardkennwort *vmw@re* (das @-Zeichen erreichen Sie auf der englischen Tastatur mit Shift+2).
6. (Optional:) Sofern das Standardkennwort des *root*-Kontos noch nicht geändert wurde, verwenden Sie den Befehl *passwd*, um das Kennwort des Stammkontos zu ändern.
7. Schließen Sie das Konsolenfenster. Die Backup-Appliance bleibt eingeschaltet und ist bereit, die Sicherungsaufgaben durchzuführen.

## Die Backup-Appliance konfigurieren

Sie können optional über die Webschnittstelle die Backup-Appliance neu starten oder Netzwerkeinstellungen an Ihre Bedürfnisse anpassen.

Falls es noch nicht geschehen ist, schalten Sie die Backup-Appliance ein, bevor Sie mit der Konfiguration beginnen.

1. Geben Sie die URL der Backup-Appliance gefolgt von einem Doppelpunkt (:) und der Portadresse 5480 in einem Webbrowser ein. Die URL der Backup-Appliance wird in der Appliance-Konsole angezeigt. Öffnen Sie dazu die Appliance-Konsole über den vSphere Client.
2. Geben Sie den Benutzernamen und das Kennwort für das Administratorkonto ein.
3. Klicken Sie auf die Registerkarte SYSTEM, um Informationen über die Appliance abzurufen, oder klicken Sie auf NEU STARTEN bzw. HERUNTERFAHREN.
4. Klicken Sie auf die Registerkarte NETZWERK und anschließend auf STATUS, um Informationen zu den aktuellen Netzwerkeinstellungen anzuzeigen.
5. Klicken Sie auf die Registerkarte NETZWERK und wählen Sie ADRESSE, um die Netzwerkeinstellungen zu konfigurieren. Sie können die Backup-Appliance so konfigurieren, dass sie ihre Adresse von DHCP erhält, oder IP-Einstellungen manuell festlegen.
6. Klicken Sie auf die Registerkarte NETZWERK und anschließend auf PROXY, um Proxy-Einstellungen festzulegen. Wenn Sie die Backup-Appliance für die Verwendung eines Proxy-Servers konfigurieren möchten, geben Sie den Namen oder die IP-Adresse und den Port für den Proxy-Server ein.

## Assistent für erste Schritte

Mit dem Assistenten für erste Schritte können Sie die Systemkonfiguration vornehmen, die für die Sicherung virtueller Maschinen notwendig ist.

Bevor Sie den Assistenten verwenden können, müssen Sie die Backup-Appliance mit dem vCenter Server verbinden (siehe oben).

1. Wählen Sie im vSphere Client HOME → LÖSUNGEN UND ANWENDUNGEN → VMWARE DATA RECOVERY.
2. Erweitern Sie die Anzeige auf der linken Fensterhälfte, bis Sie Ihre Appliance sehen, und klicken Sie sie an. Der Name wird fett dargestellt und automatisch in das Feld rechts eingetragen. Klicken Sie auf VERBINDEN.
3. Geben Sie auf der Seite ANMELDEDATEN den Benutzernamen und das Kennwort für den vCenter Server ein und klicken Sie auf WEITER (siehe Abbildung 16-5). Data Recovery verwendet diese Informationen zum Herstellen einer Verbindung mit dem vCenter Server, um Sicherungen zu erstellen. Das angegebene Benutzerkonto muss über administrative Rechte verfügen.



Abbildung 16-5: Anmeldeinformation für den vCenter Server

4. Klicken Sie anschließend auf WEITER und wählen Sie auf der Seite SICHERUNGSZIEL aus der Auswahlliste ein Ziel für die Sicherung und die Aufgaben aus, die Sie durchführen möchten.

- Klicken Sie auf AKTUALISIEREN, wenn Sie den SCSI-Bus für hinzugefügte SCSI-Festplatten erneut prüfen möchten.
- Um eine virtuelle Festplatte zu formatieren, die hinzugefügt wurde, klicken Sie auf FORMATIEREN. Nach der Formatierung wird die Festplatte als `scsi:x:y` angezeigt. Festplatten, die bereits Daten enthalten, sollten Sie mounten, statt sie zu formatieren, sonst werden alle Daten gelöscht.
- Klicken Sie zum Anschließen einer Festplatte, die einen vorhandenen Deduplizierungsspeicher enthält, auf MOUNTEN.
- Klicken Sie zum Mounten der Microsoft-CIFS-Freigabe auf NETZWERKFREIGABE HINZUFÜGEN und geben Sie die Anmeldedaten ein. Diese Anmeldedaten werden in der Appliance gespeichert – das erneute Mounten wird also automatisch ausgeführt, wenn die Appliance neu gestartet wird.

5. Klicken Sie auf WEITER.

Beachten Sie bei Netzwerkfreigaben das Hinweisfenster (siehe Abbildung 16-6). Beachten Sie zusätzlich, dass VDR Schreibberechtigungen benötigt, da die Freigabe sonst nicht hinzugefügt werden kann.

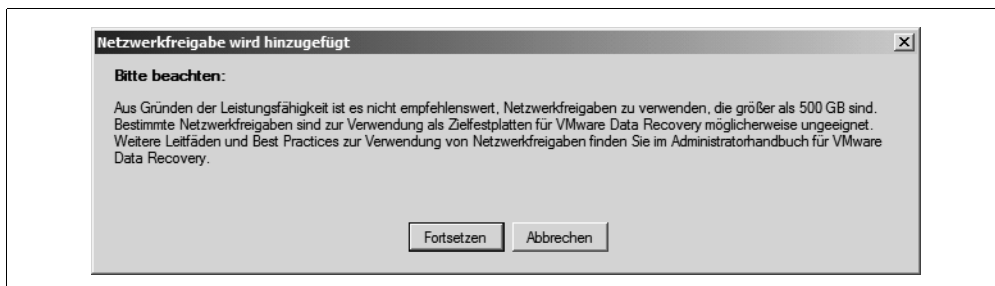


Abbildung 16-6: Warnmeldung Netzwerkfreigabe

Die notwendige Systemkonfiguration ist nun abgeschlossen und der Assistent NEUE SICHERUNGSAUFGABE ERSTELLEN wird automatisch geöffnet.

## Sicherungsaufgaben erstellen

Mithilfe von *Sicherungsaufgaben* legen Sie fest, welche virtuellen Maschinen gesichert werden sollen und wo und wie lange die Sicherungen gespeichert werden.

### VIRTUELLE MASCHINEN

Wählen Sie Gruppen von virtuellen Maschinen aus, z.B. alle virtuellen Maschinen in einem Datencenter, oder wählen Sie eine einzelne oder mehrere virtuelle Maschinen aus. Wenn Sie den gesamten Ressourcenpool, einen Host, ein Datencenter oder einen Ordner auswählen und neue virtuelle Maschinen zu einem dieser Container hinzufügen, sind diese in den nachfolgenden Sicherungen enthalten.

Wählen Sie eine einzelne virtuelle Maschine aus, werden alle zur virtuellen Maschine hinzugefügten Festplatten gesichert. Falls Sie eine virtuelle Maschine vom ausgewählten Container in einen anderen Container verschieben, wird sie nicht mehr gesichert.

Gruppieren Sie Ihre VMs möglichst nach dem Betriebssystem, damit die Deduplizierung korrekt funktioniert.

### ZIEL

Sie können Sicherungen auf Netzwerkfreigaben, in VMDKs oder auf RDMs speichern. Wenn Sie Sicherungen auf einer Netzwerkfreigabe speichern wollen und diese nicht verfügbar ist, können Sie eine andere Netzwerkfreigabe hinzufügen (siehe Abbildung 16-7).

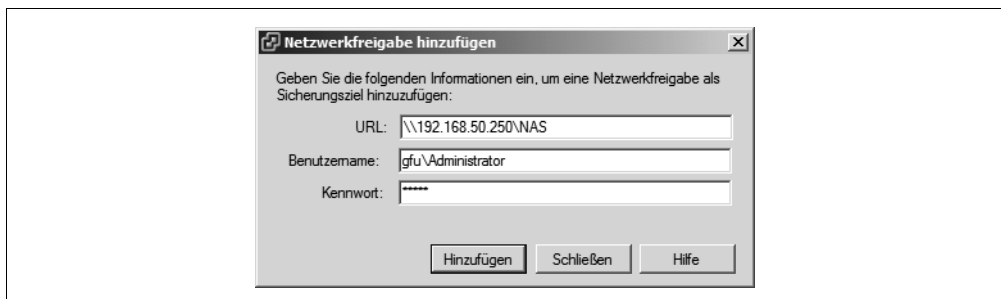


Abbildung 16-7: Netzwerkfreigabe hinzufügen

Sie müssen VMDKs und RDMs vorher partitionieren und formatieren, um Sicherungen darauf speichern zu können. Sie können Ziele, bei denen das noch nicht geschehen ist, jederzeit formatieren bzw. partitionieren.

### SICHERUNGSFENSTER

Standardmäßig werden Sicherungsaufgaben von Montag bis Freitag von nachmittags bis morgens und am Samstag und Sonntag zu jeder beliebigen Zeit ausgeführt (siehe

Abbildung 16-8). Data Recovery versucht, alle der Aufgabe zugewiesenen virtuellen Maschinen einmal täglich innerhalb des Sicherungsfensters zu sichern. Falls bei der Durchführung eines Sicherungsvorgangs der für das Sicherungsfenster festgelegte Zeitraum überschritten wird, wird die Sicherung gestoppt. Sie wird erneut gestartet, sobald sich das nächste Sicherungsfenster öffnet.

Falls während des ersten angegebenen Zeitraums zu viele virtuelle Maschinen von Data Recovery gesichert werden sollen, werden einige davon möglicherweise nicht gesichert. Letztendlich werden jedoch alle virtuellen Maschinen gesichert, und die nachfolgenden Sicherungen können in der Regel innerhalb eines Sicherungsfensters durchgeführt werden.

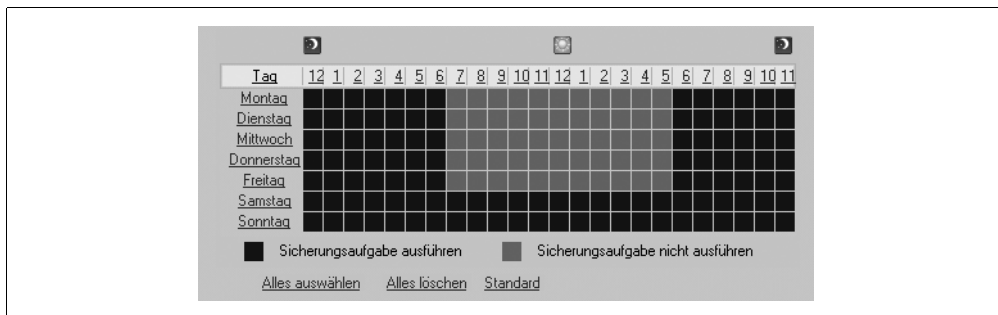


Abbildung 16-8: Sicherungszeiten

Wenn einige Maschinen während eines Sicherungsfensters nicht gesichert werden können, erhalten diese Maschinen in den nachfolgenden Sicherungen eine höhere Priorität. Dadurch wird sichergestellt, dass alle virtuellen Maschinen so oft gesichert werden, wie die Sicherungsfenster und die Ressourcen es zulassen. So wird verhindert, dass einige virtuelle Maschinen immer und andere niemals gesichert werden.

#### AUFBEWAHRUNGSRICHTLINIE

Von Data Recovery vorgenommene Sicherungen werden für einen einstellbaren Zeitraum aufbewahrt. Sie können festlegen, ob Sie mehr oder weniger Sicherungen für einen längeren oder kürzeren Zeitraum aufbewahren möchten. Wird eine größere Anzahl an Sicherungen aufbewahrt, wird natürlich mehr Festplattenplatz belegt, es stehen dann aber auch mehr Zeitpunkte für die Wiederherstellung virtueller Maschinen zur Verfügung. Mit zunehmendem Alter werden einige Sicherungen automatisch gelöscht, um Platz für neue Sicherungen zu schaffen. Auch das lässt sich beliebig einstellen.

Sie können eine vordefinierte Aufbewahrungsrichtlinie auswählen oder eine eigene Richtlinie erstellen.

#### BEREIT ZUM ABSCHLIEßEN

Überprüfen Sie die Einstellungen für die Sicherungsaufgabe. Diese Seite enthält folgende Informationen:

- Welche virtuellen Maschinen von diesem Job gesichert werden.



- Wo die Sicherungen für die angegebenen virtuellen Maschinen gespeichert werden.
- Den Zeitplan für das Sichern der virtuellen Maschinen.
- Die Anzahl der Sicherungen, die für die jeweiligen Zeiträume aufbewahrt werden (beispielsweise die Anzahl der Sicherungen, die pro Monat aufbewahrt werden).

## Assistent für Sicherungsaufgaben

Mit dem Assistenten für Sicherungsaufgaben können Sie angeben, welche virtuellen Maschinen wann gesichert werden sollen.

1. Wählen Sie im vSphere Client HOME → LÖSUNGEN UND ANWENDUNGEN → VMWARE DATA RECOVERY.
2. Klicken Sie auf NEUE SICHERUNGSAUFGABE, um den Assistenten für Sicherungsaufgaben zu starten.
3. Wählen Sie auf der Seite VIRTUELLE MASCHINEN einzelne virtuelle Maschinen oder Container aus, die zu sichernde virtuelle Maschinen enthalten, und klicken Sie auf WEITER.
4. Akzeptieren Sie auf der Seite SICHERUNGSFENSTER die Standardzeiten oder geben Sie alternative Sicherungszeiten an und klicken Sie auf WEITER.
5. Akzeptieren Sie auf der Seite AUFBEWAHRUNGSRICHTLINIE die standardmäßige Aufbewahrungsrichtlinie oder geben Sie eine alternative Aufbewahrungsrichtlinie an (siehe Abbildung 16-9). Klicken Sie dann auf WEITER.

Die Aufbewahrungsrichtlinie legt die Anzahl der Sicherungen fest, die auf dem Zielmedium aufbewahrt werden, sowie die Dauer der Aufbewahrung. Ältere Sicherungen, die nicht durch die Aufbewahrungsrichtlinie geschützt sind, werden bei Bedarf gelöscht, um Platz für neue Sicherungen freizumachen.

Aufbewahrungsrichtlinie: ☐ Wenige ☒ Mehr ☐ Viele ☐ Benutzerdefiniert

Richtlinienbeschreibung: Diese Richtlinie sorgt dafür, dass mehr Sicherungen von virtuellen Maschinen gespeichert werden als mit der Option 'Wenige'. Wählen Sie diese Richtlinie, wenn Sie mehr als nur die neuesten Sicherungen aufbewahren müssen.

Richtliniendetails: Diese Richtlinie behält mindestens die letzten  Sicherungen bei, sowie jeweils die letzte Sicherung aus den letzten:

- Wochen
- Monaten
- Quartalen
- Jahren

Abbildung 16-9: Aufbewahrungsrichtlinien für Backups virtueller Maschinen

6. Überprüfen Sie auf der Seite **BEREIT ZUM ABSCHLIEßEN** die zusammengefassten Informationen für die Sicherungsaufgabe und klicken Sie auf **WEITER**.

## Eine Netzwerkfreigabe hinzufügen

Sie können eine Netzwerkfreigabe einrichten, die zum Speichern von Sicherungen verwendet wird. Auch hier greift die Deduplizierung automatisch. Geben Sie die notwendigen Informationen über die Netzwerkfreigabe an, auf der Data Recovery die Daten speichern kann. Es handelt sich dabei normalerweise um die folgenden Informationen:

- *URL* – Der Ort, an dem sich die Netzwerkfreigabe befindet. Sie müssen eine IP-Adresse angeben. Servernamen werden nicht unterstützt.
- *Benutzername* – Der Benutzername eines Kontos mit den erforderlichen Schreibberechtigungen für die Netzwerkfreigabe. Achten Sie darauf, dass seit Windows XP die Windows-Freigabe standardmäßig nur mit Leserechten versehen wird. **ÄNDERN** reicht als Berechtigung.
- *Kennwort* – Das Kennwort für das Benutzerkonto mit Schreibrechten.

## Ein Volume formatieren

VMware Data Recovery kann Sicherungen auf Netzwerkvolumes, VMDKs und RDMs speichern. Netzwerkvolumes erfordern üblicherweise keine Formatierung, VMDKs und RDMs müssen aber vor ihrer Benutzung formatiert werden.

Bei der Formatierung eines Volume wird der Speicherplatz automatisch richtig partitioniert und formatiert. Alle darauf befindlichen Daten werden natürlich gelöscht. Formatieren Sie nach Bedarf das Volume, das Sie zum Speichern der Sicherung verwenden möchten.

## Virtuelle Maschinen wiederherstellen

Mithilfe des Wiederherstellungsassistenten wählen Sie die virtuellen Maschinen aus, die wiederhergestellt werden sollen. Zudem können Sie angeben, wie und wo sie wiederhergestellt werden sollen.

Mit Data Recovery können Sie testen, wie eine virtuelle Maschine wiederhergestellt würde, und auch den tatsächlichen Wiederherstellungsvorgang. Bei Probewiederherstellungen werden virtuelle Maschinen aus den angelegten Wiederherstellungspunkten erstellt. Aus Probewiederherstellungen erstellte virtuelle Maschinen ersetzen keine aktuellen virtuellen Maschinen, sondern dienen dazu, zu überprüfen, ob Backups von virtuellen Maschinen erwartungsgemäß erstellt und erfolgreich wiederhergestellt werden können. Sie können dazu auch noch den Datenträger ändern, ob die NIC verbunden ist und ob die VM eingeschaltet werden soll, wenn der Vorgang beendet ist. Die tatsächliche

Wiederherstellung einer virtuellen Maschine versetzt sie also in einen ausgewählten vorherigen Zustand.

Der Wiederherstellungsassistent bietet sowohl bei Wiederherstellungen als auch bei Probewiederherstellungen die Möglichkeit, die Quelle und das Ziel für das Wiederherstellen einer virtuellen Maschine zu konfigurieren (siehe Abbildung 16-10).

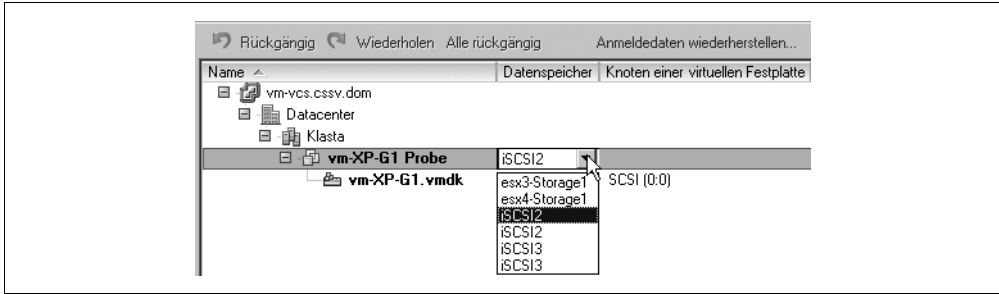


Abbildung 16-10: Probewiederherstellung einer VM



Manchmal lässt sich eine gesicherte *.vmdk*-Datei nur dort wiederherstellen, wo sie gespeichert wurde. Fällt Ihnen also ein Datenträger aus oder löschen Sie versehentlich den Ordner der VM, müssen Sie diesen erst wieder einrichten. Das bedeutet:

- Sie erstellen einen Datenträger/ein Volume mit dem gleichen Namen.
- Sie erstellen einen Ordner mit dem gleichen Namen, den er vor dem Ausfall hatte.
- Sie kopieren alle Dateien einer anderen VM in den Ordner und benennen diese so, wie die Dateien vorher hießen

Dann erst lässt sich die *.vmdk*-Datei zurückspielen. Eine Probewiederherstellung sollte dennoch möglich sein – jedoch heißt die VM dann z.B. nicht mehr *VM1*, sondern *VM1-Probe*. Hier sind große Probleme vorprogrammiert. Testen Sie unbedingt vorher alle möglichen Szenarien durch, damit in einer Stresssituation nichts schiefgeht! Oder benutzen Sie ein anderes Sicherungsprogramm, z.B. *Veeam* (preisgünstig) oder *vRanger* von Quest, ehemals *Vizioncore* (Empfehlung des Autors).



Wenn eine VM in der Bestandsliste umbenannt wurde und dann auf einen anderen Datenträger verschoben wird, ändern sich der Name des beteiligten Ordners, nicht aber die Dateien und nicht der Name im Betriebssystem der VM.

## Quellauswahl

Wählen Sie zunächst aus der Baumansicht der gesicherten vSphere-Objekte die Quelle aus. Wählen Sie dann die wiederherzustellenden virtuellen Maschinen und virtuellen Festplatten aus.

Anhand von Filtern können Sie nur den relevanten Teil der verfügbaren Auswahl anzeigen lassen. Ähnlich wie beim Erstellen von Sicherungsaufgaben können Sie Sammlungen von virtuellen Maschinen angeben, z. B. alle virtuellen Maschinen in einem Datacenter oder einzelne virtuelle Maschinen bzw. *.vmdk*-Dateien. Wenn Sie für eine einzelne virtuelle Maschine mehrere Wiederherstellungspunkte ausgewählt haben, stellt Data Recovery diese Maschine anhand des zuletzt ausgewählten Wiederherstellungspunkts wieder her.

## Zielauswahl

Diese Seite enthält eine Baumansicht des Speicherorts, an dem gesicherte Objekte wiederhergestellt werden, und Informationen darüber, wie diese Objekte bei der Wiederherstellung konfiguriert werden. Falls es seit der letzten Sicherung Änderungen in Ihrer Bestandslistenhierarchie gegeben hat, werden die Pfade nicht mehr vorhandener Bestandslistenobjekte grau dargestellt. VM-Dateien, die an Speicherorten gesichert wurden, die nicht mehr vorhanden sind, müssen in gültige Speicherorte verschoben werden, damit der Wiederherstellungsvorgang durchgeführt werden kann.

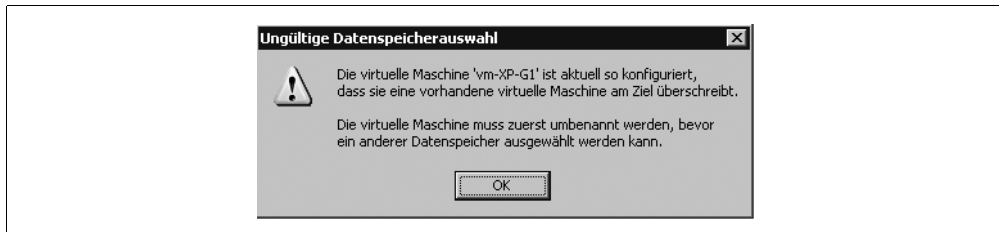


Abbildung 16-11: Warnmeldung zur Wiederherstellung

Um die Fehlermeldung aus Abbildung 16-11 zu vermeiden, können Sie Optionen neu konfigurieren, beispielsweise ...

- ... den Datenspeicher und den Knoten der virtuellen Festplatte, in dem die Dateien wiederhergestellt werden.
- ... ob die Konfiguration wiederhergestellt werden soll. Wenn die Konfiguration nicht wiederhergestellt wird, wird möglicherweise die Konfiguration einiger anderer Optionen nicht unterstützt. Beispielsweise kann in diesem Fall möglicherweise eingestellt werden, ob die virtuelle Maschine eingeschaltet wird, jedoch nicht, ob die Netzwerkkarte verbunden wird.
- ... ob die Netzwerkkarte verbunden wird.
- ... ob die virtuelle Maschine eingeschaltet wird.

Virtuelle Maschinen und VMDKs können entweder per Ziehen und Ablegen oder durch Auswählen neuer Ziele aus dem Pop-up-Baum verschoben werden. Klicken Sie zum Anzeigen weiterer Informationen über die vorhandene Bestandsliste auf den Link im oberen Teil der Seite. Benennen Sie zum Klonen einer virtuellen Maschine die virtuelle

Maschine um, die Sie wiederherstellen wollen. Wenn die Standardanmeldeinformation für das Backup keine Wiederherstellungsrechte aufweist, können Sie alternative Anmeldedaten angeben.

## Bereit zum Abschließen

Überprüfen Sie die Einstellungen für die Sicherungsaufgabe. Diese Seite enthält eine Baumstruktur von dem, was wiederhergestellt werden soll, sowie zusammenfassende Informationen. Die Baumstruktur enthält beispielsweise folgende Angaben:

- Objektnamen
- Wann der Wiederherstellungspunkt erstellt wurde
- Welcher Datenspeicher als Ziel für wiederhergestellte virtuelle Maschinen oder virtuelle Festplatten verwendet wird
- Informationen zum Knoten einer virtuellen Festplatte
- Ob die Konfiguration wiederhergestellt wird
- Ob die Netzwerkkarte verbunden wird
- Ob die virtuelle Maschine eingeschaltet wird

Die Zusammenfassung enthält die folgenden Informationen:

- Wie viele virtuelle Maschinen überschrieben werden
- Wie viele virtuelle Maschinen gegebenenfalls erstellt werden
- Wie viele virtuelle Festplatten überschrieben werden
- Wie viele virtuelle Festplatten gegebenenfalls erstellt werden
- Die Gesamtmenge an Daten, die wiederhergestellt wird



Falls auf dem Zieldatenspeicher nicht genügend Speicherplatz zum Durchführen des Wiederherstellungsvorgangs zur Verfügung steht, wird eine Warnung angezeigt. Sie können andere Datenspeicher mit einer höheren Kapazität angeben oder in Kauf nehmen, dass Wiederherstellungen möglicherweise nicht wie erwartet abgeschlossen werden.

## Erstellen einer Probewiederherstellung

Führen Sie eine Probewiederherstellung durch, um sicherzugehen, dass eine virtuelle Maschine erwartungsgemäß gesichert wurde und dass ein erfolgreicher Wiederherstellungsvorgang durchgeführt werden kann.

1. Wählen Sie im vSphere Client HOME → LÖSUNGEN UND ANWENDUNGEN → VMWARE DATA RECOVERY.
2. Klicken Sie mit der rechten Maustaste in der linken Seite des Fensters auf eine virtuelle Maschine, für die eine Sicherung verfügbar ist, und wählen Sie PROBE-WIEDER-

HERSTELLUNG. Der Wiederherstellungsassistent für virtuelle Maschinen wird mit der geöffneten Seite **BEREIT ZUM ABSCHLIEßEN** angezeigt.

3. Klicken Sie auf **WIEDERHERSTELLEN**, um die Probewiederherstellung durchzuführen, oder auf **ZURÜCK**, um die Einstellungen zu ändern.

Eine Version der virtuellen Maschine wird in der Bestandsliste wiederhergestellt.

Danach können Sie die virtuelle Maschine löschen, die beim Testen des Wiederherstellungsvorgangs erstellt wurde.

## Wiederherstellen virtueller Maschinen von einer Sicherung

Das Wiederherstellen virtueller Maschinen auf den Stand einer vorherigen Sicherung geschieht anhand des Wiederherstellungsassistenten für virtuelle Maschinen.

1. Wählen Sie im vSphere Client **HOME** → **LÖSUNGEN UND ANWENDUNGEN** → **VMWARE DATA RECOVERY**.
2. Geben Sie den Namen der virtuellen Maschine oder die IP-Adresse der Backup-Appliance ein und klicken Sie auf **VERBINDEN**.
3. Wechseln Sie zur Registerkarte **WIEDERHERSTELLEN** und klicken Sie auf den Link **WIEDERHERSTELLEN**, um den Wiederherstellungsassistenten für virtuelle Maschinen zu starten. Dieser wird nun angezeigt.
4. Geben Sie auf der Quellauswahlseite eine Quelle an, von der die virtuellen Maschinen wiederhergestellt werden sollen, und klicken Sie auf **WEITER**.
5. Geben Sie auf der Zielauswahlseite an, wie wiederhergestellte Maschinen konfiguriert werden sollen, und klicken Sie auf **WEITER**.
6. Überprüfen Sie auf der Seite **BEREIT ZUM ABSCHLIEßEN** die Konfiguration und klicken Sie auf **WIEDERHERSTELLEN**.

Die virtuellen Maschinen werden wiederhergestellt, wie es im Assistenten angegeben wurde.

## Dateien aus einer Sicherung wiederherstellen

Zum Umfang von Data Recovery gehört je ein Programm, um Windows- und Linux-Dateien aus einer Sicherung wiederherstellen zu können. Auf der CD oder dem ISO-Image von Data Recovery befinden sich die Dateien *WinFLR.exe* und *LinuxFLR.exe*. Da es sich dabei jeweils um eine Runtime-Version für Windows handelt, müssen die Dateien auf einem Speicher liegen, auf dem diese entpackt werden können. Kopieren Sie diese zum Beispiel auf eine Netzwerkfreigabe oder einen lokalen Ordner, um einzelne Dateien aus einer Sicherung an einen anderen Ort kopieren zu können. Sie können diese Funktion natürlich auch auf dem vCenter Server zur Verfügung stellen.

Wollen Sie Dateien aus einer Sicherung von einer Windows-VM bekommen, führen Sie einfach das dazugehörige Programm *WinFLR.exe* aus. Brauchen Sie Daten aus einer Linux-Maschine, nehmen Sie *LinuxFLR.exe*. Eine Version, die unter Linux selbst läuft, gibt es nicht.

Nachdem das Programm entpackt wurde, wird es automatisch gestartet und ein Fenster wird angezeigt. Wenn Sie die Anwendung nicht auf dem vCenter Server ausführen, müssen Sie im unteren Teil auf ERWEITERT klicken, um die Anmeldeinformationen für den vCenter Server eingeben zu können.

Nach erfolgreicher Anmeldung beim Data Recovery-Modul erscheinen die gesicherten Festplatten der virtuellen Maschinen. Suchen Sie sich die gewünschte Sicherung aus und klicken Sie auf MOUNTEN. Damit wird auf Ihrem Rechner eine Verknüpfung zu den in der Sicherung enthaltenen Festplatten auf *C:\<Datum+Uhrzeit>* eingerichtet. Dieses Verzeichnis enthält bei einer Windows-Sicherung die Laufwerksbuchstaben des gesicherten Systems. Mit dem Explorer können nun beliebige Dateien im Verzeichnisbaum gesucht und kopiert werden. Eine Änderung oder Löschung der Dateien ist nicht möglich.

Haben Sie eine VM von der Hardwareversion 4 auf 7 oder 8 hochgestuft, können beim Mounten der Festplatte Probleme auftauchen. Das liegt daran, dass die benötigten Treiber nicht auf dem Rechner zur Verfügung stehen. Abhilfe können Sie nur schaffen, indem Sie die alten Treiber deinstallieren und anschließend die neuen installieren. Über SYSTEMSTEUERUNG → SOFTWARE kann das Data Recovery-Plugin deinstalliert und über das oben erwähnte *.msi*-File wieder installiert werden.

## Den vCenter Server wiederherstellen

Mit der neuen Version von DR ist es jetzt auch möglich, den vCenter Server selbst wiederherzustellen:

1. Melden Sie sich direkt auf dem Host an, wo der vCenter Server lief. Das Data Recovery-Plugin muss installiert sein.
2. Trennen Sie den Host vom vCenter Server, indem Sie auf der Registerkarte ÜBERSICHT unter der Rubrik HOSTVERWALTUNG den Link HOST VON vCENTER SERVER TRENNEN anklicken. Dazu muss der ESXi Server nicht in den Wartungsmodus gefahren werden.
3. Gehen Sie zur Wiederherstellung wie oben beschrieben vor.
4. Ist der vCenter Server wieder vorhanden, können Sie ihn direkt starten.
5. Melden Sie sich am vCenter Server an und verbinden Sie den Host wieder.

## Probleme mit DR beheben

Das Protokoll von Data Recovery ist verkehrt herum: Die ältesten Einträge sind oben, die neuesten unten. Darin stehen nur Informationen, die direkt mit der Sicherung zu tun

haben. Fehler, die das System selbst entdeckt hat, findet man nur innerhalb des Betriebssystems auf der Kommandozeile mit dem Befehl `less /var/log/messages`.

VMs, die nicht komplett gesichert wurden, behalten ihre Snapshots, und ihre Festplatte ist an DR gebunden. Damit sieht es manchmal so aus, als hätte DR 20 oder mehr Festplatten und würde erheblichen Storage-Platz belegen. Das ist aber nicht so. Lediglich die Snapshots belegen unnötig Platz. Sollte das Backup bis zur angegebenen Zeit niemals fertig werden, wird immer wieder ein neuer Snapshot der VM erstellt und es tauchen erhebliche Probleme auf.

Um diese Probleme in den Griff zu bekommen, können Sie entweder das Zeitfenster vergrößern oder die Datensicherungen anders aufteilen. Sichern Sie die VMs vielleicht abwechselnd nur alle zwei Tage. Das ist immer noch besser als gar keine Sicherung. Hilft das alles nichts, müssen Sie die Snapshots manuell in die VM integrieren. Gehen Sie dazu wie folgt vor:

1. Melden Sie sich am vCenter Server an und klicken Sie auf die betreffende Maschine.
2. Wählen Sie aus dem Kontextmenü SNAPSHOT → KONSOLIDIEREN aus.
3. Wenn der Vorgang abgeschlossen ist – das sehen Sie unter KÜRZLICH BEARBEITETE AUFGABEN – öffnen Sie den Snapshot Manager, ebenfalls über das Kontextmenü.
4. Wählen Sie die Schaltfläche ALLE LÖSCHEN.

Der Vorgang kann mehrer Stunden in Anspruch nehmen, die VM läuft dabei aber ganz normal weiter.

## Empfehlungen zu Data Recovery

Wenn Sie die obigen Ausführungen aufmerksam durchgelesen haben und berücksichtigen, ist das Tool eine einfache und kostengünstige Möglichkeit, alle virtuellen Maschinen zu sichern. Behalten Sie aber unbedingt die Ereignisse von Data Recovery im Auge.

Bei der ersten Sicherung einer VM (oder wenn ein anderer Storage dafür zur Verfügung gestellt wurde) kann das Backup sehr lange dauern. Die Nachfolgesicherungen sind deutlich schneller und Sie können die Zeiten ggf. anders planen.

Schauen Sie sich alle paar Tage die Ereignisse auf der Appliance an. Dort steht, ob die Sicherung erfolgreich war oder nicht (siehe Abbildung 16-12).

| Datum             | Beschreibung                                                                                 | Warnun |
|-------------------|----------------------------------------------------------------------------------------------|--------|
| 03.12.11 08:18:07 | 192 KP6 DH (192 KP6 DH): Aufgabe unvollständig                                               | 0, 2   |
| 03.12.11 08:18:07 | Aufgabe "192 KP6 DH (192 KP6 DH)" unvollständig                                              | 0, 1   |
| 03.12.11 08:18:07 | Can't access destination /10.1.1.46/vmware2/, Fehler -1101 (Datei/Verzeichnis nicht gefur    | 0, 1   |
| 03.12.11 08:17:33 | 168 Domaincontroller B (168 Domaincontroller B): 1 task errors                               | 1, 1   |
| 03.12.11 08:17:34 | Aufgabe "168 Domaincontroller B (168 Domaincontroller B)" abgeschlossen mit 1 Fehler         | 1, 0   |
| 03.12.11 08:17:34 | Can't access destination /, Fehler -2261 (kann das Ziel erst verwenden, wenn die Integrität: | 0, 1   |

Abbildung 16-12: Fehler in der Ereignisanzeige



Behalten Sie die Anzahl der Snapshots im Auge. Ab 32 gemachten Snapshots können erhebliche Probleme mit der VM auftreten, bis hin zu Datenverlusten. Nur weil die Sicherung einmal geklappt hat, muss das kein Dauerzustand sein.

Sehen Sie auf den Storages, auf denen die Backups liegen, ab und zu nach, ob dort noch genug Platz für neue Sicherungen zur Verfügung steht.

Machen Sie in regelmäßigen Abständen eine Probewiederherstellung, um das Backup zu überprüfen. Nehmen Sie dafür jedes Mal eine andere VM. Das kann auch ein Azubi in seinen Kalender reinschreiben und regelmäßig durchführen.

Überdenken Sie die Datenaufbewahrungsrichtlinie: Wenn die letzten sieben Tagessicherungen, die letzten vier Wochensicherungen, die letzten drei Monatssicherungen und eine Jahressicherung vorgehalten werden sollen, liegen auf der Sicherungsfestplatte anschließend 15 Sicherungen der VM. Wenn Sie ein Backup dieser Dateien auf Band erstellen, ist das nicht notwendig.

Wollen Sie eine Festplatte einer VM für die Sicherung aussparen, die andere Platte aber sichern, können Sie die nicht zu sichernde Festplatte in den unabhängigen – dauerhaften – Modus schalten.

## Lösungen von Quest

Die amerikanische Firma Vizioncore aus Chicago wurde im Jahr 2002 zum Teil von ehemaligen Mitarbeitern von VMware gegründet, um als Dritthersteller Tools für VMware-Produkte herzustellen. Schon drei Jahre später brachte man die Backup-Lösung *esxRanger* auf den Markt. Vor Kurzem wurde die Firma von Quest übernommen. Die Produkte sind jetzt über diesen Anbieter zu bekommen.

Folgende Produkte bietet Quest unter anderem derzeit an:

- *vRanger*: Backup, integriert in vCenter Server, differenzielle Sicherungen und Datei-wiederherstellung, angeblich schnellste Sicherungslösung für vSphere
- *vConverter*: Konvertierung von etlichen Formaten und Import von physischen Maschinen
- *vReplicator*: Replikation laufender virtueller Maschinen, z.B. für Disaster Recovery
- NetVault Backup, Virtual Data Protection, vFoglight, vFoglight Storage, vOptimizer Waste Finder und andere

Unter <http://www.quest.com/virtualization/> können Sie weitere Informationen (z. T. als Videos) und auch Testversionen beziehen. Zu jedem Angebot gibt es ausführliche Beschreibungen, Dokumente und Whitepaper.

Gerade in mittleren und größeren Umgebungen empfehle ich den Einsatz des vRanger für Backups. Verlassen Sie sich dabei nicht auf das Produkt von VMware – es bietet sich eher bei kleineren Unternehmen an.

# Lösungen von Veeam

Die amerikanische Firma Veeam Software mit Hauptsitz in Columbus (USA) entwickelt Produkte für Datensicherung und Management in virtuellen Umgebungen. Sie wurde im Jahre 2006 gegründet.

Das kostenlos angebotene Tool FastSCP wird nach Angaben von Veeam von über 150.000 IT-Fachkräften eingesetzt und ist damit das meistgenutzte Tool für das VMware-Management (siehe auch Kapitel 18).

Die Firma bietet noch weitere interessante Tools an. Informationen zu ihnen finden Sie auf ihrer Website.

## Veeam Backup & Replication

Die Backuplösung *Veeam Backup & Replication* ist Ende November 2011 in der Version 6 erschienen und macht einen sehr guten Eindruck. Eine 30-Tage-Testversion kann unter [www.veeam.com/de](http://www.veeam.com/de) heruntergeladen werden. In dem Paket ist auch das Tool *FastSCP* enthalten, das ich in Kapitel 18 vorstelle. Lizenziert wird hier pro CPU mit bis zu sechs Kernen und einem Jahr Unterstützung. Eine Verlängerungslizenz ist für deutlich geringere Kosten erhältlich. Dieses Produkt wurde in der Vergangenheit mehrfach ausgezeichnet, z. B. als Produkt des Jahres und »Best of vmworld« 2010 und 2011.

Ebenso wie Data Recovery unterstützt Backup & Replication deduplizierten Speicher sowie Kompression vor der Übertragung auf das Sicherungsmedium, was die Netzwerkbelastung und den Storagebedarf deutlich verringert.

Eine sehr interessante Lösung ist die integrierte Near-CDP (Near-Continuous Data Protection). Damit werden Änderungen an virtuellen Maschinen erkannt und die vorher erstellten Images laufend aktualisiert (Replikation).

VMs können im Katastrophenfall direkt über die Datensicherung gestartet werden – das Zurückspielen der gesicherten VM kann dann später erfolgen. Auch lässt sich eine Art Sandbox nutzen, um in einer gesicherten Umgebung ein Backup zu überprüfen.

Selbstverständlich können auch wie bei Data Recovery über das File Level Restore einzelne Dateien aus der Sicherung wiederhergestellt werden.

Ich empfehle dieses Produkt und ziehe es dem in vSphere integrierten Data Recovery vor.

---

# Sicherheit in der virtuellen Umgebung

Die Sicherheit wird bei vSphere5 von VMware groß geschrieben. Über viele Menüs und Konfigurationsdateien lassen sich hier noch weitere Einstellungen vornehmen, um die gesamte Umgebung an eigene Sicherheitsbedürfnisse anzupassen. Das umfasst nicht nur die Zugriffe über WebAccess, vSphere Client und die Firewall, sondern noch mehrere weitere Zugriffe, an die man zunächst einmal gar nicht denkt.

In diesem Kapitel werden die wichtigsten Einstellungsmöglichkeiten zur Sicherheit in der vSphere-Umgebung vorgestellt.

## Die Architektur der Sicherheitsfeatures

In diesem Abschnitt geht es um die Sicherheitsfeatures der Speicher, des Netzwerks und des ESXi Servers.

### Speichersicherheit

Zunächst einmal unterscheidet man zwischen lokalen Festplatten und entferntem Speicher wie Fibre-Channel, Hard- und Software-iSCSI sowie NFS (*Network File System*).

Über das sogenannte *Zoning* können Zugriffsrechte für die SAN-Topologie eingestellt werden. Auf diesem Weg können Geräte außerhalb der gewählten und eingestellten Zone nicht gesehen werden. Weiterhin findet über die zugewiesenen Pfade innerhalb der *Fabric* (mehrere Pfade über Switches zum Storage) eine Kontrolle und Isolation statt. Damit wird der Zugriff von Nicht-ESXi-Systemen auf VMFS-Partitionen verhindert. Auch kann so eine Testumgebung außerhalb der Produktivumgebung keinen Schaden anrichten.



Beachten Sie dabei, dass der Speicher für Failover oder Load-Balancing innerhalb derselben Zone sein muss.

Bei sehr großen Umgebungen sollten Sie gegebenenfalls die ESXi Server bzw. die dazugehörigen Cluster, die bestimmte VMs hosten, auch im SAN separieren. Andererseits ergibt es keinen Sinn, nur zwei oder drei Hosts mit je drei bis vier virtuellen Maschinen jeweils zu separieren. Bei der Aufteilung einer solchen Infrastruktur ist ein gewisses Augenmaß erforderlich.

ESX Server ab Version 3.x unterstützen die sogenannte »Einweg-CHAP-Authentifizierung« für iSCSI-Ziele (siehe Abbildung 17-1). CHAP steht für *Challenge-Handshake Authentication Protocol*. Das heißt, dass Sie hier für die Sicherheit eine gegenseitige Hash-Regel (MD5, Message-Digest 5) erstellen können, damit unautorisierter Zugriff auf das VMFS-Volume nicht möglich ist. Diese Einstellungen erreichen Sie über die Konfiguration des ESXi Servers auf der grafischen Oberfläche unter dem Punkt STORAGE ADAPTERS. Wählen Sie dann den iSCSI-Adapter aus und klicken Sie im unteren Teil des Fensters auf PROPERTIES. Im folgenden Fenster können der Name und ein Kennwort festgelegt werden. Dieses Kennwort muss bei beiden Partnern eingegeben werden, weil es nicht übersendet wird. Vielmehr generiert jeder für sich den Hash-Wert und vergleicht ihn mit dem übermittelten. Stimmt er überein, wird der Zugriff gestattet.

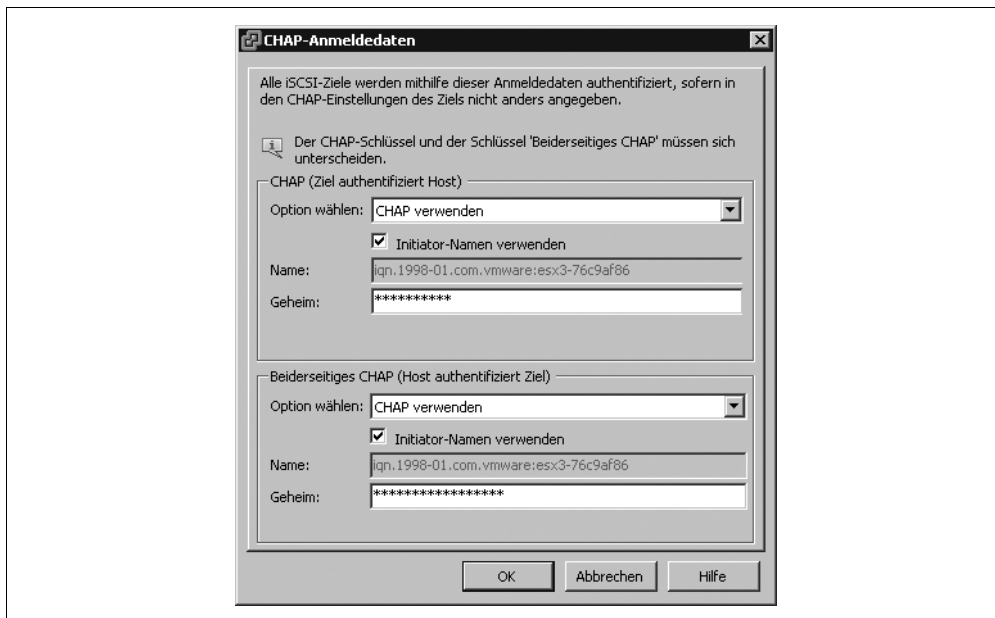


Abbildung 17-1: CHAP-Authentifizierungseinstellungen



Es ist auch möglich, anonymen Zugriff zu gewähren. Probieren Sie immer zuerst diese Methode, und erst wenn der Zugriff funktioniert, ändern Sie die Authentifizierungsanforderung – nur um sicherzugehen, dass ein etwaiges Scheitern nicht an einem falschen Passwort liegt.

## Netzwerksicherheit

Da das Thema VLAN in Kapitel 6 ausführlich beschrieben wurde, erläutere ich hier nur die Sicherheitseinstellungen der Netzwerkschwitches.

Die virtuellen Switches von VMware schützen gegen bestimmte Gefahren von VLANs. Durch den Aufbau der virtuellen Switches schützen sie VLANs gegen viele Arten von Angriffen, die meist auf VLAN-Hopping basieren. Dieser Schutz garantiert jedoch nicht, dass Ihre virtuellen Maschinen gegen andere Arten von Angriffen immun sind. So schützen virtuelle Switches zum Beispiel nicht das physische Netzwerk vor diesen Angriffen, sondern nur das virtuelle.

Die folgende Liste vermittelt Ihnen die Grundlagen zu einigen Angriffsarten, gegen die virtuelle Switches und VLANs schützen können.



Wenn Ihre Konfiguration ein iSCSI-SAN umfasst, das direkt durch den Host und nicht durch den Hardwareadapter konfiguriert wurde, sollten Sie einen eigenen virtuellen Switch anlegen, der eine gemeinsam genutzte Netzwerkkonnektivität für das Management Network und für iSCSI bietet. Diese zweite Netzwerkverbindung für das Management Network besteht zusätzlich zur primären Management Network-Netzwerkverbindung, die Sie für die Kommunikation Ihrer Management-Tools verwenden. Die zweite Management Network-Netzwerkverbindung unterstützt nur die iSCSI-Aktivitäten, und Sie sollten sie nicht für Managementaktivitäten oder die Management-Tool-Kommunikation verwenden.

- *MAC-Flooding* – Diese Angriffe überschwemmen den Switch mit Datenpaketen, die MAC-Adressen enthalten, die als von verschiedenen Quellen stammend gekennzeichnet wurden. Viele Switches verwenden eine assoziative Speichertabelle (CAM-Tabelle), um die Quelladresse für jedes Datenpaket zu speichern. Wenn die Tabelle voll ist, schaltet der Switch gegebenenfalls in einen vollständig geöffneten Status um, in dem alle eingehenden Pakete auf allen Ports übertragen werden, so dass der Angreifer den gesamten Datenverkehr des Switch abhören kann. In diesem Fall kann es auch zu Paketlecks in andere VLANs kommen. Zwar speichern die virtuellen Switches von VMware eine MAC-Adressentabelle, aber sie erhalten die MAC-Adressen nicht durch abhörbaren Datenverkehr und sind daher gegen diese Art von Angriffen immun.
- *Angriffe durch 802.1q- und ISL-Kennzeichnung* – Dabei werden die Datenblöcke durch den Switch an ein anderes VLAN weitergeleitet, indem der Switch durch einen Trick dazu gebracht wird, als Trunk zu fungieren und den Datenverkehr an andere VLANs weiterzuleiten. Die virtuellen Switches von VMware führen kein dynamisches Trunking aus, das für diese Art des Angriffs notwendig ist, und sind daher immun.
- *Doppelt eingekapselte Angriffe* – Dabei erstellt der Angreifer ein doppelt eingekapseltes Paket, in dem sich der VLAN-Bezeichner im inneren Tag vom VLAN-Bezeichner im äußeren Tag unterscheidet. Um Rückwärtskompatibilität zu gewährleisten, entfernen native VLANs standardmäßig den äußeren Tag von übertragenen Paketen.

Wenn ein nativer VLAN-Switch den äußeren Tag entfernt, bleibt nur der innere übrig, der das Paket zu einem anderen VLAN weiterleitet, als im jetzt fehlenden äußeren Tag angegeben war. Die virtuellen Switches von VMware werfen alle doppelt eingekapselten Datenblöcke, die eine virtuelle Maschine auf einem für ein bestimmtes VLAN konfigurierten Port senden möchte. Daher sind sie immun gegen diese Art von Angriffen.

- *Multicast-Brute-Force-Angriffe* – Dabei wird eine große Anzahl von Multicast-Datenblöcken fast zeitgleich an ein bekanntes VLAN gesendet, um den Switch zu überfordern, so dass er versehentlich einige Datenblöcke in andere VLANs überträgt. Die virtuellen Switches von VMware erlauben es Datenblöcken nicht, ihren richtigen Übertragungsbereich (VLAN) zu verlassen, und sind daher gegen diese Art von Angriffen immun.
- *Spanning-Tree-Angriffe* – Diese Angriffe zielen auf das *Spanning-Tree-Protokoll* (STP), das zur Steuerung der Überbrückung verschiedener Teile des LAN verwendet wird. Der Angreifer sendet Pakete der *Bridge Protocol Data Unit* (BPDU) in dem Versuch, die Netzwerktopologie zu ändern und sich selbst als Root-Bridge einzusetzen. Als Root-Bridge kann der Angreifer dann die Inhalte übertragener Datenblöcke mit-schneiden. Die virtuellen Switches von VMware unterstützen STP nicht und sind daher gegen diese Art von Angriffen immun.
- *Zufallsdatenblock-Angriffe* – Dabei wird eine große Anzahl von Paketen versendet, bei denen die Quell- und Zieladressen gleich sind, die jedoch Felder unterschiedlicher Länge und Art mit verschiedenem Inhalt enthalten. Ziel des Angriffs ist, zu erzwingen, dass Pakete versehentlich in ein anderes VLAN fehlgeleitet werden. Die virtuellen Switches von VMware sind gegen diese Art von Angriffen immun.

## Portabsicherung virtueller Switches

Wie ein physischer Netzwerkadapter kann ein virtueller Netzwerkadapter Datenblöcke versenden, die von einer anderen virtuellen Maschine zu stammen scheinen oder eine andere virtuelle Maschine imitieren, damit er Datenblöcke aus dem Netzwerk empfangen kann, die für die jeweilige virtuelle Maschine bestimmt sind.

Außerdem kann ein virtueller Netzwerkadapter, genau wie ein physischer Netzwerkadapter, so konfiguriert werden, dass er Datenblöcke empfängt, die für andere virtuelle Maschinen bestimmt sind.

Jedem virtuellen Netzwerkadapter wird bei seiner Erstellung eine eindeutige MAC-Adresse zugewiesen. Diese Adresse wird »ursprünglich zugewiesene MAC-Adresse« genannt. Obwohl die ursprüngliche MAC-Adresse von außerhalb des Gastbetriebssystems neu konfiguriert werden kann, kann sie nicht vom Gastbetriebssystem selbst geändert werden. Außerdem verfügt jeder Adapter über eine geltende MAC-Adresse, die eingehenden Netzwerkverkehr mit MAC-Adressen ausfiltert, die nicht der geltenden MAC-Adresse entsprechen. Das Gastbetriebssystem ist für die Einstellung der geltenden

MAC-Adresse verantwortlich. In der Regel stimmen die geltende MAC-Adresse und die ursprünglich zugewiesene MAC-Adresse überein.

Beim Versand von Datenpaketen schreibt das Betriebssystem die wirksame MAC-Adresse des eigenen Netzwerkadapters in das Feld QUELL-MAC-ADRESSE des Ethernet-Frames. Es schreibt auch die MAC-Adresse des Empfänger-Netzwerkadapters in das Feld ZIEL-MAC-ADRESSE. Der empfangende Adapter akzeptiert Datenpakete nur dann, wenn die Ziel-MAC-Adresse im Paket mit seiner eigenen geltenden MAC-Adresse übereinstimmt.

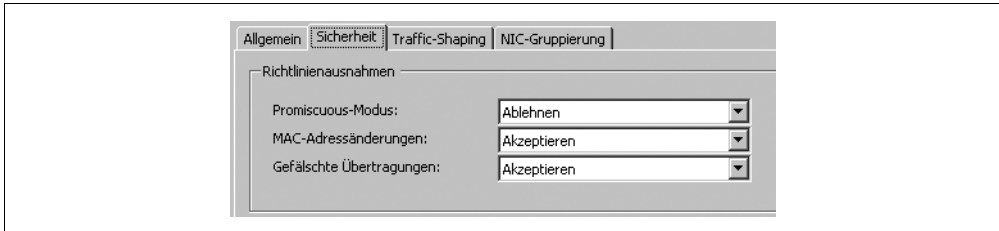


Abbildung 17-2: Sicherheitsrichtlinien des vSwitch

Mit den Sicherheitsprofilen für den virtuellen Switch (siehe Abbildung 17-2) auf den ESXi Hosts können Sie sich gegen diese Art von Angriffen schützen, indem Sie drei Optionen einstellen:

1. **MAC-ADRESSÄNDERUNGEN (MAC ADDRESS CHANGES)** – In der Standardeinstellung ist diese Option auf AKZEPTIEREN (ACCEPT) gesetzt, der ESXi Server akzeptiert also Anfragen, die geltende MAC-Adresse in eine andere als die ursprünglich zugewiesene Adresse zu ändern. Die Einstellungen der Option MAC-ADRESSEN-ÄNDERUNG beeinflussen den Datenverkehr, den eine virtuelle Maschine empfängt.

Zum Schutz gegen MAC-Imitation können Sie die Option auf REJECT (ABLEHNEN) setzen. In diesem Fall lehnt der ESXi Server alle Anfragen ab, die geltende MAC-Adresse in eine andere als die ursprünglich zugewiesene Adresse zu ändern. Stattdessen wird der Port deaktiviert, der von dem virtuellen Adapter zum Senden der Anfrage verwendet wird. Als Folge erhält der virtuelle Adapter keine weiteren Datenpakete mehr, bis er die geltende MAC-Adresse ändert, so dass sie mit der ursprünglichen MAC-Adresse übereinstimmt. Das Gastbetriebssystem erkennt nicht, dass die Änderung der MAC-Adresse nicht angenommen wurde.



In bestimmten Situationen ist es tatsächlich notwendig, dass mehrere Adapter in einem Netzwerk dieselbe MAC-Adresse haben – zum Beispiel wenn Sie Microsoft-Netzwerklastausgleich (NLB) im Unicast-Modus verwenden. Bei der Verwendung von Microsoft-NLB im Standard-Multicast-Modus haben die Adapter nicht dieselbe MAC-Adresse.

2. **GEFÄLSCHTE ÜBERTRAGUNGEN (FORGED TRANSMITS)** – In der Standardeinstellung ist diese Option auf AKZEPTIEREN (ACCEPT) gesetzt, der ESXi Server vergleicht also die Quelladresse nicht mit der geltenden MAC-Adresse. Die Einstellungen der Option

GEFÄLSCHTE ÜBERTRAGUNGEN ändern den Datenverkehr, der von einer virtuellen Maschine versandt wird.

Zum Schutz gegen MAC-Imitation können Sie die Option auf REJECT (ABLEHNEN) setzen. In diesem Fall vergleicht der Host die Quell-MAC-Adresse, die vom Betriebssystem übertragen wird, mit der geltenden MAC-Adresse des Adapters, um festzustellen, ob sie übereinstimmen. Wenn die Adressen nicht passen, verwirft der ESXi Server das Paket.

Das Gastbetriebssystem erkennt nicht, dass der virtuelle Netzwerkadapter die Pakete mit der imitierten MAC-Adresse nicht senden kann. Der Host fängt alle Pakete mit imitierten Adressen vor der Auslieferung ab. Das Gastbetriebssystem geht gegebenenfalls davon aus, dass die Pakete verworfen wurden.

3. BETRIEB IM PROMISCUOUS-MODUS (PROMISCUOUS MODE) – In der Standardeinstellung ist diese Option auf ABLEHNEN (REJECT) gesetzt, der virtuelle Netzwerkadapter kann also nicht im Promiscuous-Modus betrieben werden. Der Promiscuous-Modus deaktiviert jegliche Empfangsfilterung, die der virtuelle Netzwerkadapter normalerweise ausführen würde, so dass das Gastbetriebssystem den gesamten Datenverkehr aus dem Netzwerk empfängt.

Zwar kann der Promiscuous-Modus für die Beobachtung der Netzwerkaktivitäten nützlich sein, aber er ist ein unsicherer Betriebsmodus, da jeder Adapter im Promiscuous-Modus Zugriff auf alle Pakete hat, auch wenn manche davon nur für einen spezifischen Netzwerkadapter bestimmt sind. Das bedeutet, dass ein Administrator oder *root*-Anwender in einer virtuellen Maschine rein theoretisch den Datenverkehr einsehen kann, der für andere Gast- oder Hostbetriebssysteme bestimmt ist.



Unter bestimmten Umständen ist es notwendig, einen virtuellen Switch in den Promiscuous-Modus zu setzen – zum Beispiel wenn Sie eine Software zur Netzwerkeinbruchserkennung oder einen Paketmitschneider (Network-Sniffer, z.B. WireShark) verwenden wollen.

## Benutzerpasswortbeschränkungen

Wie leicht sich ein Angreifer auf einem ESXi Host anmelden kann, hängt davon ab, wie leicht er eine gültige Anwendername/Kennwort-Kombination finden kann. Ein böswilliger Anwender kann ein Kennwort auf verschiedene Arten erlangen. Zum Beispiel kann er unsicheren Netzwerkdatenverkehr wie z.B. Telnet- oder FTP-Übertragungen auf erfolgreiche Anmeldeversuche abhören.



Bedenken Sie immer, dass die meisten Angriffe nicht von außen, sondern von den eigenen Mitarbeitern durchgeführt werden.

Ein anderes, häufig verwendetes Verfahren zum Knacken eines Kennworts ist die Verwendung eines Kennwortgenerators. Kennwortgeneratoren können für verschiedene Kennwort-



angriffe verwendet werden, z.B. für Brute-Force-Angriffe, bei denen der Generator alle möglichen Zeichenkombinationen bis zu einer bestimmten Kennwortlänge ausprobiert, und für Wörterbuchangriffe, bei denen der Generator existierende Wörter und einfache Abwandlungen existierender Wörter ausprobiert.

Der Einsatz von Beschränkungen bezüglich der Länge, der verwendeten Zeichen und der Verwendungsdauer eines Kennworts kann Angriffe durch Kennwortgeneratoren schwieriger gestalten. Je länger und komplexer ein Kennwort ist, desto schwieriger ist es für einen Angreifer, das Kennwort herauszufinden. Je öfter Anwender ihre Kennwörter ändern müssen, desto schwieriger ist es, ein Kennwort zu finden, das mehrmals funktioniert.



Denken Sie immer an mögliche menschliche Fehler, wenn Sie die Kennwortbeschränkungen umsetzen. Wenn Sie Kennwörter setzen, die man sich kaum merken kann, oder häufige Kennwortänderungen vorschreiben, kann es sein, dass die Benutzer ihre Kennwörter aufschreiben müssen und dadurch deren Sinn verwässern.

Zum Schutz der Kennwortdatenbank gegen Missbrauch wurde das Kennwort-Shading für ESXi Server aktiviert, so dass die Kennwort-Hashes zugriffsgeschützt sind. Außerdem verwendet ESXi MD5-Kennwort-Hashes, die eine höhere Kennwortsicherheit bieten und es ermöglichen, Kennwörter mit einer Mindestlänge von mehr als acht Zeichen zu fordern.

Der ESXi Server bietet eine Kennwortkontrolle auf zwei Ebenen, um Kennwort-Policies für Anwender durchzusetzen und das Risiko des Knackens von Kennwörtern zu begrenzen:

Die *Kennwortverwendungsdauer* bestimmt, wie lange ein Anwenderkennwort aktiv sein kann, bevor der Anwender es ändern muss. Dadurch wird sichergestellt, dass das Kennwort oft genug geändert wird, so dass ein Angreifer, der ein Kennwort durch Abhören oder soziale Kontakte erhalten hat, nicht auf ewig auf ESXi Server zugreifen kann.

*Kennwortkomplexität* stellt sicher, dass Anwender Kennwörter auswählen, die für Kennwortgeneratoren schwer zu bestimmen sind.

## Kennwortverwendungsdauer

Die Umsetzung für den ESXi Server sieht folgendermaßen aus:

1. Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.
2. Führen Sie nach Bedarf einen oder mehrere der folgenden Befehle aus:
  - Änderung der Höchstanzahl an Tagen, die ein Anwender sein Kennwort behalten darf:
    - Öffnen Sie mit dem Texteditor vi die Datei *passwd*.
    - Gehen Sie zu der Zeile, die mit folgendem Argument beginnt:  
`password requisite /lib/security/$ISA/pam_passwdqc.so.`

- Fügen Sie am Ende der Zeile folgenden Parameter ein:  
`--passmaxdays=<Anzahl_von_Tagen>`  
wobei <Anzahl\_von\_Tagen> die Höchstanzahl von Tagen bis zum Ablauf des Kennworts ist.
- Änderung der Mindestanzahl von Tagen zwischen zwei Kennwortänderungen:
  - Fügen Sie am Ende der Zeile folgenden Parameter ein:  
`--passmindays=<Anzahl_von_Tagen>`  
wobei <Anzahl\_von\_Tagen> die Mindestanzahl von Tagen zwischen zwei Kennwortänderungen ist.
- Änderung der Hinweiszeit vor einer Kennwortänderung:
  - Fügen Sie am Ende der Zeile folgenden Parameter ein:  
`--passwarnage=<Anzahl_von_Tagen>`  
wobei <Anzahl\_von\_Tagen> die Anzahl der Tage ist, die ein Anwender vor dem Auslaufen eines Kennworts Warnhinweise erhält.

## Kennwortkomplexität

Standardmäßig verwendet ESXi die PAM-Konfiguration (Pluggable Authentication Modules) unter `/etc/pam.d/system-auth-generic` zur Festlegung der Regeln, die Anwender bei der Erstellung von Kennwörtern beachten müssen, und zur Überprüfung der Kennwortqualität im Erstellungsprozess.

Das Plugin *pam\_passwdqc.so* ermöglicht es Ihnen, Standards festzulegen, die alle Kennwörter erfüllen müssen. In der Standardeinstellung wendet der ESXi Server keine Beschränkungen auf das Root-Kennwort an. Wenn jedoch andere Anwender als der *root*-Anwender versuchen, ihr Kennwort zu ändern, müssen die Kennwörter, die sie auswählen, die Standards von *pam\_passwdqc.so* erfüllen. Außerdem können Anwender (*root*-Anwender ausgenommen) nur eine bestimmte Anzahl von Kennwortänderungsversuchen vornehmen, bevor *pam\_passwdqc.so* eine Warnmeldung ausgibt und schließlich das Dialogfeld zur Änderung des Kennworts schließt. Es gibt bei ESXi Server folgende Kennwortstandards und Versuchsbeschränkungen für *pam\_passwdqc.so*:

- *Mindestlänge* – Der Mindestlänge-Parameter von *pam\_passwdqc.so* für ESXi Server-Systeme wurde auf 9 festgelegt. Das bedeutet, dass der Anwender mindestens acht Zeichen eingeben muss, wenn er nur eine Zeichenklasse (Kleinbuchstaben, Großbuchstaben, Zahlen usw.) verwendet.
- *Wiederholungsversuche* – Der Wiederholungsversuchsparameter von *pam\_passwdqc.so* ist für ESXi Server-Systeme auf 3 gesetzt. Das Kennwortänderungsdialogfeld wird also nach drei Versuchen, ein gültiges Kennwort einzugeben, von *pam\_passwdqc.so* geschlossen. Der Anwender muss eine neue Sitzung zur Änderung des Kennworts öffnen, um es wieder zu versuchen.

## Konfiguration einer Regel zur Wiederverwendung von Kennwörtern

1. Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.
2. Wechseln Sie in der Eingabeaufforderung über den Befehl `cd /etc/pam.d/` das Verzeichnis.
3. Öffnen Sie mit dem Texteditor `vi` die Datei `passwd`.
4. Gehen Sie zu der Zeile, die mit folgendem Argument beginnt:  
`password requisite /lib/security/$ISA/pam_passwdqc.so.`
5. Fügen Sie am Ende der Zeile folgenden Parameter ein: `remember=X`.  
Hierbei bedeutet `X` die Anzahl der alten Kennwörter, die ESXi Server für jeden Anwender speichern soll. Trennen Sie den vorangehenden Parameter und `remember=X` durch ein Leerzeichen.
6. Speichern Sie die Änderungen und schließen Sie die Datei.
7. Wechseln Sie in das Verzeichnis `/etc/security/` und geben Sie folgenden Befehl ein, um eine Nulllängendatei mit dem Namen `opasswd` zu erstellen: `touch opasswd`.
8. Geben Sie folgende Befehle ein:

```
chmod 0600 opasswd
chown root:root /etc/security/opasswd
```

## Änderung der Standardkomplexität von Kennwörtern für das Plug-in `pam_passwdqc.so`

Die Standardkomplexität von Kennwörtern auf dem ESXi Server können Sie wie folgt ändern:

1. Melden Sie sich auf der Servicekonsole an und erlangen Sie Root-Privilegien.
2. Geben Sie den folgenden Befehl ein:  
Gehen Sie zu der Zeile, die mit folgendem Argument beginnt:  
`password requisite /lib/security/$ISA/pam_passwdqc.so.`
  - Fügen Sie am Ende der Zeile folgende Parameter ein:  
`--usecrack=<Versuche> <Mindestlänge> <KB_Bonus> <GB_Bonus> <Z_Bonus> <AZ_Bonus>`
  - `Versuche` ist hierbei die Anzahl der Wiederholungsversuche, die der Anwender hat, bis ESXi Server ihn aus dem Kennwortänderungsmodus ausschließt.
  - `Mindestlänge` ist die Mindestanzahl von Zeichen, die ein Anwender eingeben muss, damit das Kennwort angenommen wird. Diese Anzahl ist die Gesamtlänge vor der Anwendung jeglicher Zeichenboni.

Es wird immer mindestens ein Zeichenbonus angewendet, daher ist die Kennwortlänge effektiv ein Zeichen kürzer als im Parameter `Mindestlänge` angegeben. Da `pam_passwdqc.so` nur Kennwörter mit mindestens sechs Zeichen annimmt, muss der `Mindestlänge`-Parameter so berechnet werden, dass die Kennwortlänge nach Abzug der Zeichenboni nicht kleiner als sechs sein kann.

- KB\_Bonus ist die Anzahl von Zeichen, um die der Parameter Mindestlänge verringert wird, wenn im Kennwort mindestens ein Kleinbuchstabe enthalten ist.
- GB\_Bonus ist die Anzahl von Zeichen, um die der Parameter Mindestlänge verringert wird, wenn im Kennwort mindestens ein Großbuchstabe enthalten ist.
- Z\_Bonus ist die Anzahl von Zeichen, um die der Parameter Mindestlänge verringert wird, wenn im Kennwort mindestens eine Ziffer enthalten ist.
- AZ\_Bonus ist die Anzahl der Zeichen, um die der Parameter Mindestlänge verringert wird, wenn der Anwender mindestens ein Sonderzeichen verwendet (z.B. einen Unterstrich oder einen Bindestrich).

Geben Sie die Zeichenbonusparameter als positive Zahl oder – wenn der Anwender keinen Bonus für diese Zeichenklasse erhalten soll – als 0 an. Die Zeichenboni werden addiert. Je mehr verschiedene Zeichenarten der Anwender eingibt, desto weniger Zeichen sind notwendig, um ein gültiges Kennwort zu erstellen.

Mit dieser Einstellung benötigt ein Anwender, der ein Kennwort aus Kleinbuchstaben und einem Unterstrich erstellt, acht Zeichen, um ein gültiges Kennwort zu erstellen. Wenn der Anwender hingegen alle Zeichenarten (Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen) einfügt, benötigt er nur sechs Zeichen.

## Allgemeine Sicherheitsempfehlungen

Sie sollten bei der Überprüfung der Servicekonsolensicherheit und der Verwaltung der Servicekonsole die im Folgenden angeführten Sicherheitsempfehlungen beachten.

### Installation von Antivirensoftware

Auch wenn Sie einen ESXi Server betreiben können, ohne dass das Management Network an ein Netzwerk angeschlossen ist, ermöglichen die meisten Implementierungen des Management Network den Netzwerkzugriff. Da das Management Network aber kein vollständiges Betriebssystem ist, brauchen Sie es – anders als normale Betriebssysteme und virtuelle Maschinen am Standort – nicht vor Viren zu schützen.

### VMsafe

Bei VMsafe handelt es sich um ein neues Sicherheitsfeature von VMware, um die virtuelle Umgebung vor Viren, Trojanern und Ähnlichem zu schützen. VMware stellt dabei eine API (Application Programming Interface) bereit, die von Drittanbietern z.B. in Form von VMs genutzt werden kann. Diese virtuelle Maschine (*Appliance*) kommuniziert mit dem Hypervisor und hat somit Einblick in alle VMs und in das, was diese so tun. Somit können Schadprogramme und Schadcode erkannt und eliminiert werden.

Vorteil dabei ist, dass nicht jede VM ihre eigene Software braucht und so keine Ressourcen durch zusätzlich installierte Programme verschwendet werden und die Schädlinge gar nicht erst in das Betriebssystem der virtuellen Maschine gelangen können.

Insgesamt 29 Firmen haben sich für dieses Projekt als Partner bei VMware eintragen lassen. Die ersten Lösungen von Trend Micro und McAfee gibt es bereits auf dem Markt.

## Beschränkung des Anwenderzugriffs

Beschränken Sie zur Verbesserung der Sicherheit den Anwenderzugriff auf das Management Network und setzen Sie Policies für die Zugriffssicherheit wie Kennwortbeschränkungen um – zum Beispiel durch Vorgabe der Kennwortlänge, Zeitbeschränkungen für Kennwörter und Verwendung eines *grub*-Kennworts beim Hochfahren des Hosts (siehe oben).

Das Management Network hat privilegierten Zugriff auf bestimmte Teile des ESXi Servers. Daher sollten nur vertrauenswürdige Anwender Zugriff darauf erhalten. In der Standardeinstellung ist der Root-Zugriff beschränkt, wodurch eine SSH-Anmeldung als *root* normalerweise nicht möglich ist. Soll ein User Shell-Zugriff bekommen, muss dieser zusätzlich zu dem Häkchen in Abbildung 17-3 eine Rolle als Administrator auf dem Objekt zugewiesen bekommen.

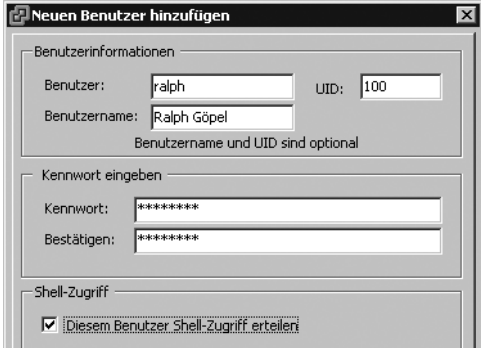


Abbildung 17-3: Shell-Zugriff für die Anmeldung am ESXi Server

Wenn von einem Benutzer auf den ESXi Server zugegriffen wird und Sie ihn löschen, bleibt er weiterhin angemeldet. Setzen Sie die Berechtigung für diesen User allerdings auf »kein Zugriff«, dann wirkt das sofort – er bleibt zwar angemeldet, kann aber nichts mehr sehen, geschweige denn ändern.

Versuchen Sie auch, so wenige Prozesse wie möglich auf dem Management Network auszuführen. Im Idealfall sollten nur die Prozesse, Dienste und Agenten ausgeführt werden, die wirklich notwendig sind, zum Beispiel Antivirenprogramme, Backups für die virtuellen Maschinen usw.

## Verwaltung über den vSphere Client

Verwenden Sie den vSphere Client, WebAccess oder Netzwerkmanagement-Programme von Drittanbietern zur Verwaltung der ESXi Hosts, wenn es möglich ist, statt als *root*

über die Befehlszeilenoberfläche zu agieren. Mit dem vSphere Client können Sie die Anzahl der Konten einschränken, die Zugriff auf das Management Network haben, Verantwortungen sicher weitergeben und Rollen einrichten, damit Administratoren und Anwender keine Funktionen nutzen können, die sie nicht benötigen.

## Sperrmodus für ESXi

Der Sperrmodus für den ESXi Host ist ebenfalls eine Sicherheitsmaßnahme, die aber sehr restriktive Einschränkungen mit sich zieht. Außer dem *vpxuser* kann sich kein anderer Benutzer mehr an dem Host anmelden, Skripten über RCLI können nicht mehr abgesendet werden und einige Programme von Drittanbietern schlagen fehl. Da der vCenter Server über *vpx* auf den ESXi zugreift, können hier aber weiterhin alle Funktionen genutzt werden. Einzig der User *root* hat die Möglichkeit, sich direkt an der Konsole des Rechners anzumelden. Das geht auch über ssh mit autorisierten Schlüsseln und mit dem vSphere Client.

Der Sperrmodus kann erst aktiviert werden, wenn der ESXi Server über den vCenter Server verwaltet wird. Das erreichen Sie dann an der Konsole des ESXi Servers und mit dem vSphere Client über den vCenter Server unter KONFIGURATION → SICHERHEITSPROFIL des ESXi Hosts.



Aktivieren Sie den Sperrmodus über die direkte Konsole, werden alle Berechtigungen von Usern und Gruppen auf dem Host gelöscht – aber nicht, wenn Sie über den vSphere Client gehen.

## Verwendung von Paketen anderer Hersteller

Auf dem Host können zur Unterstützung von notwendigen Managementschnittstellen oder -aufgaben viele Pakete von Drittanbietern installiert und ausgeführt werden. Bei VMware können diese Pakete nur über eine VMware-Quelle aktualisiert werden. Wenn Sie einen Download oder Patch aus einer anderen Quelle nutzen, können die Sicherheit und die Funktionen des Servers gefährdet werden. Überprüfen Sie die Internetseiten von Drittanbietern und die VMware Knowledgebase regelmäßig auf Sicherheitswarnungen. Über die Konfiguration des Hosts erreichen Sie u. a. das Sicherheitsprofil. Dort lässt sich im unteren Teil des Fensters die Akzeptanzebene für Installationsmedien festlegen. Über den Link BEARBEITEN können vier Einstellungsmöglichkeiten gewählt werden (siehe Abbildung 17-4).



Abbildung 17-4: Akzeptanzebene des Host-Image-Profiles

# Firewall-Konfiguration im vCenter Server

Wenn Sie einen vCenter Server verwenden, können Sie Firewalls an allen in Abbildung 17-5 gezeigten Punkten installieren.

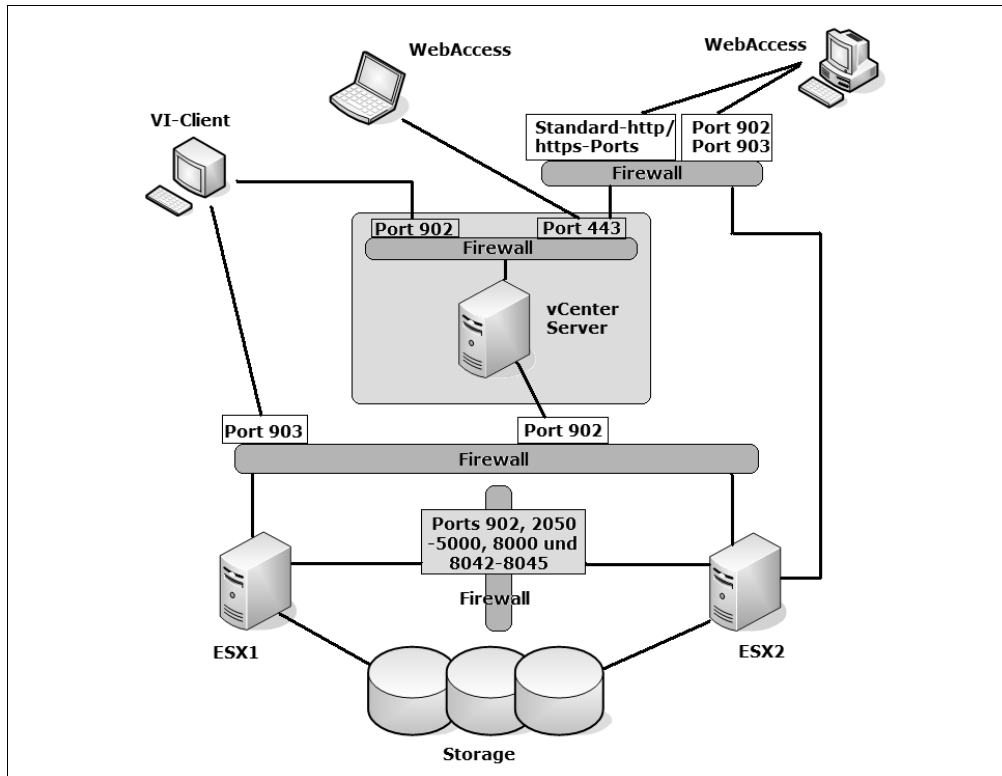


Abbildung 17-5: Übersicht der notwendigen Ports



Abhängig vom konkreten Aufbau sind gegebenenfalls nicht alle in der Abbildung dargestellten Firewalls nötig – es können aber auch weitere, nicht dargestellte Firewalls notwendig sein.

Netzwerke, die über einen vCenter Server konfiguriert werden, können Daten über verschiedene Typen von Clients erhalten: den vSphere Client, WebAccess und die Netzwerkmanagement-Clients von Drittanbietern, die SDK als Schnittstelle mit dem Host verwenden. Während des normalen Betriebs wartet vCenter auf bestimmten Ports auf Daten von verwalteten Hosts und Clients. vCenter geht auch davon aus, dass die verwalteten Hosts auf bestimmten Ports auf Daten von vCenter warten. Wenn sich zwischen diesen Elementen eine Firewall befindet, muss sichergestellt werden, dass in der Firewall Ports für den Datenverkehr freigegeben wurden.

## TCP- und UDP-Ports

In diesem Abschnitt werden voreingestellte TCP- und UDP-Ports aufgeführt, die für den Managementzugriff auf den vCenter Server, die ESXi Server und andere Netzwerkkomponenten verwendet werden. Wenn Netzwerkkomponenten, die außerhalb einer Firewall liegen, verwaltet werden müssen, muss gegebenenfalls die Firewall neu konfiguriert werden, damit auf die entsprechenden Ports zugegriffen werden kann.

| Port       | Zweck                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Art des Datenverkehrs                   |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| 80         | HTTP-Zugriff. Nicht abgesicherter Standard-TCP-Webport, der normalerweise in Verbindung mit Port 443 als Frontend zum Zugriff auf ESXi Server-Netzwerke vom Internet aus verwendet wird. Port 80 leitet Datenverkehr auf eine HTTPS-Startseite (Port 443) um, von der Sie die Konsole der virtuellen Maschine aufrufen. Verwenden Sie Port 80 für Verbindungen zu WebAccess vom Internet.                                                                                          | Eingehendes TCP                         |
| 443        | HTTPS-Zugriff. Standard-SSL-Internetport. Verwenden Sie Port 443 für folgende Aufgaben: <ul style="list-style-type: none"><li>• Verbindung zu WebAccess vom Internet</li><li>• WebAccess und Verbindungen von Netzwerkmanagement-Clients von Drittanbietern an den vCenter Server</li><li>• direkter WebAccess und Zugriff der Netzwerkmanagement-Clients von Drittanbietern auf ESXi Server-Hosts</li></ul>                                                                       | Eingehendes TCP                         |
| 902        | Datenverkehr zur Authentifizierung für die Konfiguration von ESXi Server-Host und virtuellen Maschinen. Verwenden Sie Port 902 für folgende Aufgaben: <ul style="list-style-type: none"><li>• vSphere Client-Zugriff auf den vCenter Server</li><li>• vCenter Server-Zugriff auf die ESXi Server-Hosts</li><li>• direkter vSphere Client-Zugriff auf die ESXi Server-Hosts</li><li>• ESXi Server-Hostzugriff auf andere ESXi Server-Hosts für Migration und Provisioning</li></ul> | Eingehendes TCP, abgehendes UDP         |
| 903        | Datenverkehr der Remote-Steuerung, der durch Zugriffe der Anwender auf virtuelle Maschinen auf einem bestimmten ESXi Server-Host entsteht. Verwenden Sie Port 903 für folgende Aufgaben: <ul style="list-style-type: none"><li>• vSphere Client-Zugriff auf die Konsolen von virtuellen Maschinen</li><li>• WebAccess Client-Zugriff auf die Konsolen von virtuellen Maschinen</li></ul>                                                                                           | Eingehendes TCP                         |
| 2049       | Datenübertragungen von den NFS-Speichergeräten. Dieser Port wird auf der VMkernel-Schnittstelle verwendet, nicht auf der Management Network Schnittstelle.                                                                                                                                                                                                                                                                                                                         | Eingehendes und abgehendes TCP          |
| 2050– 2250 | Datenverkehr zwischen ESXi Server-Hosts für VMware-Hochverfügbarkeit (HA) und den EMC Autostart Manager                                                                                                                                                                                                                                                                                                                                                                            | Abgehendes TCP, ein- und abgehendes UDP |
| 3260       | Datenübertragungen von den iSCSI-Speichergeräten. Dieser Port wird auf der VMkernel-Schnittstelle und auf der Servicekonsolenschnittstelle verwendet.                                                                                                                                                                                                                                                                                                                              | Abgehendes TCP                          |
| 8000       | Eingehende Anfragen von VMotion. Dieser Port wird auf der VMkernel-Schnittstelle verwendet, nicht auf der Servicekonsolenschnittstelle.                                                                                                                                                                                                                                                                                                                                            | Eingehendes und abgehendes TCP          |
| 8042– 8045 | Datenverkehr zwischen ESXi Server-Hosts für VMware-Hochverfügbarkeit (HA) und den EMC Autostart Manager                                                                                                                                                                                                                                                                                                                                                                            | Abgehendes TCP, ein- und abgehendes UDP |





ESXi Server und vCenter verwenden intern die Ports 8085, 8087 und 9080. Für den ESXi Server sind die Ports 8085, 8087 und 9080 geschützt, da sie keine Remote-Verbindungen akzeptieren.

Weitere Ports können für den SSH-Zugang (22), DNS-Client (53), DHCP-Client (68), SNMP-Server (161) usw. bei Bedarf manuell geöffnet werden.

## Firewall-Ports freigeben über die GUI

Das Wichtigste vorweg: Ohne installierten Dienst oder einen Management-Agenten können keine Ports der Firewall über den VSC freigegeben werden, das funktioniert nur über die Kommandozeile!

Bei der Installation des ESXi Servers ist die Firewall so eingestellt, dass nur die notwendigen Dienste unterstützt und nur die unabdingbaren Ports geöffnet sind (siehe Abbildung 17-6).

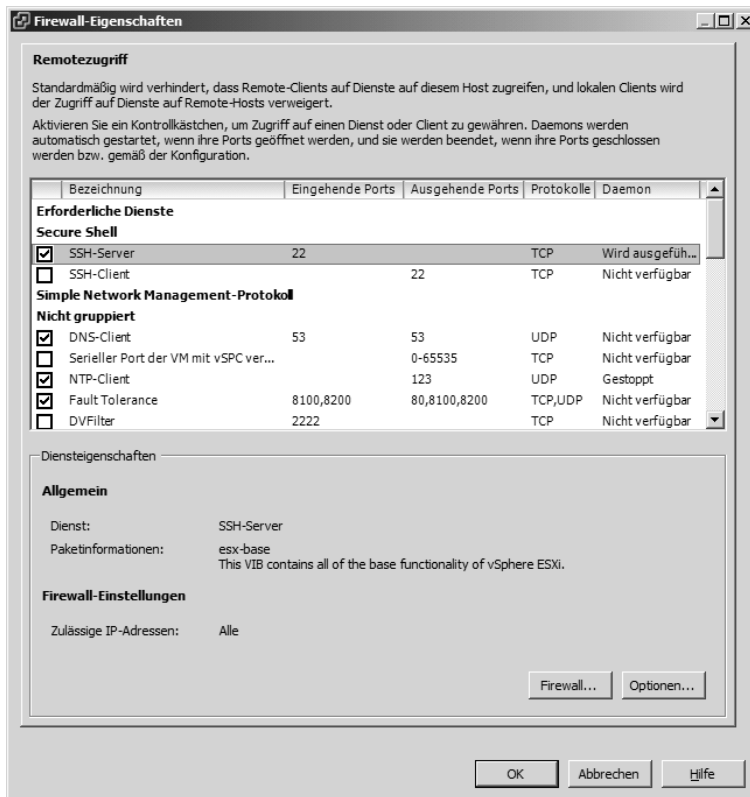


Abbildung 17-6: Firewall-Einstellungen grafisch

Wenn Sie das Sicherheitsprofil des ESXi Hosts im vCenter konfigurieren, werden durch das Hinzufügen oder Entfernen dieser Dienste bzw. Agenten automatisch festgelegte Ports freigegeben oder geschlossen, damit die Kommunikation mit dem Dienst oder dem Agenten möglich ist.

## Firewall-Ports freigeben über die Konsole

Die Änderung der Sicherheitseinstellungen des ESXi Servers über die Kommandozeile sollte nur vorgenommen werden, wenn kein anderer Weg zum Erfolg führen kann. Um überflüssige Schritte zu vermeiden, überprüfen Sie immer erst die Firewall-Einstellungen und Ihre Möglichkeiten in der grafischen Oberfläche, bevor Sie manuelle Änderungen auf der Kommandozeile machen.

Wie bereits in Kapitel 9 »Arbeiten auf der Kommandozeile« erwähnt, sind die Möglichkeiten des ESXi Servers gegenüber der vorherigen ESX-Variante sehr eingeschränkt. Den früheren Befehl `esxcfg-firewall` gibt es nicht mehr, stattdessen werden eingeschränkte Möglichkeiten über den Befehl `esxcli network firewall` geboten.

Um sich die aktuellen Einstellungen der Firewall anzeigen zu lassen, können Sie sich auf der ESXi Shell als *root* anmelden und folgenden Befehl mit Parametern benutzen:

```
esxcli network firewall ruleset list
```

Daraufhin bekommen Sie eine Tabelle mit den Namen der Dienste und der Angabe, ob die zugehörigen Ports geöffnet (*Dienst aktiv*) oder geschlossen (*Dienst deaktiviert*) sind.

Eine ausführliche Anzeige im Listenformat mit den eingehenden und ausgehenden Ports, dem Protokolltyp (TCP oder UDP) sowie dem dazugehörigen Dienst bekommen Sie, wenn Sie folgende Parameter mit angeben:

```
esxcli network firewall ruleset rule list
```

Um eine sortierte Liste zu bekommen (z.B. nach den Einträgen in der fünften Spalte), können Sie den Befehl um die Angabe von »| sort -k 5« erweitern. Der vollständige Aufruf sieht dann folgendermaßen aus:

```
esxcli network firewall ruleset rule list | sort -k 5
```

Folgende weitere Parameter können Sie mit `esxcli network firewall` nutzen, um Informationen zur Firewall zu bekommen oder Änderungen zu machen:

| Parameter | Bemerkung                                                                                                            |
|-----------|----------------------------------------------------------------------------------------------------------------------|
| get       | Standardaktion (Default Action) und Status der Firewall (Enabled und Loaded)                                         |
| load      | Neues Laden der Firewall-Konfigurationsdateien                                                                       |
| refresh   | Aktualisierung der Firewall-Konfiguration durch erneutes Lesen der Firewallkonfigurationsdateien                     |
| unload    | Firewall deaktivieren und Filter löschen                                                                             |
| set       | Aktivierung oder Deaktivierung (--enabled / --disabled) der Firewall und Setzen der Standardaktion (--defaultaction) |

| Parameter                | Bemerkung                                          |
|--------------------------|----------------------------------------------------|
| ruleset allowedall       | Setzt die Firewall außer Kraft                     |
| ruleset allowedip list   | Listet IP-Adressen auf, denen Zugriff gewährt wird |
| ruleset allowedip add    | Ermöglicht IP-Adressen den Zugriff auf Dienste     |
| ruleset allowedip remove | Verbietet IP-Adressen den Zugriff auf Dienste      |

Die eigentliche Konfigurationsdatei für die Firewall befindet sich auf dem ESXi Server unter `/etc/vmware/firewall/` und heißt `service.xml`.

Diese XML-Datei ist nach einem bestimmten Schema aufgebaut, das nach kurzer Betrachtung auch ohne Probleme erweiterbar ist. Das sollte allerdings vermieden werden, denn nach einem Update sind die Änderungen oder Erweiterungen ggf. weg. Besser ist es, eine neue XML-Datei in das Verzeichnis zu legen und nach dem Muster von `service.xml` zu erstellen. Wird der Firewall-Dienst neu gestartet (siehe Tabelle oben), wird auch eine neue Datei eingelesen und verarbeitet.

Haben Sie eine eigene Datei erstellt und den Befehl `esxcli network firewall refresh` eingegeben, erscheint auf der grafischen Oberfläche ebenfalls die Einstellung.

Dazu ein Beispiel: Die Datei `goepel.xml` kann auf der Kommandozeile mit dem `vi` erstellt werden oder auch über ein Tool wie WinSCP. Der Inhalt könnte so aussehen:

```
<!-- Firewall configuration for service goepel -->
<ConfigRoot>
 <service id='0000'>
 <id>goepel</id>
 <rule id='0000'>
 <direction>inbound</direction>
 <protocol>tcp</protocol>
 <porttype>dst</porttype>
 <port>4711</port>
 </rule>
 <enabled>false</enabled>
 <required>false</required>
 </service>
</ConfigRoot>
```

Anschließend bewegen Sie die Firewall zum Einlesen der Datei:

```
esxcli network firewall refresh
```

Über den VSC gehen Sie auf das Sicherheitsprofil des ESXi Hosts und klicken bei der FIREWALL auf EIGENSCHAFTEN. Rollen Sie in dem Fenster nach unten, bis Sie Ihren Dienst sehen. Dort kann dann das Häkchen bei *Aktiviert* gesetzt werden, und fertig.

Damit wird nur der eingehende Datenverkehr erlaubt (inbound). Möchten Sie eingehenden und ausgehenden Datenverkehr zulassen, finden Sie in der Datei `service.xml` hinreichend Beispiele dazu.



Die Änderung der Sicherheitsstufe der Verwaltungsschnittstelle beeinflusst bestehende Verbindungen nicht. Wenn die Firewall zum Beispiel auf niedriger Sicherheitsstufe läuft und ein Backup auf einem Port ausgeführt wird, den Sie nicht ausdrücklich freigegeben haben, beendet eine Erhöhung der Sicherheitsstufe auf »Hoch« das Backup nicht. Weil die Firewall so konfiguriert ist, dass die Pakete für zuvor hergestellte Verbindungen durchgelassen werden, werden das Backup abgeschlossen und die neue Verbindung freigegeben. Anschließend werden für diesen Port keine weiteren Verbindungen mehr akzeptiert.



VMware unterstützt das Öffnen und Blockieren der Firewall-Ports nur durch den vSphere Client oder den Befehl `esxcli` (siehe oben). Eine Verwendung anderer Methoden oder Skripten zum Öffnen oder Blockieren der Firewall-Ports kann zu einem unerwarteten Verhalten führen.

Weitere Informationen zur Sicherheit finden Sie online bei VMware auf mehreren verschiedenen Seiten, die nach Gebieten unterteilt sind. Allgemeine Informationen über Sicherheit mit Warnungen und Downloads befinden sich auf <http://www.vmware.com/security> und im Technical Resource Center unter <http://www.vmware.com/go/security>. Interessant ist auch die Seite <http://www.vmware.com/go/vmsafe>, die Infos zur oben genannten VMsafe-Technologie bietet.

# Ressourcen, Optimierung und Troubleshooting

In diesem Kapitel geht es in erster Linie um die bestmöglichen Einstellungen zu den Ressourcen der virtuellen Maschinen, die Optimierung der vSphere5-Umgebung und die Fehlerbehebung in unserem Datacenter. Im Anschluss stelle ich noch ein paar nützliche Tools vor, die ich regelmäßig bei meinen Kunden einsetze.

## Ressourcenverwaltung

Jede virtuelle Maschine verbraucht einen Teil der CPU-, Speicher- und Netzwerkbandbreitenressourcen des ESXi Servers. Basierend auf einer Reihe von Faktoren garantiert der Host jeder virtuellen Maschine ihren Anteil an den darunter liegenden Hardwareressourcen:

- Verfügbare Ressourcen für den Host (oder den Cluster)
- Werte für Reservierung, Grenzen und Shares der virtuellen Maschine. Diese Attribute der virtuellen Maschine verfügen über Standardwerte, die allerdings für die Anpassung der Ressourcenzuweisung geändert werden können.
- Anzahl der eingeschalteten virtuellen Maschinen und ihre Ressourcennutzung
- Werte für Reservierung, Grenzen und Shares, die der Administrator den Ressourcenpools innerhalb der Ressourcenpool-Hierarchie zugewiesen hat
- Erforderlicher Overhead zum Verwalten der Virtualisierung

Der Server verwaltet unterschiedliche Ressourcen auf verschiedene Weise: Er verwaltet CPU- und Speicherressourcen auf Basis der insgesamt verfügbaren Ressourcen und der oben aufgeführten Faktoren, Netzwerk- und Festplattenressourcen dagegen Host-bezogen.

Der VMware ESXi Server übernimmt Folgendes:

- Verwaltung von Festplattenressourcen über einen anteilsproportionalen Mechanismus
- Steuerung der Netzwerkbandbreite durch Netzwerktraffic-Shaping

Für jede virtuelle Maschine kann der Benutzer Werte für Shares (Anteile), Reservierungen und Grenzen (Limits) festlegen. Der Ressourcenmanager berücksichtigt diese Infor-

mationen anschließend, wenn er den einzelnen virtuellen Maschinen CPU und Speicher zuweist.

## CPU und Arbeitsspeicher bestmöglich zuweisen

Die virtuelle Maschine kann in zwei verschiedenen Modi ausgeführt werden:

- *Direktausführung*: Unter bestimmten Umständen kann der ESXi Server Virtual Machine Monitor (VMM) die virtuelle Maschine direkt auf dem zugrunde liegenden Prozessor ausführen. Dieser Modus wird als *Direktausführung* bezeichnet und bietet eine beinahe originalgetreue Performance bei der Ausführung der CPU-Anweisungen der virtuellen Maschine.
- *Virtualisierungsmodus*: Wenn Direktausführung nicht möglich ist, müssen die Befehle der virtuellen Maschine der CPU virtualisiert werden. Je nach auszuführendem Vorgang wird durch diesen Prozess ein variabler Anteil an Virtualisierungs-Overhead hinzugefügt.

In den meisten Fällen gilt Folgendes:

- Nicht privilegierter Code für Anwendungen auf Benutzerebene wird im Direktausführungsmodus ausgeführt, da in den meisten Betriebssystemen der Code auf Benutzerebene nicht auf privilegierte Statusdaten zugreift.
- Der Betriebssystemcode ändert hingegen privilegierte Statusdaten und macht deshalb den Virtualisierungsmodus erforderlich.

Folglich wird ein Mikro-Benchmark, der nur Systemaufrufe durchführt, in einer virtuellen Maschine erheblich langsamer ausgeführt als auf einem ursprünglichen System. Im Direktausführungsmodus ausgeführter Code führt jedoch nur zu geringen Zusatzkosten für die Performance und profitiert von einer ursprungsnahen Geschwindigkeit der CPU-Anweisungen.



Stellen Sie Einzelthread-Anwendungen auf virtuellen Einzelprozessormaschinen bereit (statt auf virtuellen SMP-Maschinen), um eine optimale Performance und Ressourcennutzung zu erzielen.

Einzelthread-Anweisungen können nur eine einzelne CPU nutzen. Durch das Bereitstellen solcher Anwendungen in virtuellen Maschinen mit zwei Prozessoren kann die Anwendung nicht beschleunigt werden. Das führt dazu, dass die zweite virtuelle CPU physische Ressourcen nutzt, die sonst von anderen virtuellen Maschinen genutzt werden könnten.

## CPU-Affinität

CPU-Affinität bedeutet, dass in Systemen mit mehreren Prozessoren die Zuweisung virtueller Maschinen auf eine Untermenge der verfügbaren Prozessoren eingeschränkt werden kann (siehe Abbildung 18-1). Das geschieht durch Festlegen einer Affinitätseinstellung für jede virtuelle Maschine.



Abbildung 18-1: CPU-Affinität bei der virtuellen Maschine

### Probleme mit der Affinität

Im Rahmen der Affinität virtueller Maschinen wird jede virtuelle Maschine den Prozessoren gemäß der festgelegten Affinitätseinstellung zugewiesen. Bedenken Sie vor der Verwendung der Affinität folgende mögliche Probleme:

- Bei Systemen mit mehreren Prozessoren führen die ESXi Server-Systeme einen automatischen Lastausgleich durch. Durch das Vermeiden der manuellen Spezifikation bei der Affinität der virtuellen Maschinen kann das Steuerprogramm die Last besser prozessorübergreifend ausgleichen.
- Affinität kann die Fähigkeit des ESXi Hosts beeinträchtigen, der für eine virtuelle Maschine festgelegten Reservierung und den Anteilen gerecht zu werden.
- Da die CPU-Zugangskontrolle die Affinität nicht berücksichtigt, erhält eine virtuelle Maschine mit manuellen Affinitätseinstellungen möglicherweise nicht immer die für sie vorgesehene volle Reservierung.
- Umgekehrt werden virtuelle Maschinen ohne manuelle Affinitätseinstellungen nicht durch virtuelle Maschinen mit manuellen Affinitätseinstellungen beeinträchtigt.
- Bei der Verschiebung einer virtuellen Maschine zwischen zwei Hosts wird die Affinität möglicherweise aufgehoben, wenn der neue Host beispielsweise über eine andere Prozessorzahl verfügt.
- Das NUMA-Planungsprogramm ist möglicherweise nicht in der Lage, eine virtuelle Maschine zu verwalten, die bereits unter Verwendung von Affinität bestimmten Prozessoren zugewiesen wurde.

## Hyperthreading und Affinität

Überdenken Sie Ihre Situation sorgfältig, bevor Sie die CPU-Affinität auf Systemen mit aktivierter Hyperthreading-Funktion einstellen. Wenn beispielsweise eine virtuelle Maschine mit hoher Priorität an CPU 0 und eine andere virtuelle Maschine mit hoher Priorität an CPU 1 gebunden ist, müssen beide virtuellen Maschinen denselben physischen Core verwenden. In diesem Fall ist es eventuell nicht möglich, den Ressourcenanforderungen der beiden Maschinen gerecht zu werden. Sie müssen sicherstellen, dass die benutzerdefinierten Affinitätseinstellungen auf einem System mit Hyperthreading Sinn ergeben. In einem Beispiel könnten Sie das sicherstellen, indem Sie die virtuellen Maschinen an CPU 0 und CPU 2 binden. Idealerweise sollten Sie gar keine Affinitätseinstellung verwenden.



In einem DRS-Cluster ist die Option *CPU-Affinität* nicht zulässig, und ihre Einstellungen werden ggf. gelöscht, wenn die VM auf einen anderen Server migriert wird. Falls die VM nicht verschoben werden kann, müssen Sie sich direkt am ESXi Server anmelden und die Affinität löschen. Der Sinn dieser Option liegt allein in der Optimierung der Performance einer bestimmten Gruppe virtueller Maschinen auf demselben Server.

Wird die Affinität im DRS-Cluster nicht automatisch gelöscht, müssen Sie sich direkt mit dem ESXi Host verbinden, um die Einstellungen ändern zu können.

## Virtueller Speicher der VMs

Auf physischen Maschinen werden virtuelle Speicheradressen durch Seitentabellen in physische Speicheradressen übertragen. Bei virtuellen Maschinen pflegen die Seitentabellen des Gastbetriebssystems die Zuordnung von virtuellen Seiten des Gasts zu physischen Seiten des Gasts. Der ESXi Server virtualisiert den physischen Speicher des Gasts, indem eine zusätzliche Ebene der Adressübertragung hinzugefügt wird.

- Der Virtual Machine Monitor (VMM) der einzelnen virtuellen Maschinen übernimmt die Zuordnung der physischen Speicherseiten des Gastbetriebssystems zu den physischen Speicherseiten der darunterliegenden Maschine. (VMware bezeichnet die darunterliegenden physischen Seiten als »Maschinenseiten« und die physischen Seiten des Gastbetriebssystems als »physische Seiten«.)
- Jede VM verfügt über einen angrenzenden nullbasierten, adressierbaren physischen Speicherplatz. Der darunterliegende Maschinenspeicher des von den virtuellen Maschinen verwendeten Servers ist nicht unbedingt angrenzend.
- Der VMM fängt Anweisungen virtueller Maschinen auf, die die Speicherverwaltungsstrukturen des Gastbetriebssystems manipulieren, so dass die eigentliche Speicherverwaltungseinheit (MMU) des Prozessors nicht direkt durch die virtuelle Maschine aktualisiert wird.



- Der Host pflegt die Zuordnungen von virtuellen Seiten zu Maschinenseiten in einer Schattenseitentabelle, die entsprechend den Zuordnungen von physischen Seiten zu Maschinenseiten (wird durch den VMM gepflegt, siehe oben) auf dem aktuellen Stand gehalten wird.
- Die Schattenseitentabellen werden anschließend direkt durch die Paging-Hardware des Prozessors verwendet.

Sobald die Schattenseitentabellen eingerichtet sind, ermöglicht dieser Ansatz der Adressübertragung, dass normale Speicherzugriffe innerhalb der virtuellen Maschine ohne zusätzlichen Adressübertragungs-Overhead erfolgen können. Da der TLB (*Translation Look-aside Buffer*) auf dem Prozessor direkte Caches der virtuell-maschinellen Zuordnungen erstellt, die er aus den Schattenseitentabellen abliest, wird durch den VMM beim Zugriff auf den Speicher kein zusätzlicher Overhead hinzugefügt.

Das Diagramm in Abbildung 18-2 veranschaulicht die Implementierung der Speichervirtualisierung beim ESXi Server.

- Durch die Kästchen in der Abbildung werden Seiten dargestellt (*4k-paging*); die Pfeile veranschaulichen die verschiedenen Speicherzuordnungen.
- Die Pfeile vom virtuellen Speicher des Gasts zum physischen Speicher des Gasts zeigen die durch die Seitentabellen des Gastbetriebssystems gepflegte Zuordnung. (Die Zuordnung vom virtuellen Speicher zum linearen Speicher für Prozessoren mit x86-Architektur ist in der Abbildung nicht dargestellt.)
- Die Pfeile vom physischen Speicher des Gasts zum Maschinenspeicher stellen die durch den VMM gepflegte Zuordnung dar.
- Die gestrichelten Pfeile in der Abbildung zeigen die Zuordnung vom virtuellen Speicher des Gasts zum Maschinenspeicher in den Schattenseitentabellen, die ebenfalls durch den VMM gepflegt werden. Der darunterliegende Prozessor, der die VM ausführt, verwendet die Zuordnungen in der Schattenseitentabelle.

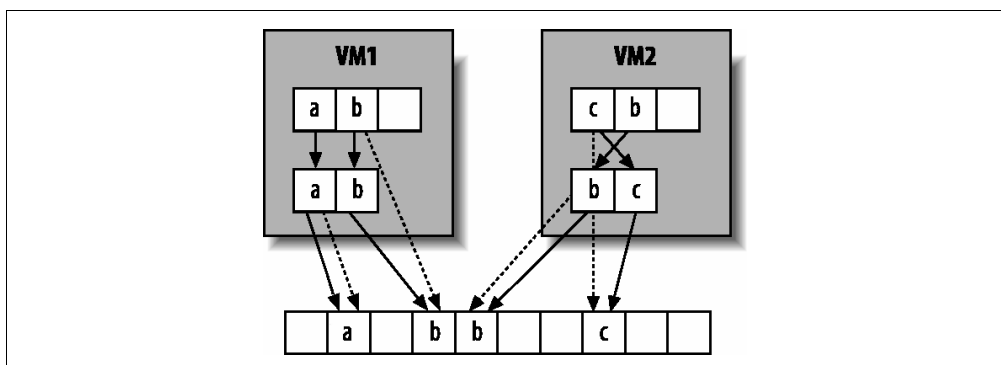


Abbildung 18-2: Speichervirtualisierung beim ESXi Server

Der Host führt die virtuelle Speicherverwaltung ohne Wissen des Gastbetriebssystems aus, und ohne das eigene Speicherverwaltungssubsystem des Gastbetriebssystems zu stören.

Die Parameter `Mem.IdleTax` und `Mem.SamplePeriod` steuern diesen Zugriff. Mithilfe der erweiterten Einstellung, die in Abbildung 18-3 dargestellt ist, können diese Parameter verändert werden. Zu `Mem.IdleTax` (Standard: 75 %) können Sie die Policy für das Abrufen von Leerlaufspeicher explizit steuern. Diese Option kann zusammen mit dem erweiterten Attribut `Mem.SamplePeriod` (Standard: 60 Sekunden) verwendet werden, um zu steuern, wie das System Speicher abruft.

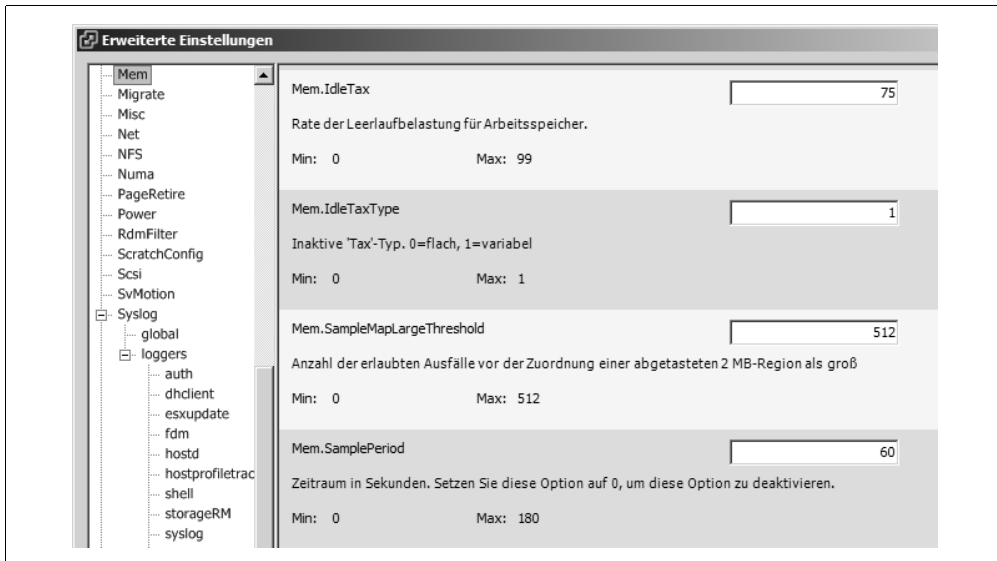


Abbildung 18-3: Einstellungen zum Speicherverhalten der VMs



In den meisten Fällen ist eine Änderung von `Mem.IdleTax` und `Mem.SamplePeriod` weder notwendig noch angebracht.

## Speicherballontreiber

Im Gastbetriebssystem ist durch die Installation der VMware Tools üblicherweise der Speicherballontreiber `vmemctl.exe` geladen. ESXi Server verwenden Swapping, um Speicher von einer virtuellen Maschine zu erzwingen, wenn aus folgenden Gründen kein `vmemctl`-Treiber verfügbar ist:

- Er wurde nie installiert.
- Er wurde explizit deaktiviert.
- Er wird nicht ausgeführt (beispielsweise während des Startvorgangs des Gastbetriebssystems).

- Er ist vorübergehend nicht in der Lage, erforderlichen Speicher schnell genug abzurufen, um die aktuellen Systemanforderungen zu erfüllen.

Standardabruf-Paging-Verfahren lagern die Seiten wieder ein, sobald die virtuelle Maschine sie benötigt.



Bei einem Ausfall eines ESXi Servers, auf dem virtuelle Maschinen ausgeführt wurden, die Swap-Dateien verwendet haben, bestehen diese Swap-Dateien weiterhin und belegen auch nach einem Neustart des ESXi Servers Speicherplatz. Starten Sie die virtuelle Maschine neu und halten Sie sie anschließend explizit an. Dann können Sie die Dateien löschen.

## Ressourcenpools für VM-Gruppen

Jede virtuelle Maschine verbraucht einen Teil der CPU-, Speicher- und Netzwerkbandbreitenressourcen des ESXi Servers. Basierend auf einer Reihe von Faktoren garantiert der Host jeder virtuellen Maschine ihren Anteil an den darunterliegenden Hardwareressourcen, wie bereits eingangs erwähnt.

Der Host oder der Cluster verwalten CPU- und Speicherressourcen auf Basis der insgesamt verfügbaren Ressourcen und der oben aufgeführten Faktoren. Diese Faktoren gelten gleichermaßen für einen Host wie für einen Cluster oder Ressourcenpool.

## Sinn und Unsinn eines Ressourcenpools

Bei einem Ressourcenpool können CPU und RAM fest und dynamisch vergeben und in ihnen mehrer VMs gruppiert werden. Sie können bis zu 1.600 Pools pro Host anlegen, diese auch bis zu einer Tiefe von 8 (bei DRS nur 6) verschachteln und in einem Cluster bis zu 512 davon nutzen.

Für die CPU- und Arbeitsspeicherressourcen können auch Anteile vergeben werden (wurde bereits in Kapitel 4 beschrieben).



Haben Sie einen reinen HA-Cluster erstellt, also ohne DRS, ist es nicht möglich, einen Ressourcenpool hinzuzufügen. Aktivieren Sie DRS, fügen einen Pool hinzu und wählen DRS wieder ab, kommt die in Abbildung 18-4 gezeigte Meldung.

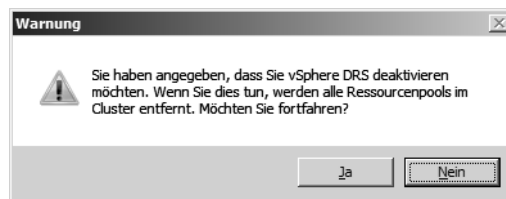


Abbildung 18-4: DRS deaktivieren

Die im Pool enthaltenen VMs landen, wenn Sie auf JA klicken, wieder im HA-Cluster, und der Ressourcenpool wird gelöscht.

Bei den meisten meiner Kunden wurden schon erstellte Ressourcenpools wieder aufgelöst, nachdem ich Ihnen die Bedeutung von Anteilen (Prioritäten) erklärt hatte. Mit Anteilen können einer VM viel präziser CPU, RAM und Festplattenzugriffe zugeordnet werden. Jede Maschine bekommt so lange alle Ressourcen, bis keine mehr frei sind. Erst dann wird nach den Prioritäten der VM geschaut, um niedrigeren etwas wegzunehmen und höheren etwas dazugeben. Für die meisten produktiven Einsatzgebiete ist das die bessere Wahl und deutlich flexibler. Das Schaubild in Abbildung 18-5 verdeutlicht das nochmals.

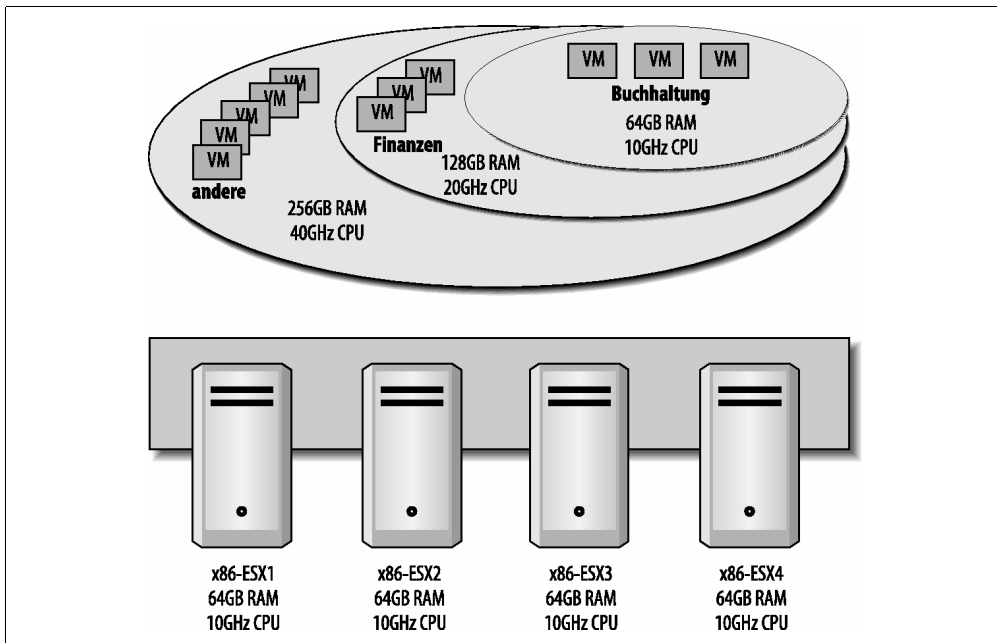


Abbildung 18-5: Ressourcenpool-Beispiel

Alle vier ESXi Server bringen eine CPU-Leistung von 10 GHz, also zusammengefasst 40 GHz. Wenn die Buchhaltung alle Ressourcen verbraucht, bleiben der Finanzabteilung nur noch 10 GHz übrig. Braucht diese ebenfalls alles, bleiben dem Rest auch nur 10 GHz. Arbeitet die Buchhaltung nicht, kann die Finanzabteilung auf 20 GHz zugreifen. Arbeiten beide Abteilungen nicht, haben die anderen 40 GHz zur Verfügung. Gesetzt den Fall, die Buchhaltung muss einen Monatsabschluss machen und die anderen sowie die Finanzabteilung haben Dienstschluss, bekommt sie trotzdem nur 10 GHz CPU-Leistung. Hätte man Anteile eingesetzt, wäre es egal, wie hoch oder niedrig diese sind, und die Buchhaltung könnte mit bis zu 40 GHz Leistung arbeiten.

Einer meiner Kunden hat einen Teil seiner Ressourcen an eine benachbarte Firma vermietet. Hier ist ein Ressourcenpool sinnvoll. Arbeitet der Mieter, kann er auf seine bezahlten und garantierten Ressourcen zugreifen. Ist er zu Hause, kann mein Kunde diese mitnutzen.

## Ressourcenpool-Richtlinien

Die folgenden Richtlinien helfen Ihnen dabei, eine optimale Performance Ihrer virtuellen Maschinen zu erreichen:

- Wenn Sie eher häufige Änderungen der insgesamt verfügbaren Ressourcen erwarten, verwenden Sie besser den Parameter Shares (Anteile) statt der Reservierung, um die Ressourcen den virtuellen Maschinen gleichmäßig zuzuweisen. Wenn Sie nämlich Shares verwenden und beispielsweise ein Host-Upgrade durchführen, verfügt jede virtuelle Maschine weiterhin über dieselbe Priorität (dieselbe Anzahl von Shares), obwohl jeder einzelne Anteil einen größeren Speicher- oder CPU-Wert darstellt.
- Verwenden Sie den Parameter Reservierung, um eine annehmbare Mindestgröße festzulegen. Der Host weist bei entsprechender Verfügbarkeit zusätzliche Ressourcen zu und richtet sich dabei nach der Anzahl der Shares und der für die virtuelle Maschine festgelegten Grenze (Limit).
- Verwenden Sie den Parameter Reservierung, um die Mindestreservierung für jede einzelne virtuelle Maschine festzulegen. Der Umfang der tatsächlichen durch die Reservierung dargestellten Ressourcen ändert sich bei einer Änderung der Umgebung nicht, z. B. wenn virtuelle Maschinen hinzugefügt oder entfernt werden.
- Stellen Sie Reservierung nicht zu hoch ein. Eine zu hohe Reservierung kann zu einer Begrenzung der Anzahl virtueller Maschinen in einem Ressourcenpool führen.
- Lassen Sie beim Festlegen der Reservierungswerte für virtuelle Maschinen etwas Spielraum und vergeben Sie nicht alle Ressourcen. Je dichter Sie sich an einer vollständigen Reservierung aller Kapazitäten des Systems bewegen, desto schwieriger wird es, Änderungen an der Reservierung und der Ressourcenpool-Hierarchie vorzunehmen, ohne dabei die Zugangskontrolle zu verletzen. In einem Cluster mit aktivierter DRS-Funktion kann eine Reservierung, die eine vollständige Vergabe der Kapazität eines Clusters oder einzelner Hosts des Clusters vorsieht, dazu führen, dass VMs nicht über DRS zwischen zwei Hosts migriert werden.
- Verwenden Sie für ein delegiertes Ressourcenmanagement Ressourcenpools. Um einen Ressourcenpool vollständig zu isolieren, setzen Sie den Ressourcenpool auf den Typ fest und verwenden Reservierung und Grenzwert.
- Gruppieren Sie VMs für einen Multi-Tier-Dienst in einem Ressourcenpool. Mithilfe von Ressourcenpools kann der ESXi Server Ressourcen für den Dienst insgesamt zuweisen.

- Aktivieren Sie *PortFast* an PortFast-fähigen physischen Switches, um die Kommunikation zwischen HA-Clustern und anderen Cluster-Nodes sicherzustellen.

## VM-Speicherprofil und Storage DRS

Eine weitere neue Funktion, die mit vSphere5 eingeführt wurde, sind *Datenspeicher-Cluster*. Damit ist es möglich, VMs per Storage vMotion automatisch auf die Volumes zu verteilen, ähnlich wie es bei DRS in Kapitel 10 erwähnt wurde. Das nennt sich dann »Storage DRS« (Speicher-DRS). Damit kann man Schwellenwerte für I/O und Platz definieren, die beim Erreichen dazu führen, dass VMs verschoben werden oder zumindest eine Empfehlung für den Fall generiert wird, dass der Speicher auf einem Volume zu knapp wird oder überlastet ist.

Weiterhin können Affinitätsregeln für bestimmte VMDKs erstellt werden, damit bestimmte Maschinen immer auf dem Storage verbleiben oder Festplatten einiger VMs auf verschiedene Storages aufgeteilt werden.

Die Vorgehensweise beim Speicher-DRS ist also vom Sinn her mit der beim herkömmlichen DRS vergleichbar. Nach dem Einrichten bekommen Sie die neue Registerkarte SPEICHER-DRS-EMPFEHLUNGEN, auf der Migrationsempfehlungen mit Begründungen aufgelistet werden, wenn Sie nicht den Automatikmodus verwenden.

Über den vCenter Server können Sie solche Cluster erstellen, indem Sie unter HOME auf DATENSPEICHER UND DATENSPEICHER-CLUSTER klicken. Dort wählen Sie dann NEUER DATENSPEICHER-CLUSTER und beantworten die Fragen des Assistenten. Anschließend wählen Sie in den DATENSPEICHER-CLUSTEREINSTELLUNGEN das Häkchen zum Aktivieren aus. Dann können Sie ggf. noch die SDRS-LAUFZEITREGELN und die SDRS-AUTOMATISIERUNG einstellen.

Beachten Sie dabei, dass

- NFS- und VMFS-Datenspeicher nicht in einem Storage-Cluster vereint werden können,
- replizierte und nicht replizierte Speicher nicht in einem Storage-Cluster vereint werden dürfen,
- nur ESXi 5.0 Hosts auf so einen Cluster zugreifen können,
- der Speicher nur für ein Datacenter zugänglich sein darf und
- die Hardwarebeschleunigung bei allen Storages nicht aktiv oder bei allen aktiv sein muss, also kein Mischbetrieb möglich ist.

## VM-Speicherprofil

Was in der englischen Literatur von VMware als »Profile-Driven Storage« bezeichnet wird, heißt in der deutschen Einstellung VM-SPEICHERPROFIL. Dabei wird für eine virtu-

elle Maschine zwischen den Konfigurations- und Logdateien (VM-Home-Dateien) sowie der bzw. den Festplatte/n unterschieden, die über unterschiedliche Profile verfügen können. Beim Erstellen, Klonen und Verschieben einer VM können die jeweiligen Volumes nach dem Bedarf (Profil) ausgesucht werden, falls Sie über die Version Enterprise Plus verfügen.

So ein Profil kann nach Kapazität, Leistung, Verfügbarkeit, Redundanz usw. ausgesucht und erstellt werden, nicht aber für RDM (Raw Device Mapping). Über die VMware vStorage-APIs, die von einigen Storage-Herstellern angeboten werden, bekommt man viele Details zum angeschlossenen Speicher mitgeteilt und kann diese für eine Einstufung benutzen. Werden über die APIs bestimmte Funktionen automatisch erkannt und eingetragen, nennt man diese *systemdefinierte Funktionen* im Gegensatz zu *benutzerdefinierten Funktionen*. Jeder Datenspeicher kann maximal eine *systemdefinierte* und eine *benutzerdefinierte Funktion* haben.

Die VM-Speicherprofile finden Sie über HOME → MANAGEMENT → VM-SPEICHERPROFIL. Wenn Sie dort in der Menüzeile auf SPEICHERFUNKTIONEN VERWALTEN klicken, erhalten Sie ein Fenster, in dem die systemdefinierten und ggf. die benutzerdefinierten Profile aufgelistet sind. Über die Schaltfläche HINZUFÜGEN können benutzerdefinierte Funktionen hinzugefügt werden. Die vom System selbstständig entdeckten Funktionen können nicht geändert werden.

Haben Sie ein benutzerdefiniertes Profil erstellt, können Sie anschließend ein VM-SPEICHERPROFIL anlegen und es mit dem STORAGE-PROFIL verknüpfen. Über HOME → DATENSPEICHER UND DATENSPEICHERCLUSTER wählen Sie nun einen Storage aus. Anschließend können Sie dem erstellten Profil diesen Speicherplatz zuweisen, indem Sie die Schaltfläche BENUTZERDEFINIERT SPEICHERFUNKTION ZUWEISEN anklicken und anschließend aus dem Drop-down-Feld eines auswählen. Im rechten Teil des Fensters sollte dann unter SPEICHERFUNKTIONEN Ihre Auswahl erscheinen.

Haben Sie eine Liste der Storages aufgerufen, können Sie auch mehrere auswählen, indem Sie die Strg-Taste gedrückt halten und dann über das Kontextmenü die Funktion zuweisen.

Haben Sie alles so weit eingerichtet, können Sie die Speicherprofile aktivieren, um sie anschließend beim Migrieren oder Erstellen einer VM auch auswählen zu können. Gehen Sie dafür wieder zu den VM-Speicherprofilen und klicken Sie oben rechts auf den Link VM-SPEICHERPROFILE AKTIVIEREN. Wählen Sie dort den Cluster oder die ESXi Server aus, die über die Enterprise Plus-Version verfügen, und klicken Sie anschließend auf AKTIVIEREN. Selbstverständlich können Sie auch nachträglich ausgeschaltete oder laufende VMs mit einem Speicherprofil verknüpfen, indem Sie es in den Einstellungen der VM über die Registerkarte PROFILE oder im Kontextmenü der VM über VM-SPEICHERPROFIL → PROFIL VERWALTEN auswählen.

Bei beiden Vorgehensweisen erhalten Sie das gleiche Fenster, in dem Sie den Home-Dateien (den Konfigurations- und Logdateien) und den Festplattendateien jeweils ein

oder mehrere Profile zuordnen können. Hat die VM mehrere Festplatten, können auch unterschiedliche Profile dafür genutzt oder über die Schaltfläche WEITERGEBEN AN FESTPLATTEN dasselbe zugewiesen werden.

Über das Kontextmenü VM-SPEICHERPROFIL → PROFIL ÜBEREINSTIMMUNG PRÜFEN können Sie dann abfragen, ob alles in Ordnung ist oder die VMDK-Festplatten eventuell verschoben werden müssen.

## Optimierung von VMs

Über die Methoden und Faktoren, die die virtuelle Infrastruktur zur Verfügung stellt, habe ich bereits gesprochen. Innerhalb der virtuellen Maschine kann aber ebenfalls einiges erreicht werden, um die Ressourcen besser zu verteilen.

### Optimierung über den vSphere Client

Ob man mit dem vSphere Client nun auf den ESXi Host oder den vCenter Server zugreift, ist bei den folgenden Optimierungen gleich. Beachten Sie zunächst Folgendes:

- Achten Sie bei der Erstellung virtueller Maschinen darauf, ihre Größe – genau wie bei physischen Maschinen – dem tatsächlichen Bedarf anzupassen. Überkonfigurierte virtuelle Maschinen verschwenden gemeinsam nutzbare Ressourcen.
- Deaktivieren Sie zugunsten der besseren Performance sämtliche nicht verwendeten Geräte wie COM-Ports, LPT-Ports, Diskettenlaufwerke, CD-ROMs, USB-Adapter usw. Diese Geräte werden nämlich auch dann regelmäßig vom Gastbetriebssystem abgefragt, wenn sie nicht verwendet werden. Durch dieses unproduktive Abfragen werden gemeinsam nutzbare Ressourcen verschwendet. Achten Sie darauf, dass im BIOS der VM diese Geräte ggf. ebenfalls deaktiviert werden müssen.
- Installieren Sie die VMware Tools. Die unterstützen Sie beim Erreichen einer erhöhten Performance, können zu einer effizienteren CPU-Nutzung führen und enthalten Treiber zum Abrufen von Festplatten-, Netzwerk- und Speicherressourcen.

### Optimierung innerhalb der VM

Optimieren Sie – genau wie beim physischen System – das Betriebssystem der virtuellen Maschine durch Register, Swap-Bereich usw. und passen Sie die Größe der Auslagerungsdatei an. Deaktivieren Sie unnötige Programme und Dienste wie Bildschirmschoner und WLAN-Adapter. Unnötige Programme und Dienste verschwenden gemeinsam nutzbare Ressourcen. Aktualisieren Sie das Gastbetriebssystem stets durch aktuelle Patches. Falls Sie als Gastbetriebssystem Microsoft Windows verwenden, überprüfen Sie, ob es in der Wissensbasis von Microsoft Artikel über bekannte Probleme mit dem Betriebssystem gibt.



Beobachten Sie den Graphen für den Host, den Ressourcenpool und den Cluster (siehe Abbildung 18-6). Stellen Sie ihn gegebenenfalls auf eine andere Ansicht um oder exportieren Sie die Daten nach Excel, um eine Langzeitübersicht zu bekommen.

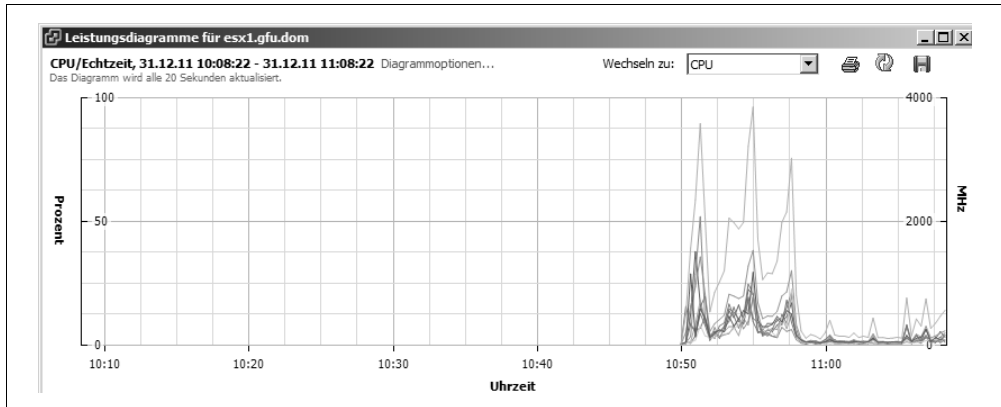


Abbildung 18-6: Leistungsdiagramm über die CPU-Auslastung



Beachten Sie auch, dass sich auf der linken Seite die Prozentzahlen auf den Graphen beziehen und nicht auf die Gesamtkapazität! Hoovern Sie mit der Maus über die dargestellten Linien, um die tatsächliche Last zu sehen (siehe Abbildung 18-7).

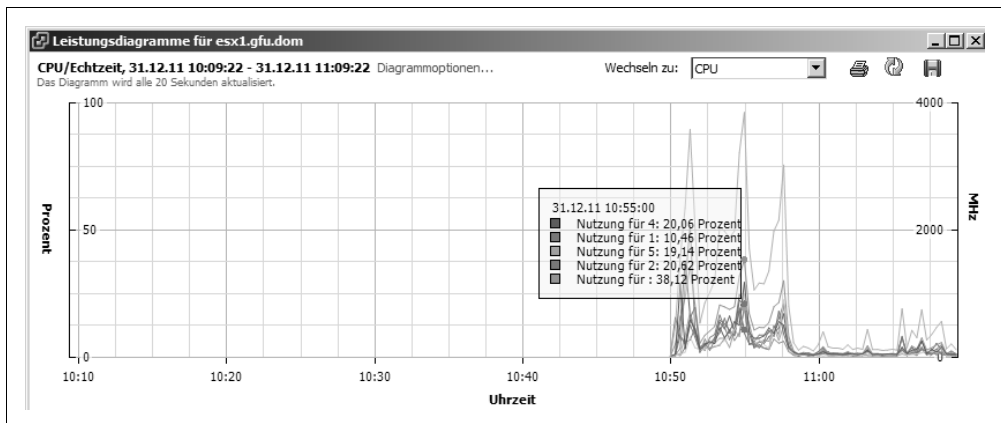


Abbildung 18-7: Genauere Angaben zur prozentualen Auslastung

## Empfehlung für VM-Optimierung

Hier noch einmal zentral die wichtigsten Optimierungsmöglichkeiten für die virtuelle Maschine:

- VM-Hardwareeinstellungen
  - Floppylaufwerk entfernen
  - CD/DVD nicht verbinden
- VM-BIOS
  - Floppy und seine Schnittstelle deaktivieren
  - LPT und COM deaktivieren
  - IDE nur am primären Anschluss
  - Boot von Festplatte
- VM-Betriebssystem (Beispiel Windows)
  - Anzeigeauflösung nur 16 Bit
  - Grafik-Hardwarebeschleunigung auf maximal
  - Bildschirmschoner ausschalten (oder wenigstens nur schwarz)
  - unnötige Dienste ausschalten
  - Autostart und Registry-RUN-Zweige überprüfen

Das sind allgemein gefasste Empfehlungen. Wenn Sie in der VM beispielsweise ein Diskettenlaufwerk oder einen LPT-/COM-Anschluss benötigen, schalten Sie diese natürlich nicht ab.

Nach der Konvertierung einer physischen in eine virtuelle Windows-Maschine sollten Sie die nicht mehr vorhandene Hardware deinstallieren. Geben Sie in einer DOS-Box Folgendes ein:

```
set devmgr_show_nonpresent_devices=1
devmgmt.msc
```

Schalten Sie im Gerätemanager anschließend unter ANSICHT die AUSGEBLENDETEN GERÄTE ein und deinstallieren Sie die nicht mehr vorhandenen, abgeblendet dargestellten Geräte in allen Zweigen – mit Ausnahme des RAS-Adapters und des gesamten Zweigs NICHT-PNP-GERÄTE.

## Performance überwachen

Über die Kommandozeile können Sie die Performance des ESXi Servers ebenfalls überwachen. Das Linux-Kommando `top` gibt es aber nicht für den ESXi Server, verwenden Sie stattdessen `esxtop`.

Das Befehlszeilentool `esxtop` bietet einen sehr ausführlichen Überblick darüber, wie der ESXi Server Ressourcen in Echtzeit nutzt. Das Tool wird auf der Kommandozeile des Hosts ausgeführt.

1. Stellen Sie sicher, dass Sie *root*-Rechte besitzen.
2. Geben Sie den Befehl mit den gewünschten Optionen ein:

```
esxtop [-] [h] [v] [b] [s] [R vm-support_dir_path] [d delay] [n iter]
```

Das *esxtop*-Dienstprogramm liest seine Standardkonfiguration aus der Datei *~/esxtoprc*. In den ersten vier Zeilen sind Klein- und Großbuchstaben enthalten, durch die die Felder und deren Reihenfolge in den Fenstern CPU, ARBEITSSPEICHER, SPEICHER und NETZWERK festgelegt werden. Die Buchstaben entsprechen den Buchstaben in den Fenstern FELDER oder REIHENFOLGE des jeweiligen *esxtop*-Fensters. In der fünften Zeile sind Informationen über die anderen Optionen enthalten. Wichtig ist dabei Folgendes: Wenn Sie eine Konfiguration im sicheren Modus gespeichert haben, erhalten Sie erst dann ein unsicheres *esxtop*, wenn Sie das *s* aus der fünften Zeile der Datei *~/esxtoprc* entfernt haben. Die Verzögerungszeit zwischen einzelnen Aktualisierungen wird durch eine Zahl festgelegt. Wie im interaktiven Modus wird durch die Eingabe von *c*, *m*, *d* oder *n* festgelegt, mit welchem Feld *esxtop* startet.



Von der Bearbeitung der Datei wird abgeraten. Wählen Sie stattdessen die Felder und die Reihenfolge in einem gerade ausgeführten *esxtop*-Prozess aus, nehmen Sie die gewünschten Änderungen vor und speichern Sie diese Datei mithilfe des interaktiven Befehls *w*.

### Beispielanzeige

```
7:32:59am up 19 min, 49 worlds; CPU load average: 0.01, 0.01, 0.01
PCPU(%): 3.87, 0.87 ; used total: 2.37
CCPU(%): 0 us, 1 sy, 99 id, 0 wa ; cs/sec: 58
 ID GID NAME NWLD %USED %RUN %SYS %WAIT %RDY
 1 1 idle 2 195.25 196.86 0.00 0.00 3.14
 2 2 system 6 0.01 0.01 0.00 599.95 0.00
 6 6 helper 22 0.01 0.01 0.00 2199.89 0.01
 7 7 drivers 16 0.34 0.34 0.00 1599.58 0.02
 8 8 vmotion 1 0.00 0.00 0.00 100.00 0.00
 9 9 console 1 2.77 2.78 0.01 97.14 0.08
 15 15 vmware-vmkauthd 1 0.00 0.00 0.00 100.00 0.00
```

Folgende Kommandos sind in dem Fenster verfügbar:

```
^L - redraw screen
space- update display
h or ?- help; show this text
q - quit
```

Interaktive Kommandos sind folgende:

```
fF Add or remove fields
oO Change the order of displayed fields
s Set the delay in seconds between updates
Set the number of instances to display
W Write configuration file ~/esxtoprc
e Expand/Rollup Cpu Statistics
V View only VM instances
```

Sortierung nach:

```
U:%USED R:%RDY N:Default
```

Anzeige umschalten:

m:ESX memory   d:ESX disk adapter   u:ESX disk drive   v:ESX disk VM  
n: ESX nic

Die Zeile Betriebszeit, die sich oben befindet, zeigt die aktuelle Zeit, die Zeit seit dem letzten Neustart sowie die Anzahl der derzeit ausgeführten *worlds* (Welten) und durchschnittliche Lasten an. Als »Welt« bezeichnet man eine durch den ESXi VMkernel planbare Instanz, die mit einem Prozess oder Thread anderer Betriebssysteme vergleichbar ist.

Darunter werden die Durchschnittslasten der letzten Minute, der letzten 5 Minuten und der letzten 15 Minuten angezeigt. Innerhalb der Lastendurchschnitte werden sowohl die gerade ausgeführten als auch die betriebsbereiten Welten berücksichtigt.



Ein Lastendurchschnitt von 1,00 bedeutet, dass alle physischen CPUs vollständig genutzt werden. Ein Lastendurchschnitt von 2,00 heißt, dass das System möglicherweise doppelt so viele physische CPUs benötigt, wie derzeit verfügbar sind. Dementsprechend bedeutet ein Lastdurchschnitt von 0,50, dass die physischen CPUs nur zur Hälfte genutzt werden.

## Statistikspalten und die Reihenfolge

Wenn Sie f, F, o oder O eingeben, zeigt das System eine Seite an, in der die Feldreihenfolge in der oberen Zeile sowie kurze Beschreibungen der Feldinhalte zu sehen sind. Handelt es sich bei dem Buchstaben in der zu einem Feld gehörenden Feldzeichenfolge um einen Großbuchstaben, wird das Feld angezeigt. Ein Sternchen vor der Feldbeschreibung bedeutet, dass ein Feld angezeigt wird.

Die Reihenfolge der Felder entspricht der Reihenfolge der Buchstaben in der Zeichenfolge. Folgende Aktionen sind im Fenster FELDAUSWAHL möglich:

- Wechseln zwischen der Anzeige eines Felds durch Eingabe des entsprechenden Buchstaben.
- Verschieben eines Felds nach links durch Eingabe des entsprechenden Großbuchstaben.
- Verschieben eines Felds nach rechts durch Eingabe des entsprechenden Kleinbuchstaben.

## esxtop im Batch-Modus

Mithilfe des Batch-Modus können Sie Ressourcennutzungsstatistiken in einer Datei erfassen und speichern. Für die Ausführung im Batch-Modus sind einige vorbereitende Schritte erforderlich.

So bereiten Sie das Ausführen von *esxtop* im Batch-Modus vor:

1. Führen Sie *esxtop* im interaktiven Modus aus.
2. Wählen Sie in allen vier Fenstern die für Sie interessanten Spalten aus.

3. Speichern Sie diese Konfiguration in der Datei `~/.esxtop3rc`, indem Sie den interaktiven Befehl `W` ausführen. (`~` ist das jeweilige Home-Verzeichnis des Users.)

So führen Sie *esxtop* im Batch-Modus aus:

1. Rufen Sie *esxtop* auf, um die Ausgabe in eine Datei umzuleiten, zum Beispiel so:

```
esxtop -b > daten.csv
```

Der Dateiname muss die Erweiterung `.csv` haben. Diese ist zwar für *esxtop* selbst nicht zwingend erforderlich, aber für die nachverarbeitenden Tools.

2. Die im Batch-Modus erfassten Statistiken können in Tools wie Microsoft Excel und Perfmon verarbeitet werden.

Im Batch-Modus akzeptiert *esxtop* keine interaktiven Befehle. Im Batch-Modus wird es ausgeführt, bis es die angeforderte Anzahl von Wiederholungen erzeugt hat (weitere Informationen finden Sie unter der Befehlszeilenoption unten) oder bis Sie den Prozess durch Drücken der Tasten `Strg+C` abbrechen.

Die folgenden Befehlszeilenoptionen sind im Batch-Modus verfügbar:

- b Führt *esxtop* im Batch-Modus aus.
- d Legt die Verzögerung zwischen einzelnen Statistik-Snapshots fest. Die Standardeinstellung ist fünf Sekunden. Das Minimum beträgt zwei Sekunden. Wird ein Wert unter zwei Sekunden festgelegt, wird die Verzögerung automatisch auf zwei Sekunden eingestellt.
- n Anzahl der Wiederholungen. *esxtop* sammelt und speichert Statistiken so oft wie hier angegeben und wird dann beendet.

## vSphere5-Troubleshooting

Nun kommen einige Hinweise, Tipps und Tricks zum Troubleshooting für virtuelle Maschinen, ESXi Hosts und Cluster.

### IDE-Festplatte in SCSI umwandeln

Haben Sie bei einer VM aus Versehen eine IDE- anstelle einer SCSI-Platte genommen und das Betriebssystem schon installiert, kann die Performance beim Datenzugriff darunter erheblich leiden. Haben Sie bei der Erstellung einer älteren Workstation-Version von Windows (2000/XP) TYPISCH gewählt, wird Ihre VM mit ziemlicher Sicherheit einen IDE-Adapter mit Festplatte haben.

Um diesen Missstand zu beheben, gehen Sie wie folgt vor:

1. Gehen Sie in die Einstellungen der VM und klicken Sie auf die Schaltfläche HINZUFÜGEN.
2. Wählen Sie FESTPLATTE und klicken Sie auf WEITER, dann auf NEUE VIRTUELLE FESTPLATTE ERSTELLEN und nochmals auf WEITER.

3. Im nächsten Fenster brauchen Sie nichts zu ändern (außer eventuell die Größe auf MB umzuschalten, da die Größe keine Rolle spielt). WEITER.
4. Bei KNOTEN DES VIRTUELLEN GERÄTES wählen Sie SCSI. WEITER und BEENDEN.
5. Starten Sie das Betriebssystem und melden Sie sich mit administrativen Rechten an. Das neue Gerät müsste automatisch erkannt werden und nach den Treibern fragen.
6. Legen Sie einen Datenträger mit den richtigen Treibern für den SCSI-Adapter ein (z.B. das Floppy-Image *LSI.FLP* von der Website zum Buch) und lassen Sie automatisch nach den Treibern suchen.
7. Ist der Vorgang beendet, schauen Sie im Festplattenmanager nach, ob auch die Platte angezeigt wird. Wenn ja, VM herunterfahren und ausschalten, wenn nein, anderen Treiber wählen.
8. Gehen Sie wieder in die Einstellungen der VM und klicken Sie auf die zweite Festplatte (SCSI) und entfernen sie und löschen sie auch von der Festplatte.

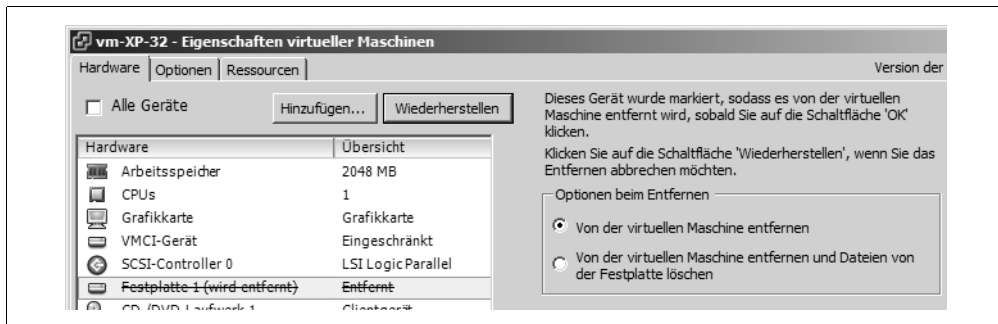


Abbildung 18-8: Festplatte der virtuellen Maschine löschen

9. Wählen Sie nun die erste Platte aus und entfernen Sie diese von der VM – ohne sie von der Festplatte zu löschen – und klicken Sie auf OK (siehe Abbildung 18-8).
10. Verbinden Sie sich mit der Kommandozeile des ESXi Servers (durch putty, WinSCP oder die direkte Konsole) und editieren Sie die *.vmdk*-Datei der VM.
11. Suchen Sie nach dem Eintrag *ide* und ersetzen ihn durch *lsilogic*:
  - `ddb.adapterType = "lsilogic"`
12. Wieder zurück in den Einstellungen der VM fügen Sie eine bestehende Festplatte hinzu, handeln sich bis zum Verzeichnis der VM und wählen die *.vmdk*-Datei aus.
13. Stellen Sie sicher, dass der richtige SCSI-Controllertyp passend zum installierten Treiber ausgewählt wurde. Ändern Sie ihn gegebenenfalls und klicken Sie auf OK.
14. Starten Sie Ihre VM. Fertig.

Sollte es wider Erwarten nicht funktionieren, z.B. weil ein falscher Treiber genommen wurde, können Sie den obigen Vorgang jederzeit wiederholen, in die *.vmdk*-Datei *ide* hineinschreiben und von vorne beginnen.

## Hardwareversion 8 in 7/4 umwandeln

Wenn eine virtuelle Maschine eine Hardwareversion hat, die auf einem älteren ESX Server nicht läuft, weigert sich dieser, die VM zu starten. Das Problem lässt sich leicht auf der Kommandozeile des Hosts abstellen:

1. Gehen Sie, z.B. mit WinSCP, auf das Verzeichnis der virtuellen Maschine. Die Hardwareversion wird nur in zwei Dateien zur VM festgehalten: in der *.vmx*- und *.vmdk*-Datei.
2. Öffnen Sie die Datei *<Name der VM>.vmdk* und editieren Sie sie: Suchen Sie nach der Zeile mit `ddb.virtualHWVersion = "8"` und ändern Sie die 8 in eine 7 oder 4 um. Speichern und schließen Sie die Datei.
3. Öffnen Sie die Datei *<Name der VM>.vmx* und editieren Sie sie: Suchen Sie nach der Zeile mit `virtualHW.version = "8"` und ändern Sie die 8 in eine 7 oder 4 um. Speichern und schließen Sie die Datei.
4. Starten Sie Ihre VM auf dem alten Host.

Sollte Ihre VM neuere Hardware benutzen, die die alte Version des ESX Servers nicht unterstützt, bekommen Sie ggf. eine Fehlermeldung. Das lässt sich aber einfach durch Entfernen und Hinzufügen über den vSphere Client erledigen. VMs mit einem paravirtuellen SCSI-Adapter können z.B. nicht auf Hosts mit der Version 3.x laufen.

## Zeitsynchronisierung in der vSphere-Umgebung

Für die Zeitsynchronisierung in einer typischen Umgebung unterscheidet man zwischen vier verschiedenen Systemen: dem ESXi Host, dem ersten Domänencontroller (PDC-Emulator), Domänenmitgliedern und allein stehenden Rechnern (nicht Mitglied einer Domäne).

Der Domänencontroller, der die Rolle als PDC-Emulator hat (einmal pro Domäne, was bedeutet, dass auch untergeordnete Domänen jeweils einen haben), ist für die Zeitsynchronisierung in der gesamten Domäne verantwortlich. Er sollte mit einer externen Zeit synchronisiert werden (z.B. von einer Funkuhr, aus dem Internet oder vom Zeitserver der übergeordneten Domäne). Alle Domänenmitglieder halten sich an diesen Rechner, was die Zeit anbelangt.

Da eine VM beim Starten und beim Fortsetzen (Resume) die Zeit vom ESXi Server bekommt, sollten Sie alle Hosts ebenfalls mit dem PDC-Emulator abgleichen. Das können Sie über den vSphere Client unter KONFIGURATION → UHRZEITSYNCHRONISATION einstellen. Wenn Sie die Hosts mit derselben Quelle (z.B. dem Internet) abgleichen und die ESXi Server ggf. keinen Zugriff darauf haben, kann auch hier die Zeitinformation nach einiger Zeit erheblich abweichen.

Bei Rechnern, die nicht Mitglieder der Domäne sind, haben Sie drei Möglichkeiten: Sie aktualisieren die Zeit über das Häkchen in den Einstellungen zur VM oder über die

VMware Tools mit dem ESXi Host oder Sie stellen manuell die Synchronisierung im Betriebssystem ebenfalls mit dem Domänenzeitserver ein.

Auf keinen Fall sollten Sie in Ihrer Active Directory-Umgebung gemischte Zeitquellen nutzen. Beachten Sie auch, dass bei unterschiedlichen Uhrzeiten (mehr als 5 Minuten Abweichung) das Zugriffsdomänenticket (Kerberos) seine Gültigkeit verliert. Dann können die User nicht mehr auf Freigaben u. Ä. in der Domäne zugreifen!

## Probleme bei vMotion und HA

Das Verschieben einer virtuellen Maschine von einem Host auf einen anderen wird Migration genannt. Die Migration einer laufenden virtuellen Maschine nennt man vMotion. Die Migration mit vMotion, die zur Verwendung in hochkompatiblen Systemen entwickelt wurde, ermöglicht es Ihnen, eingeschaltete virtuelle Maschinen ohne Ausfallzeiten zu verschieben. Der Protokollstapel des VMkernels muss richtig eingerichtet sein, damit vMotion ordnungsgemäß funktioniert.

»IP-Speicher« bezeichnet jede Art von Speicher, die auf TCP/IP-Netzwerkkommunikation beruht. Dazu gehören iSCSI und NAS/NFS für ESXi Server. Da diese beiden Speichertypen netzwerkbasiert sind, können beide dieselbe Portgruppe verwenden.

Die vom VMkernel zur Verfügung gestellten Netzwerkdienste (iSCSI, NFS und vMotion) verwenden einen TCP/IP-Stapel im VMkernel. Dieser TCP/IP-Stapel ist vollständig getrennt von dem TCP/IP-Stapel, der im Management Network verwendet wird. Jeder dieser TCP/IP-Stapel greift durch die Anbindung mindestens eines vSwitch an mindestens eine Portgruppe auf verschiedene Netzwerke zu.

## Richtlinien

Beachten Sie bei der Konfiguration des VMkernel-Netzwerks folgende Richtlinien:

- Die IP-Adresse, die Sie dem Management Network während der Installation zuweisen, darf nicht der IP-Adresse entsprechen, die Sie dem TCP/IP-Stapel des VMkernels auf der Registerkarte KONFIGURATION → NETZWERK über den vSphere Client zugewiesen haben.
- Vor der Konfiguration von Software-iSCSI für den ESXi Host muss ein Firewall-Port durch Aktivierung des iSCSI-Software-Clientdienstes geöffnet werden. Meist geschieht das automatisch bei der Aktivierung vom iSCSI-Softwareadapter.
- Überprüfen Sie das Kontrollkästchen DIESE PORT-GRUPPE FÜR VMOTION VERWENDEN, damit diese Portgruppe anderen ESXi Servern melden kann, dass sie die Netzwerkverbindung ist, an die vMotion-Datenverkehr gesendet werden soll.
- Achten Sie auf die Schreibweise bei vMotion-Portgruppen: Sie muss bei allen beteiligten Hosts identisch sein.





Auf jedem ESXi Host kann diese Eigenschaft nur für eine vMotion- und IP-Speicher-Portgruppe aktiviert werden. Wenn die Eigenschaft für keine der Portgruppen aktiviert wurde, ist vMotion-Migration auf diesen Host nicht möglich.

Benennen Sie Ihre VMkernel-Portgruppen eindeutig, also z.B. *VMkernel iSCSI*, damit Sie beim Zuordnen nicht durcheinander kommen.

## An HA beteiligte Komponenten

Das Herzstück eines VMware High Availability-Konzepts ist ein Cluster. Fügen Sie möglichst drei oder mehr ESXi Server dieser Unterteilung hinzu. Beachten Sie auch den Hinweis aus Kapitel 10, dass bei sehr vielen Hosts lieber in mehrere Cluster unterteilt werden sollte.

Beim Hinzufügen eines Hosts zum Cluster werden die Informationen und Komponenten auf diese Maschine übertragen.

- Der vCenter Agent *vpva* wird nach dem Übertragen automatisch gestartet.
- AAM ist die VMware High Availability-Komponente, die für die Hochverfügbarkeit zuständig ist.
- VMap ist das Verbindungsstück zwischen *vpva* und AAM.



In einem Cluster sollten Sie möglichst nur gleich ausgestattete ESXi Server einsetzen. Vermeiden Sie unterschiedliche Prozessoren, eine unterschiedliche Anzahl logischer CPUs sowie verschiedene RAM-Ausbaustufen. Gerade im Zusammenhang mit DRS können die nämlich zu Problemen führen.

## High Availability: Isolation und Neustart

Überlegen Sie sich beim Einrichten und Konfigurieren von HA, was Ihnen wichtiger ist: das Starten aller VMs auf den nicht ausgefallenen Servern oder, dass bestimmte Maschinen mit einigermaßen guter Performance laufen.



Wenn Sie in einem Cluster die Zugangssteuerung aktivieren, wird ein gewisser Prozentsatz der zur Verfügung stehenden Ressourcen für einen Hostausfall reserviert. Das bedeutet, dass Sie diese Ressourcen erst nutzen können, wenn ein HA-Fall eintritt – wollen Sie das wirklich?

Sie können über die grafische Oberfläche des vSphere Clients für jede virtuelle Maschine einzeln einstellen, was passieren soll, wenn ein ESXi Server ausfallen sollte (siehe Abbildung 18-9). Richten Sie sich bei diesen Einstellungen nach den Bedürfnissen Ihrer Umgebung!

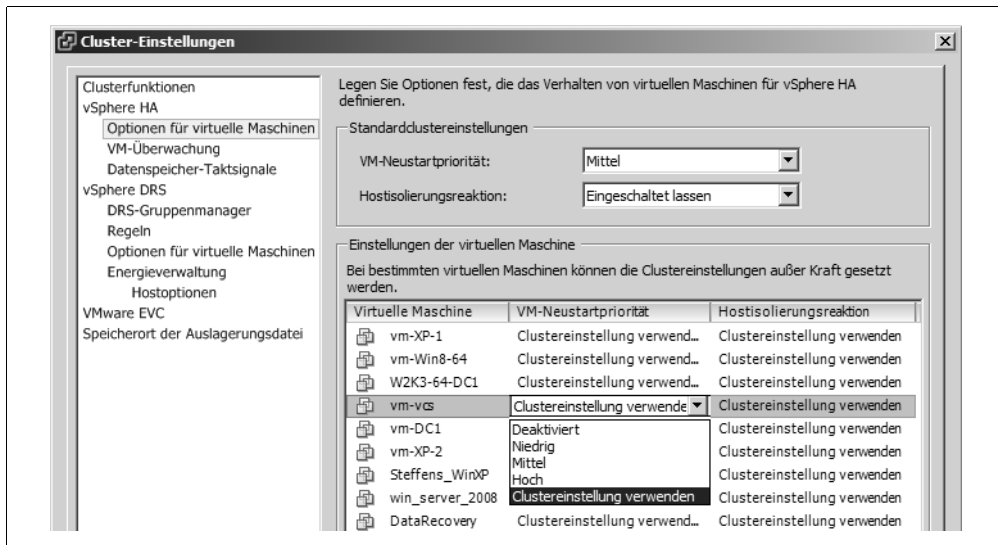


Abbildung 18-9: HA-Einstellungen zur virtuellen Maschine

Sie können HA benutzerdefiniert anpassen, um NEUSTARTPRIORITÄT und ISOLIERUNGSREAKTION zu bestimmen:

- Die NEUSTARTPRIORITÄT bestimmt, in welcher Reihenfolge virtuelle Maschinen nach einem Hostausfall neu gestartet werden. Die Neustartpriorität wird zwar immer berücksichtigt, ist allerdings in folgenden Fällen besonders wichtig:
  - Wenn für den Hostausfall eine Hostanzahl bestimmt wurde (z.B. drei), tatsächlich aber mehr Hosts ausfallen (z.B. vier).
  - Wenn die strikte Zugangskontrolle deaktiviert wurde und mehr virtuelle Maschinen gestartet wurden, als HA einstellungsbedingt unterstützt.



Diese Priorität gilt nur bezogen auf den jeweiligen Host. Fallen mehrere Hosts aus, migriert vCenter zuerst alle virtuellen Maschinen des ersten Hosts in der Reihenfolge der festgelegten Priorität, dann alle virtuellen Rechner des zweiten Hosts ebenfalls in der Reihenfolge der festgelegten Priorität usw.

- Die ISOLIERUNGSREAKTION bestimmt, was geschieht, wenn die Netzwerkkonsolenverbindung eines Hosts innerhalb eines HA-Clusters unterbrochen wird, der Host aber weiterhin ausgeführt wird. Die anderen Hosts des Clusters erhalten kein Signal mehr von diesem Host, erklären ihn für ausgefallen und versuchen, die anderen virtuellen Maschinen neu zu starten.
- Durch eine Festplattensperre wird verhindert, dass zwei Instanzen einer virtuellen Maschine auf zwei unterschiedlichen Hosts ausgeführt werden. Standardmäßig wer-

den virtuelle Maschinen im Fall eines Hostisolierungsereignisses auf dem isolierten Host über die VMware Tools heruntergefahren. Ist das nicht möglich, werden sie automatisch nach fünf Minuten ausgeschaltet, damit sie auf einem anderen Host neu gestartet werden können. Dieses Verhalten kann für einzelne virtuelle Maschinen geändert werden. Sie können die Option **INGESCHALTET LASSEN** auswählen, wenn Sie möchten, dass die virtuelle Maschine auf dem isolierten Host weiterhin ausgeführt wird, auch wenn der Host nicht mehr mit den anderen Hosts des Clusters kommunizieren kann. Das wäre beispielsweise dann angebracht, wenn sich das Netzwerk der virtuellen Maschine auf einem anderen stabilen und redundanten Netzwerk befindet oder die virtuellen Maschinen einfach weiterhin ausgeführt werden sollen. Beachten Sie dazu die ausführlichen Hinweise zur Isolierungsreaktion in Kapitel 10!

## HA-Fehlervermeidung

Bei NAS- oder iSCSI-Speicher verliert die virtuelle Maschine bei der Trennung des Hosts von der Netzwerkkonsole möglicherweise auch den Zugriff auf ihre Festplatte. In diesem Fall können die Festplattensperre aufgehoben und die virtuelle Festplatte erfolgreich auf einem anderen Host eingeschaltet werden. Die virtuelle Maschine auf dem isolierten Host wird weiterhin ausgeführt, hat jedoch keinen Zugriff mehr auf ihre Festplatte (auch wenn die Netzwerkverbindung wiederhergestellt wird), da sie ihre Festplattensperre verloren hat. Diese virtuelle Maschine kann Netzwerk-I/O-Last erzeugen und verbrauchen. Es wird daher dringend empfohlen, die Isolierungsreaktion für virtuelle Maschinen auf NFS- oder iSCSI-Speicher auf *Ausschalten* (je nach Ihrem Netzwerkdesign) zu ändern.

Um bei der Isolierungsreaktion ganz sicherzugehen, dass die VM nicht doch noch Zugriff auf ihre Festplatte hat, können Sie einen weiteren Management Network Port (MNP) auf demselben vSwitch wie den iSCSI- oder NFS-Storage VMkernel Port anlegen. Wird auch diese MNP nicht von den anderen Hosts erreicht, hat die VM auch keinen Zugriff auf ihre Festplatte und kann getrost ausgeschaltet werden. Herunterfahren ist dann nicht mehr möglich.

Wenn Sie einen Host einem Cluster hinzufügen, wird die Neustartpriorität für alle virtuellen Maschinen in diesem Cluster standardmäßig auf Mittel und die Isolierungsreaktion auf Herunterfahren eingestellt.

## HA-Troubleshooting

Falls Sie häufiger Probleme mit dem sekundlichen Taktsignal (Heartbeat) zwischen den ESXi Servern bekommen, können Sie bei den Clustereinstellungen unter **ERWEITERTE OPTIONEN** die zusätzliche Variable `das.failureDetectionInterval` mit einem höheren Wert als eine Sekunde eintragen. Keiner der folgenden Werte ist üblicherweise vorhanden. Intern wird übrigens immer noch die Abkürzung DAS für High Availability genutzt. Sie können auch der Fehlerzeit `das.failureDetectionTime` einen neuen Wert in Millisekunden zuweisen, z.B. 60.000. Dadurch wird ein Host erst als isoliert betrachtet, wenn

das Signal 60 Sekunden lang nicht kommt. Standardmäßig ist dieser Wert 15 Sekunden (15.000 Millisekunden).

Zwei weitere interessante Einstellungen betreffen das Netzwerk: Über den Eintrag `das.allowVmotionNetworks` mit dem Wert `true` können Sie einem Host, der nur eine Netzwerkkarte für das Management Network und vMotion hat, trotzdem das Migrieren von VMs erlauben. Sonst wird diese Portgruppe ignoriert und vMotion ist nicht möglich. Und um den HA-Netzwerkverkehr über eine andere als die Standardadresse laufen zu lassen, z.B. wenn man verschiedene Subnetze dafür generiert hat, kann man den Eintrag `das.allowNetworkX` (wobei X ein Wert von 0 bis 10 sein kann) z.B. mit dem Wert `Management Network 2` belegen, also dem Namen der jeweiligen Portgruppe. Es sind auch mehrere Einträge möglich:

- `das.allowNetwork0Management Network`
- `das.allowNetwork1Management Network 2`

usw.

Standardmäßig kann ein isolierter Host seine eigene Netzwerkisolation feststellen, indem er das Gateway des Management Network überprüft und nicht erreicht (siehe Abbildung 18-10). Damit er dann nicht gleich mit dem Herunterfahren oder Ausschalten der VMs beginnt, kann man auch hier noch eine weitere Sicherheit einbauen: Über den Eintrag `das.isolationaddressX` (X von 1 bis 10) lassen sich ihm weitere IP-Adressen zur Überprüfung mitgeben.

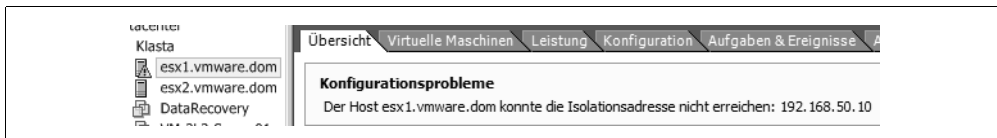


Abbildung 18-10: HA-Konfigurationsprobleme

- `das.isolationAddress1`                      `192.168.150.11`
- `das.isolationAddress2`                      `192.168.50.10`

Dafür kann auch eine IP aus einem anderen Subnetz gewählt werden, wenn sich dort ein weiterer Management Network Port befindet. Überprüfen Sie unbedingt, ob sich diese Adressen auch pinggen lassen. Kann das Standardgateway keinen »Echo Respond«, also keine Antwort auf einen Ping-Befehl senden, dann ergänzen Sie die Liste um folgenden Eintrag:

- `das.useDefaultIsolationAddress`                      `false`

Der Eintrag (Standard ist gesetzt, wird aber nicht angezeigt) `das.maxVmRestartCount` ist intern auf 5 gesetzt. Das bedeutet, dass fünfmal versucht wird, eine VM neu zu starten. Der Wert kann durch einen Eintrag in der Liste auch auf 0 gesetzt werden, damit gar

nicht versucht wird, die VM zu starten. Der Wert kann aber auch höher gewählt werden, was meist aber nicht sinnvoll ist.

Um die Warnung im vCenter Server zu unterbinden, die anzeigt, dass keine Netzwerkredundanz vorhanden ist, tragen Sie in die Liste das `.ignoreRedundantNetWarning` mit dem Wert `true` ein. Tun Sie das aber nur, wenn es nicht möglich ist, eine zusätzliche Netzwerkkarte an das MNP zu binden oder eine weitere Portgruppe dafür einzurichten.

Es gibt noch weitere mögliche Einträge in den erweiterten Einstellungen zu HA, die aber eher seltener gebraucht werden. Ich möchte nochmals ausdrücklich darauf hinweisen, dass ich nicht empfehle, eine der oben genannten Einstellungen *als Standard* zu nehmen und einzutragen. Nur in absoluten Ausnahmesituationen ist es angebracht, hier andere als die Standardwerte zu verwenden.

Ab vSphere 4.1 gibt es die Möglichkeit, Fehler in HA über den neuen Link BETRIEBSSTATUS DES CLUSTER (Cluster Operational Issues) auf der Registerkarte ÜBERSICHT zu sehen. Ist der Fensterinhalt grau, gibt es keine Probleme, ansonsten werden der oder die Einträge angezeigt (siehe Abbildung 18-11).

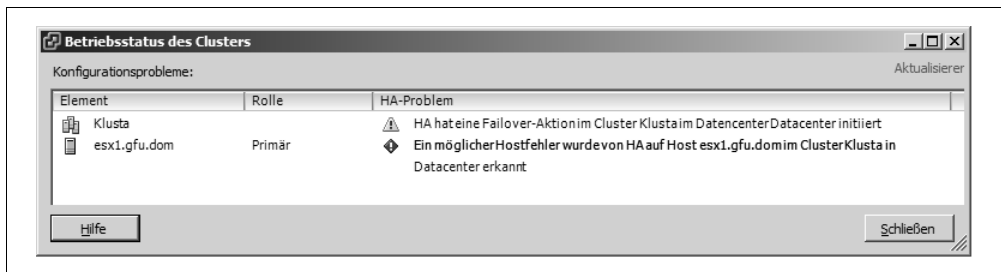


Abbildung 18-11: Betriebsstatus des Clusters

Sollten übrigens zwei Ihrer Hosts ausfallen, werden zuerst die VMs des ersten und anschließend erst die des zweiten ESXi Servers neu gestartet, da sich nur einer der primären Hosts (*master primary*) um den Neustart kümmert. Sollte dieser ausfallen, wird ein anderer automatisch zum Master.

## Datenspeicher-Taktsignale

Sie können das erweiterte Attribut `das.heartbeatdsperhost` verwenden, um die Anzahl der Taktsignal-Datenspeicher zu ändern, die für jeden Host vom vCenter Server ausgewählt wurden. Der Standardwert beträgt zwei und der Maximalwert fünf.



Wenn Sie eine Netzwerkumgebung bereitstellen, in der der Speicher- und der Verwaltungsnetzwerkverkehr über dieselben physischen Netzwerkkarten übertragen werden, deaktivieren Sie die Datenspeicher-Taktsignale. Sie bieten bei dieser Art von Netzwerk keine Vorteile.

## Weitere Tools

In diesem Abschnitt möchte ich Ihnen noch ein paar weitere Tools näher erläutern, unter anderem für die Kommandozeile und ihre Benutzung.

### lspci

Über die vorhandenen PCI-Geräte und -Busse informiert das Programm *lspci*, das Sie über die Kommandozeile als *root* ausführen können. Detaillierte Informationen können mit dem Schalter *-p* erreicht werden, noch mehr Ausgaben erhält man häufig mit *-v*. Der Parameter *-n* zeigt numerisch die Hersteller- und Geräte-ID an, ohne die Namen und weitere Infos aufzulisten.

### tail

Das Programm *tail* ist eigentlich dafür gedacht, jeweils die letzten Zeilen einer Datei zu betrachten. Für Logdateien ist es sinnvoll, sich damit über die letzten Meldungen zu informieren. Über den Schalter *-f* kann man sich aber auch interaktiv die Zeilen einer Datei anzeigen lassen, und die Anzeige wird so lange aktualisiert, bis man sie mit der Tastenkombination Strg+C abbricht. Hier ein Beispiel:

```
tail -f /var/log/vmkwarning
```

Um zu sehen, in welche Logdatei als Letztes geschrieben wurde, kann man eine Kombination von *ls -al* mit *sort* verwenden. Das Tool *sort* sortiert dabei nach Nummern und Alphabet in der Spalte, die Sie angegeben haben.

Mit dem Befehl kann man auch eine umgekehrte Sortierung (reverse) anzeigen lassen:

```
ls -al | sort -r
```

Anschließend können Sie die zuletzt angezeigte Logdatei mit *tail -f* überwachen.

Einfacher geht es mir den Parametern *-ltr* beim Aufruf von *ls*. Geben Sie also *ls -ltr* ein, um die Anzeige nach Datum und Uhrzeit sortiert zu bekommen.

Kommt es in der Datei */var/log/vmkwarning* häufig zu Meldungen über SCSI-Reservierungskonflikte, kann das übrigens an einer falschen Konfiguration des Fibre-Channel-Switch liegen. Stellen Sie dann die Übertragungsrate auf beiden Seiten der Verbindung auf »fix« ein, also z.B. »2G«.

## ESXi Server hängt

Sollte es beim Starten oder Herunterfahren zum Hängen des Systems kommen, hilft oft die Ausgabe von Informationen auf der zwölften Konsole. Schalten Sie mit (Strg+)*Alt+F12* auf diese Konsole und lesen Sie die Meldungen, die der ESXi Server dort auflistet.

Ein häufige Ursache ist das Fehlen oder Nichtreagieren von SAN- und iSCSI-Speicher. Normalerweise reicht ein Timeout von zwei bis drei Minuten, so dass der ESXi Server mit dem Herauf- oder Herunterfahren weitermacht. Sollte das nicht zum Ziel führen, hilft leider nur noch der harte Reset. Das ist allerdings keine Garantie dafür, dass es anschließend besser geht. Wenn nicht, starten Sie den Server mit zusätzlichen oder weniger Optionen, indem Sie beim Start die Tastenkombination Shift+O drücken.

## RVTools

Ein sehr mächtiges Werkzeug hat der Holländer Rob de Veij auf .NET 2.0-Basis mit dem VI SDK (Software Development Kit) programmiert. Unter [www.robware.net](http://www.robware.net) kann man es samt einer englischsprachigen Dokumentation kostenlos herunterladen. Zurzeit ist die Version 3.2 vom Oktober 2011 aktuell und kann auch die Umgebung eines vSphere5 untersuchen.

Nicht nur, dass man damit in Listenform Informationen der ESXi Server und der virtuellen Maschinen erhält, z.B. zu CPU, Netzwerkkarten, IP-Adressen, Arbeitsspeicher und anderem – es werden auch aktive Snapshots sowie verbundene optische und Diskettenlaufwerke ausgegeben und viele weitere nützliche Informationen aufgelistet, die in diesem Kapitel eine Rolle gespielt haben. Man kann darüber sogar Änderungen bei der Konfiguration der VMs durch einfaches Setzen eines Häkchens erreichen.

Auf der letzten Registerkarte TABVHEALTH werden unter anderem

- VM-Festplatten angezeigt, die zu keiner virtuellen Maschine mehr gehören,
- der Speicherplatz auf den Laufwerken der VMs angezeigt, die weniger als 10 % freien Speicher haben,
- angezeigt, ob die VMware Tools aktualisiert werden müssen oder gar nicht installiert sind, und
- angezeigt, ob der Ordnername mit dem Namen der VM in der Bestandsliste übereinstimmt.

Die gesammelten Ergebnisse lassen sich exportieren – sogar in eine Excel-Arbeitsmappe.

Auf der letzten Registerkarte mit Namen TABVHEALTH, wie in Abbildung 18-12 zu sehen ist, werden unter anderem:

- VM-Festplatten angezeigt, die zu keiner virtuellen Maschine mehr gehören,
- der Speicherplatz auf den Laufwerken der VMs angezeigt, die weniger als 10% freien Speicher haben,
- angezeigt, ob die VMware Tools aktualisiert werden müssen oder gar nicht installiert sind, und
- angezeigt, ob der Ordnername mit dem Namen der VM in der Bestandsliste übereinstimmt

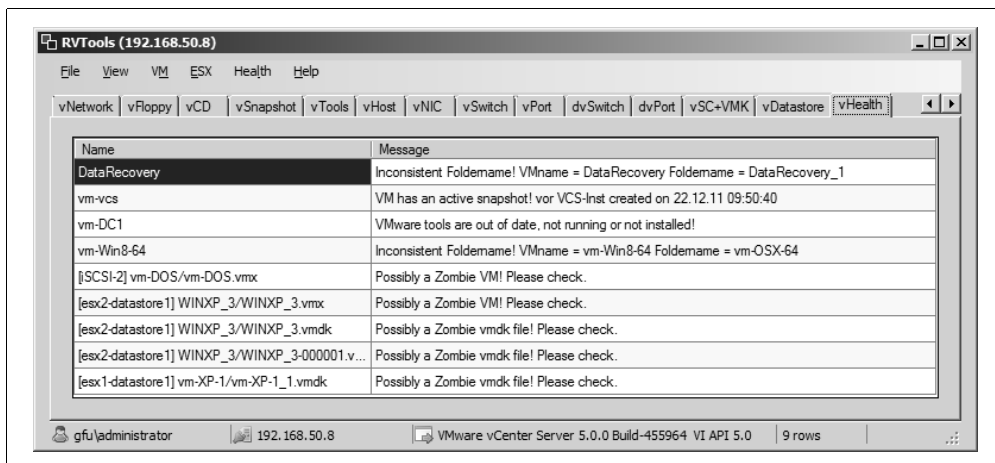


Abbildung 18-12: RVTools, Beispielkarte vHealth

Die gesammelten Ergebnisse lassen sich exportieren – sogar in eine Excel Arbeitsmappe.

Ähnlich wie ich es in Kapitel 4, *Die virtuelle Maschine* beschrieben habe, können dem Programm Parameter übergeben werden, die ähnlich denen des vSphere Clients sind. Dazu gehört auch der Username mit -u, das Passwort mit -p und der vCenter Server mit -s. Des Weiteren können für den Aufruf noch Exportbefehle mit Verzeichnis -d und Dateiname -f übergeben werden und ob es eine CSV- oder XLS-Datei sein soll.

Ein Beispielaufruf kann also folgendermaßen aussehen:

```
RVTools.exe -u root -p ganzgeheim -s 192.168.100.50 -c ExportAll2xls -d c:\Temp -f 2011-12-24.xls.
```

Um nur eine Tabelle zu exportieren, also die oben erwähnte »Gesundheitsliste«, kann man beispielsweise die Parameter -c ExportHealth2xls -d c:\Temp -f vHealth.xls angeben.

Ich kann nur jedem empfehlen, dieses Tool einmal auszuprobieren und sich bei Bedarf die ausführliche, 61 Seiten starke Dokumentation anzusehen.

Bei den Kunden, die ich betreue, nehme ich dieses Werkzeug regelmäßig zur Hand und bin begeistert davon – mit einer Ausnahme: Auf der Seite mit den verbundenen optischen (*tabvCD*) und Diskettenlaufwerken (*tabvFloppy*) der virtuellen Maschinen stimmen die Angaben häufig nicht. Aber man sieht hier wenigstens, ob die Laufwerke verbunden sind oder nicht – und diese Anzeige stimmt.

## Veeam Fast SCP

Dieses Tool ist die richtige Lösung für schnelles Kopieren auf den Storage eines Hosts und für das Kopieren oder Verschieben zwischen ESXi Servern. Der Transfer läuft über eine sichere Verbindung mit SSH, das auch vom ESXi unterstützt wird. Die Geschwindigkeit eines Transfers über FastSCP (Secure Copy) geht ca. sechsmal schneller als über her-



kömmliches SCP oder dem Datastore-Browser. Weiterhin können Sie zu mehreren Hosts gleichzeitig eine Verbindung aufbauen (Single Sign-On). FastSCP stellt die Umgebung ähnlich wie im Explorer dar und ermöglicht es sogar, Attribute von Dateien und Ordnern zu ändern. Und das Ganze ist kostenlos von der Internetseite des Herstellers herunterladbar, [www.veeam.com/de/](http://www.veeam.com/de/).



## A

- Acronis Backup&Recovery 346
- Active Directory 121
- Adapertypen 49
- Affinität 99
  - Probleme 439
- Affinitätsregeln 446
- Agent-VM-Einstellungen 124
- Akzeptanzebene 123
- Alarm
  - benutzerdefiniert 387
- Alarmer 385
  - ändern 386
  - Bedingungslänge 390
  - Befehle 390
  - Beispiel Bedingungen 389
  - Beispiel CPU Auslastung 386
  - Beispiel CPU-Nutzung 390
  - Beispiel Skript 391
  - Beispiel VM starten 387
  - Benachrichtigungen 387
  - bestätigen 388
  - deaktivieren 393
  - eigene 386
  - Komponenten 385
  - mehrere Bedingungen 389
  - Schwellenwerte 390
  - Skripte 390
  - Vererbung 386
  - Zeitangaben 389
- Alarmfunktionen 385
- AMD Pacifica 4
- AMD RVI 94
- AMD-V 4, 24, 94
- Anpassungsspezifikation 369

- Anteile 97, 444
- Antivirensoftware 428
- Anwendungsüberwachung 301
- Appliance 137, 322
- Appliances 124
- Arbeitsspeicher
  - der VM ändern 73
  - Ressourcen zuweisen 97
- Asset-Instanz 282
- ausdrückliche Failover-Reihenfolge verwenden 163
- Authentication Proxy 276
- Authentifizierungsdienste 121
- Auto Deploy 276
- Automatische Upgrades
  - VMware Tools 65

## B

- Backup
  - Ziele 398
- Befehle
  - alias 233
  - cat 233
  - cd 233
  - chgrp 233
  - chmod 233
  - chown 233
  - clear 233
  - cp 233
  - date 233
  - dd 234
  - df 234
  - du 234
  - esxcfg-fcoe 244
  - esxcfg-hwiscsi 244

- esxcfg-ipsec 244
- esxcfg-rescan 244
- esxcfg-scsidevs 244
- esxcfg-volume 244
- find 234
- grep 234
- groupadd 234
- gunzip 234
- gzip 234
- halt 234
- head 234
- hostname 234
- kill 234
- less 235
- ls 235
- lsuf 235
- lspci 235
- md5sum 235
- mkdir 235
- mv 235
- passwd 235
- ps 235
- pwd 235
- reboot 236
- rm 236
- rmdir 236
- scp 236
- set 236
- su 236
- tail 236
- tar 236
- touch 237
- useradd 237
- userdel 237
- usermod 237
- which 237
- who 237
- whoami 237
- Benachrichtigungen 354
- Benutzer 131
  - Standardrollen 135
- Berechtigungen 133
  - auf der Kommandozeile ändern 233
  - Beispiel 134, 136
  - WebAccess 338
- Betriebssysteme lizenzieren 283
- BIOS 24
- BIOS-Einstellungen 100
- boot.cfg-Datei 33

## C

- CD-/DVD-ROM 76
- CDP siehe Cisco Discovery Protocol 164
- Challenge-Handshake Authentication Protokoll (CHAP) 420
- CHAP 420
- Cisco Discovery Protocol 164
- Cisco-Switch-Informationen 165
- CleanShutdown 292
- Clienteneinstellungen 125
- Cloud 14
- Cluster 291
  - einrichten 295
  - erstellen 291
- config-Datei 30
- Configure Keyboard 29
- Configure Management Network 28
- Configure Password 26
- Consolidated Backup 397
- Converter 345
  - abschließende Arbeiten 350
  - Festplatte anpassen 78
  - Importmöglichkeiten 346
  - Installation 347
  - Probleme 351
  - Voraussetzungen 347
- Converter Client 347
- Converter Server 347
- Converter Standalone 345
- CPU
  - Ressourcen zuweisen 96
  - Zuweisung 438
- CPU-Affinität 438
- CPU-Hotplug 91
- CPU-ID-Maske 91
- CPU-Maske 91

## D

- Daemon 226
- DAS 295
- Data Recovery 397
  - Anforderungen 400
  - Assistent 405, 409
  - Aufbewahrungsrichtlinie 408
  - Backup-Ziele 398
  - Editionen 399
  - einschalten 403
  - Festplatte hinzufügen 402
  - installieren 401

- Konfiguration 403, 405
- Plug-In 398, 401
- Probewiederherstellung 413
- Probleme beheben 415
- Sicherungsaufgabe 407
- Sicherungszeiten 407
- Snapshot 398
- Systemkonfiguration 405
- Wiederherstellung 410
- Datacenter 288
- Datastore-Browser 104
- Datei
  - esx.conf 228
  - hosts 226
  - inittab 245
  - nsswitch.conf 226
  - ntp.conf 246
  - passwd 227
  - resolv.conf 226
  - shadow 227
  - sshd\_config 227
- Dateibedeutung
  - dsk 106
  - flat.vmdk 106
  - hlog 106
  - lck 106
  - log 106
  - nvrn 105
  - redo 106
  - vmdk 106
  - vmsd 106
  - vmsn 106
  - vmss 106
  - vmx 105
  - vmxf 105
  - vmxt 106
  - vswp 106
- Dateien der virtuellen Maschine 104
- Datenspeicher
  - Dateien hochladen 43
- Datenspeicher-Taktsignale 301, 461
- Dauerhaft (Festplattenmodus) 216
- Deduplizierter Speicher 397
- Deduplizierungsspeichertechnologie 400
- Disaster Recovery 370
- Diagrammoptionen 130
- DirectPath I/O-Konfiguration 116
- Direktausführung 438
- Disable ESXi Shell 29
- Disable SSH 29

- Diskettenlaufwerke 76
- Distributed Power Management (DPM) 293, 308
- Distributed Resource Scheduling (DRS) 292
- DNS (Domain Name System) 226
- DNS- und Routing 121
- DPM 293
  - einrichten 308
- DRS 292, 302
  - Beispiel 303
  - Gruppen 303
  - Konfiguration 301
  - Regeln 303
- Duplexeinstellung 163
- Duplexmodus 164
- DVD-/CD-ROM 76
- DVfilter 120

## E

- e1000 84
- Editor vi 224
- EFI-Einstellungen 104
- Ein-Wege-CHAP-Authentifizierung 420
- Emulation 1
- Enable ESXi Shell 27, 29, 227
- Enable SSH 29
- Energieverwaltung 90, 305
- Enhanced vMotion Compatibility (EVC) 294
- Enterprise Plus 15
- Enterprise Plus AK 16
- Ereignisse 132
- Erweiterte Einstellungen 124
- Essentials Plus 15
- Essentials Plus Kit 16
- ESX
  - Hardwareanforderungen 21
- ESX Server
  - Upgrade 359
- ESX -Server über Kommandozeile konfigurieren 241
- esxcfg-tools 241
- ESXi
  - Backup 396
  - Befehle 127
  - Benutzer anlegen 131
  - Berechtigungen 133
  - Dienste 225, 245
  - Embedded 20
  - Energieverwaltung 118
  - Ereignisse 132
  - Gruppe anlegen 131

- Herunterfahren 127
- Hostprofil 315
- Installable 20
- Installation 23
- Installation über USB 33
- Installationsskript 31
- Konfiguration 26
- Konfigurationsdateien 225
- Lockdown 27
- Logdateien 30
- Maximalwerte 259
- Netzwerkeinstellungen 28
- Neu starten 127
- Passwort 26
- Sicherheitsprofil 122
- Sperrmodus 430
- Systemstatus 114
  - updaten 355
- ESXi Dump Collector 275
- ESXi Server 11
  - Hardwareeinstellungen 114
  - in vCenter integrieren 289
  - Leistungsdaten 130
  - Menü-Überblick 137
  - Softwareeinstellungen 118
  - Standardrollen 135
  - Überblick über die Registerkarten 125
- ESXi Shell
  - Befehle 233
- ESXi Single Server 15
- esxtop 450, 451
- esxtop im Batch-Modus 452
- esxtoprc 451
- Ethernet-Adapter 83
- eui (Extended Unique Identifier) 188
- EVC 294, 306

## F

- Failover Reihenfolge 173
- Failover-Host 296
- Fault Tolerance (FT) 294, 309
  - einschalten 311
  - SiteSurvey 314
  - Voraussetzungen 309
- Fehlerbehebung
  - Management Network 172
  - Namensauflösung 171
  - Netzwerk 169
  - Netzwerkadapter 170
  - Portgruppe 171

- Fehlermeldung
  - Log-Dateien 38
- Fehlermeldungen 339
- Fernzugriff 27, 327
  - RDP 342
  - WebAccess 332
- Festplatte
  - emulieren 6
- Festplattenanschlusstyp ändern 86
- Festplattendateien
  - verwalten 239
- Festplattenformate 52
- Festplattenmodus
  - Dauerhaft 78
  - Nicht-dauerhaft 78
- Fibre Channel-NPIV 93
- Filter 130
- Firewall 122, 431, 432
- Firewall-Einstellungen 122, 230
- Firewall-Ports 433, 434
- flexibel (Adaptertyp) 84
- FLP-Dateien 77
- Forged Transmits 423
- FT 294

## G

- Gefälschte Übertragungen 162, 423
- Gerätemanager 450
- Grafikbeschleunigung 60
- Grafikkarteneinstellungen 75
- Grenzen 437
- Grenzwert 97
- Gruppen 131
- GUI aktualisieren 231

## H

- HA
  - Fehlervermeidung 459
    - konfigurieren 295
    - Master 295
    - Troubleshooting 459
  - HA (High Availability) 291, 295
    - Isolation 457
    - Komponenten 457
    - Neustart 457
    - Probleme 456
- Hardware
  - Anforderungen für ESX Server 21
  - Kompatibilität 19

- Hardwareversion 8 in 7/4 umwandeln 455
- Heartbeat 297
- Hewlett-Packard Integrated Lights-Out (iLO) 308
- High Availability 291, 457
- Hilfe 140
- Hochverfügbarkeit 291, 457
- Host 19
  - Definition 1
  - in der vSphere-Umgebung 11
  - Patches bereitstellen 356
  - Standardisieren 356
  - updaten 355
- Host-Cache-Konfiguration 124
- hostd-Datei 30
- Hostisolierungsmodus
  - ausschalten 299
  - eingeschaltet lassen 298
  - herunterfahren 298
- Hostisolierungsreaktion 296
  - Einstellung 297
- Hostprofil
  - ändern 317
  - anhängen 318
  - bearbeiten 317
  - erstellen 315
  - Richtlinie 317
  - Übereinstimmung prüfen 318
- Hosts-Datei 226
- Hostübersicht 139
- Hostüberwachungsstatus 295
- Hostverwaltung 126
- Hot-Cloning 348
- Hyperthreading 24, 99, 115, 440
- Hypervisor 11

## I

- IDE Festplatte in SCSI umwandeln 453
- IIS 268
- iLO 308
- Imagedateien 77
- Intel EPT 94
- Intel VT 4
- Intel VT-x 94
- Intelligent Platform Management Interface (IPMI) 308
- Intel-VT 24
- IOMMU 87
- IP Configuration 28
- IPMI 308
- IP-Pool 330

- IP-Speicher 146
- IPv6 147, 148
- IPv6 aktivieren 147
- iqn (iSCSI Qualified Name) 188
- iSCSI
  - Initiatoren 181, 191
  - Konfiguration 183
  - Netzwerkkonfiguration 186, 187
  - Probleme 190
  - Softwareadapter 188
  - Target 181
- ISO-Datei 42, 77
- ISO-Images erstellen 234
- Isolierungsreaktion 458

## J

- Jumbo-Frames 166
  - aktivieren 167
  - VMkernel 167
- JVM-Arbeitsspeicher 271

## K

- Kennwortkomplexität 425, 426
- Kennwortverwendungsdauer 425
- Klonen 374
- Kommandozeilenbefehle 233
  - Liste 247
- Konfiguration
  - ESXi Server 26
  - vSphere Client 36
- Konfigurationsprobleme 125
- Konsolidierung 345
- ks.cfg-Datei 31

## L

- Leistungsdaten 130
- Linux-Befehle 233
- Lizenzschlüssel 282
- Lockdown Mode 27
- Log-Dateien
  - vCenter Server-Installation 284
- lspci 462
- LUN Number 181

## M

- MAC-Adressänderungen 162
- MAC-Adresse 111
- MAC-Flooding 421

- MAC-Imitation 424
- Management Network
  - ändern 159
  - einrichten 159
- Maximalwerte
  - ESXi 259
  - Konfigurationsoptionen 263
  - Netzwerk 261
  - Ressourcenpools 262
  - Update Manager 264
  - vCenter Server 263
  - VM 258
  - vSphere5 257
- Memory Management Unit (MMU) 94
- Microsoft .NET 3.5 SP1 34
- Migration 292, 456
  - einer physischen Maschine in eine VM 348
  - im laufenden Betrieb 348
  - Probleme 351
  - Schwellenwerte 302
- MKS (Mouse, Keyboard, Screen) 55, 334
- Modify ESXi Shell timeout 29
- Mouse-Keyboard-Screen (MKS) 334
- MPIO/Multi-Pathing 120
- MTU 147, 166
- Multicast-Brute-Force-Angriffe 422

## N

- Namensauflösung 171, 226
- NetQueue 168
- Network Time Protocol (NTP) 229
- Netzwerk
  - Maximalwerte 261
- Netzwerkadapter
  - Problemlösungen 170
- Netzwerkadaptertypen 84
- Netzwerkdienste 149
- Netzwerkkarten aufteilen 173
- Netzwerkkonfiguration 28
  - Fehlerbehebung 169
- Netzwerkloadbalancing 162
- Netzwerkoptimierungen 169
- Neustartpriorität 458
- NIC-Gruppierung 146, 162
- Nicht dauerhaft (Festplattenmodus) 217
- NIC-Teaming 146
- NTP (Network Time Protocol) 120, 229
- NTP-Client 229
- NTP-Einstellungen 62

- NUMA 100, 439
- NX-Flag 91

## O

- Optimierung 437
  - virtuelle Maschinen 69
- Outbound-Adapter 144
- OVF-Format 124, 137
- OVF-Vorlage 56
  - exportieren 137
- OVF-Vorlage bereitstellen 137

## P

- Pacifica 4
- Parallelport 80
- Passthrough-Geräte 116
- passwd 27, 227
- Passwort
  - Beschränkungen 424
  - Kennwortverwendungsdauer 425
  - Komplexität 426
- Passwortlänge 27, 227
- Patch-Download-Einstellungen 354
- Patch-Download-Zeitplan 354
- Patches 231, 345
- PCI-Geräte 87
- PCI-Passthrough 87
- Performance überwachen 450
- Plattenbelegung 234
- Portabsicherung 422
- Portgruppen 154
  - Problemlösungen 171
  - Übersicht 160
- Profile Driven Storage 446
- Promiscuous-Modus 161, 424
- Prozessor Exception 5
- Prüfsummen erstellen 235
- putty 29
- PXE 101

## Q

- Quest 417

## R

- RCLI 20
- Rechtevererbung 134
- Rechtevergabe 133
- Registerkarte Erste Schritte 37



- Remote Command Line Interface (RCLI) 20
- Remote Desktop Protokoll 342
  - Parameter 343
- Remote-Console 337
- Remotedesktop-Verbindung 76
- Reservierung 97, 437
- Reset System Configuration 31
- Ressourcen verwalten 437
- Ressourcenpool 443
  - Richtlinien 445
  - versus vApp 327
- Ressourcenpools
  - Maximalwerte 262
- Restart Management Agent 30
- Restart Management Network 28
- Restore Management Network 28
- Restore Standard Switch 29
- Ring-Modi eines Betriebssystems 5
- Rolle
  - Administrator 135
  - Kein Zugriff 135
  - Nur Lesen 135
- Rollen 133, 135
  - Standardrollen 135
- Routing
  - anhand der Quelle der Port-ID routen 163
  - anhand des IP-Hashes routen 163
  - anhand des Quell-MAC-Hashs routen 163
- Routing-Tabelle 158

## S

- SAN-LUN 50
- scratch/log/ 285
- SCSI
  - Sharing 77
- SCSI-Controller 77
- SCSI-Hardware 85
- Sensoren 114
- Serieller Port 81
- Shares 437
- Sicherheit 419
  - CHAP-Authentifizierung 420
  - Gefälschte Übertragungen 423
  - MAC-Adressänderungen 423
  - MAC-Flooding 421
  - MAC-Imitation 423, 424
  - Multicast-Brute-Force-Angriffe 422
  - Netzwerk 421
  - Portabsicherung 422
  - Promiscuous Mode 424

- Spanning-Tree-Angriffe 422
- Storage 419
  - VMsafe 428
  - Zufallsdatenblock-Angriffe 422
- Sicherheitsempfehlungen 428
- Skripte 245
- SMASH-Profil 114
- Snapshot
  - Dateien 221
  - Definition 213
  - Domänencontroller 215
  - Empfehlungen 214
  - erstellen 215
  - Fehlerbehebung 221
  - Festplattenmodi 216
  - Funktionsweise 214
  - löschen 218
  - Manager 217
  - übergeordneter 219
  - wechseln zu 218
  - wiederherstellen 219
- Snapshots 398
- Software-Assets 282
- Speicher DRS 446
- Speicherballontreiber 442
- Speicherprofile
  - aktivieren 447
- Sperrmodus 27, 430
- SSD Festplatte 124
- Standardgateway
  - festlegen 159
- Standard-Hardware 6
- Standardisieren 356
- Standard-Switches
  - Eigenschaften 161
- Standby-Adapter 173
- Storage
  - formatieren 189
  - hinzufügen 188, 189
  - vMotion 211
- Storage Appliance Manager 324
- Storage DRS 446
- Storage vMotion 292
- Storage-Profil 447
- Syslog Collector 275
- syslog-Datei 30
- Syslog-Dienst 38
- Sysprep 370, 372
- Systemprotokolle 137
- Systems Management Architecture for Server
  - Hardware (SMASH) 114

## T

- tail 462
- Tastaturlayout 29
- TCP Segmentation Offload (TSO) 146, 166
- TCP-Ports 432
- Templates 369
  - Anpassung 372
  - Assistent 374
  - Empfehlungen 369
  - Konfigurationsdatei 379
- Test Management Network 28
- Thick-Provision Lazy-Zeroed 52
- Thin-Bereitstellung (Festplattenformat) 52
- TLB 441
- Tool
  - Backup & Replication 418
  - FastSCP 418
  - lspci 462
  - tail 462
  - vConverter 417
  - vRanger 417
  - vReplicator 417
- Tool esxcli 250
- Tool localcli 250
- Tool vim-cmd 251
- Tool vmkvsitools 251
- top 450
- Traffic-Shaping 162
- Treiberproblem
  - Windows 2008 60
  - Windows 7 60
- Troubleshooting Mode Options 27, 227
- Troubleshooting Options 29
- TSO 146, 166

## U

- UDP-Ports 432
- Uhrzeitkonfiguration 120
- UID 131
- Unbeaufsichtigte Installation
  - VMware Tools 66
- Update Manager 345
  - Baseline 353
  - Benachrichtigungen 355
  - Datenbank 274
  - Ereignisse 355
  - ESX Upgrade 362
  - Hardware-Upgrade 366
  - Installation 273

- Konfiguration 353
- Maximalwerte 264
- Patch-Repository 355
- Plug-In 352
- Proxy Einstellungen 274
- Repository 354
- vApp 355
- Updates 231, 345
  - Update Manager X, 345
- Upgrade 320, 358
  - von ESX auf ESXi 360
- Uplink-Adapter 144
- USB Dongels 343
- USB-Anschlüsse 342
- USB-Controller 83

## V

- VA Marketplace 139
- vAAI 120
- Vanderpool 4
- vApp 327
  - Einstellungen 328
  - erstellen 328
  - IP-Pools 329
  - löschen 332
  - OVF-Export 327
  - Startreihenfolge 329
- vApp bereitstellen 137
- vCenter
  - Appliance 266
  - Komponenten 255
  - Orchestrator 272
- vCenter Orchestrator 265
- vCenter Server
  - Active Directory 383
  - Anmeldung 288
  - Checkliste 268
  - Datenbankaufbewahrungsrichtlinie 384
  - Datenbankgröße 382
  - Datenbankverbindungen 384
  - Dienstabhängigkeiten 286
  - Dienste 276
  - Einstellungen 381
  - E-Mail Einstellungen 384
  - Ereignisse 286
  - Erweiterte Einstellungen 385
  - Firewall konfigurieren 431
  - Hardwareanforderungen 265
  - herunterladen 126
  - Installation 269

- Laufzeiteinstellung 382
- Lizenzen 280
- Lizenzierung 381
- Log-Dateien 283
- Maximalwerte 263
- Ports 266
- Protokolloptionen 384
- SNMP 384
- SSL Einstellungen 384
- Startprobleme 286
- Statistik 382
- virtuell 269
- Voraussetzungen 265
- Zeitüberschreitung 384
- vCenter Server Appliance 278
  - Einschränkungen 278
  - Hardware 279
  - Konfiguration 279
- vCenter Support-Tools 275
- vCenter-Agent 119
- vConverter 346
- VIB-Dateien 123
- vi-Editor 224
- View Support Information 30
- Virtual Local Area Network (VLAN) 150
- Virtual Machine Monitor (VMM) 94, 440
- Virtual Switch Tagging 151, 152
- Virtualisierung
  - Grenzen 3
  - Konzept 5
  - Überblick 1
  - Vorteile 2
- Virtualisierungsmodus 438
- Virtuelle Appliance 137
- Virtuelle Maschine
  - Betriebszustand 89
  - BIOS-Einstellungen 100
  - CD-/DVD-Laufwerke 77
  - CPU 4
  - CPU-Anzahl 74
  - Dateien 104
  - debuggen 90
  - Definition 1
  - Desktopverknüpfung 337
  - Diskettenlaufwerke 77
  - DRS-Optionen 305
  - EFI-Einstellungen 104
  - emulierte Komponenten 3
  - erstellen 41
  - Fernzugriff 327
  - Festplatte 6
  - Festplattendateien verwalten 239
  - Festplattengröße ändern 78
  - HA-Einstellungen 300
  - Hardware 6
  - Hardware ändern 72
  - Hardware hinzufügen 80
  - in einer vApp zusammenfassen 327
  - Konfigurationsdatei .vmx 107
  - Liste der ~ im ESXi Server 128
  - MAC-Adresse 111
  - mehrere Monitore 75
  - Name 44
  - Optimierung 68, 448
  - Optionen 88
  - OS installieren 53
  - PCI-Gerät hinzufügen 87
  - Portgruppen 154
  - PVSCSI-Adapter 49
  - Ressourcenkontrolle 95
  - SCSI-Gerät hinzufügen 85
  - Startoptionen 92
  - Startverzögerung 92
  - USB-Anschlüsse 342
  - USB-Controller 83
  - verschieben, manuell 211
  - Version 44
  - wiederherstellen 410
- Virtuelle Switches
  - Portabsicherung 422
- Virtueller Prozessor 4
- Virtueller Switch 144
- virtuelles Netzwerk 145
- Vizioncore 417
- VLAN (Virtual Local Area Network) 146, 150
- Vlance 84
- VLAN-Hopping 421
- vLockstep 294
- VM
  - Auslagerungsdatei 122
  - Backup 396
  - Betriebssystem anpassen 372
  - Bootreihenfolge 54
  - Chipsatz 2
  - exportieren 56
  - Festplattengröße anpassen 349
  - Grafikkarte 60
  - Hardware-Upgrade 366
  - Hardwareupgrade 364
  - Jumbo-Frames 167

- Konvertierung 71
- Leistungsdiagramm 69
- Maximalwerte 258
- Netzkartenauswahl 49
- Optimierung 448
- Portgruppenauswahl 50
- Ressourcenkontrolle 95
- SCSI-Adaptertyp 50
- Überwachung 297, 300
- umbenennen 292
- VM starten/herunterfahren 121
- VMCI (Virtual Machine Communication Inter-  
face) 76
- VMDirectPath 87
- VMkernel
  - Dienste 149
  - Kommandozeilenbefehle 237
  - NetQueue 168
- VMkernel Netzwerk
  - Richtlinien 456
- VMkernel-Befehle
  - esxtop 237
  - vdf 237
  - vmkload\_mod 237
  - vm-support 238
- vmkernel-Datei 30
- vmkfstools 239
- VMM (Virtual Machine Monitor) 94, 440
- vmmemctl.exe 442
- VM-Neustartpriorität 296, 300
- vMotion 292
  - Probleme 456
- vMotion Metro 120
- VMsafe 119, 122, 428
- VM-Speicherprofil 446
- vmsyslogd 285
- VM-Überwachung 300
- VMware
  - ACE 9
  - Converter 345
  - Data Recovery 397
  - Firma 8
  - Fusion 9
  - High Availability (HA) 457
  - Hochverfügbarkeit 291
  - Kommunikations-Interface 76
  - Player 8
  - Remote-Console 339
  - ThinApp 9
  - Thinstall 9
  - VDI 9
  - View 9
  - Virtual Desktop Infrastructure 9
  - vMotion 292
  - WebAccess 332
  - Workstation 8
- VMware Essentials 15
- VMware Essentials Kit 16
- VMware Kernel
  - konfigurieren 228
- VMware Remote-Console 334
- VMware Tools
  - anpassen 61
  - automatisches Upgrade 65
  - Dienste 61
  - Einschränkungen 56
  - Geräte 63
  - Hardwarebeschleunigung 60
  - Info 65
  - Installation 55
  - Massen-Upgrades 65
  - Optionen 63
  - Skripte 63, 89
  - unbeaufsichtigte Installation 66
  - Verkleinern 65
- VMware vApp 327
- vmware-cmd 238
- vmware-vmrc.exe 339
- vmx-Datei 107
- vmxnet 84
- vmxnet 2 84
- vmxnet 3 85
- vNetwork-Standard-Switche 153
- vobd-Datei 30
- Volumenschattenkopien 398
- vpaa-Datei 30
- vpxuser 255, 430
- vRAM 282
  - Lizenzierungsart 282
- VSA 322
  - Einschränkungen 323
  - Voraussetzungen 323
- VSA Cluster Service 324
- VSA Installer 325
- VSA Installieren 324
- VSA Instanz 324
- VSA Manager 325
- VSA Ports 324
- VSA-StorageCluster 322
- vServices 331

- vShield-Zonen 120
- vSphere 11
  - Enterprise-Edition 15
  - Enterprise-Edition AK 16
  - Komponenten 11
  - Netzwerkkonzept 145
  - Standard-Edition 15, 16
- vSphere Auto Deploy 321
- vSphere Client
  - Einstellungen 37
  - Hardwareanforderungen 34
  - Installation 34
  - Konfiguration 36
  - Parameter 36
  - Softwareanforderungen 34
  - Update 361
  - Update Manager 352
  - updaten 358
  - VMs optimieren 69
- vSphere Storage Appliance 322
- vSphere Upgrade 358
- vSphere View Accelerator 120
- vSphere5
  - Acceleration Kits 16
  - Bündels 15
  - Editionen 15
  - Kernkomponenten 257
  - Maximalwerte 257
  - Sicherheit 419
- vStorage-APIs 119, 397, 447
- vSwitch 144, 153
- vSwitche optimieren 166
- VT-d 87

## W

- Wake-On-LAN (WOL) 308
- Wartungsmodus 127

- Web Client 273
- WebAccess 332
  - ESXi-Server 340
  - Fehlerbehebung 339
  - Tastenkombination 338
  - Zugriffsrechte 338
- Webverknüpfung 338
- Wichtige Dateien
  - .vmdk 106
  - .vmx und .vmxf 106
  - /etc/inittab 245
  - /etc/nsswitch.conf 226
  - /etc/ntp.conf 246
  - /etc/resolv.conf 226
  - /etc/vmsyslog.conf.d/vpxa.conf 228, 229
  - /etc/vmware/esx.conf 228
  - /etc/vmware/firewall/service.xml 230
  - /etc/vmware/vpxa 229
  - /var/log/ 245
  - /var/log/vpxa.log 228
  - flat.vmdk 106
  - service.xml 435
- WinSCP 29
- Wirt
  - Definition 1
- WOL 308

## Z

- Zeitsynchronisierung 61, 62, 455
- ZFS 181
- Zufallsdatenblock-Angriffe 422
- Zugangskontrolle 458
- Zugangssteuerung 291, 295
- Zugangssteuerungsrichtlinie 295
- Zugriffsrechte
  - WebAccess 338
- Zuteilung von Systemressourcen 124



# Über den Autor

**Ralph Göpel** ist Diplominformatiker, Microsoft Certified System Engineer und VMware Certified Professional. Er gibt Unterricht in den verschiedensten IT-Bereichen und Themen. Seit ca. sieben Jahren arbeitet er insbesondere als Consultant und Dozent mit den Produkten von VMware, seit Mitte 2011 unterrichtet er die neue Version von VMware vSphere 5. Er unterstützt seine Kunden bei der Implementierung, macht Troubleshooting und übernimmt die Betreuung von Upgrades. In seiner Freizeit fährt er liebend gerne Motorrad und joggt.

# Kolophon

Die auf dem Cover dieses Buchs dargestellte *Stephalia Corona* gehört zu den Staatsqualen (Siphonophoren), einer Ordnung der Nesseltiere. Sie werden Staatsqualen genannt, weil sie freischwebende oder schwimmende Kolonien bilden, deren Einzeltiere polymorph und hochspezialisiert sind. Man findet sie vor allem im westlichen Südpazifik in unterschiedlicher Tiefe.

Das Coverlayout der deutschen Ausgabe wurde von Hanna Dyer und Bret Kerr mit Quark XPress 4.1 unter Verwendung der Schriftart ITC Garamond von Adobe erstellt. Als Textschrift verwenden wir die Linotype Birka, die Überschriftenschrift ist die Adobe Myriad Condensed und die Nichtproportionalschrift für Codes ist LucasFont's TheSans Mono Condensed. Die in diesem Buch enthaltenen Abbildungen stammen vom Autor und von Michael Oreal, der dafür Adobe Photoshop CS und Macromedia FreeHand MX verwendet hat.

