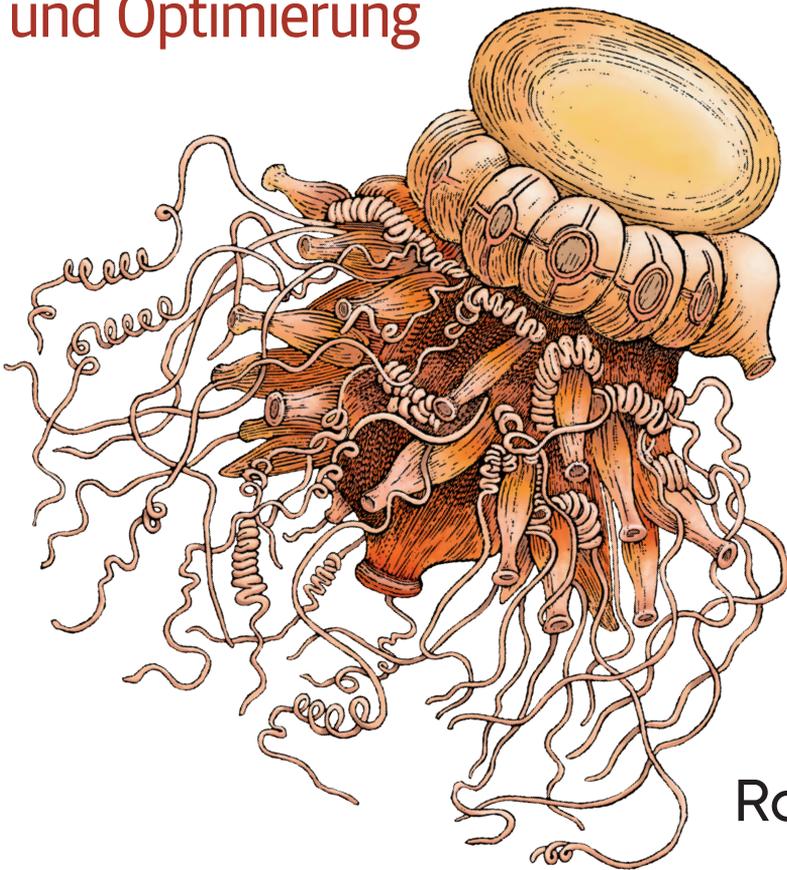


O'REILLY®

5.  
aktualisierte  
Auflage

# Praxishandbuch VMware vSphere 7

Leitfaden für Installation, Konfiguration  
und Optimierung



Ralph Göpel

Papier  
plus<sup>+</sup>  
PDF.

Zu diesem Buch – sowie zu vielen weiteren O'Reilly-Büchern – können Sie auch das entsprechende E-Book im PDF-Format herunterladen. Werden Sie dazu einfach Mitglied bei oreilly.plus<sup>+</sup>:

[www.oreilly.plus](http://www.oreilly.plus)

5., aktualisierte Auflage

---

# Praxishandbuch VMware vSphere 7

*Leitfaden für Installation, Konfiguration und Optimierung*

*Ralph Göpel*

**O'REILLY®**

Ralph Göpel

Lektorat: Dr. Michael Barabas

Projektkoordinierung: Anja Weimer

Copy-Editing: Ursula Zimpfer, Herrenberg

Satz: Gerhard Alfes, mediaService, Siegen, [www.mediaservice.tv](http://www.mediaservice.tv)

Herstellung: Stefanie Weidner

Umschlaggestaltung: Karen Montgomery, Michael Oréal, [www.oreal.de](http://www.oreal.de)

Druck und Bindung: mediaprint solutions GmbH, 33100 Paderborn

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.

ISBN:

Print 978-3-96009-167-7

PDF 978-3-96010-483-4

ePub 978-3-96010-484-1

mobi 978-3-96010-485-8

Dieses Buch erscheint in Kooperation mit O'Reilly Media, Inc. unter dem Imprint »O'REILLY«. O'REILLY ist ein Markenzeichen und eine eingetragene Marke von O'Reilly Media, Inc. und wird mit Einwilligung des Eigentümers verwendet.

*Hinweis:*

Dieses Buch wurde auf PEFC-zertifiziertem Papier aus nachhaltiger Waldwirtschaft gedruckt. Der Umwelt zuliebe verzichten wir zusätzlich auf die Einschweißfolie.



5., aktualisierte Auflage

Copyright © 2021 dpunkt.verlag GmbH

Wieblinger Weg 17

69123 Heidelberg

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Es wird darauf hingewiesen, dass die im Buch verwendeten Soft- und Hardware-Bezeichnungen sowie Markennamen und Produktbezeichnungen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

Alle Angaben und Programme in diesem Buch wurden mit größter Sorgfalt kontrolliert. Weder Autor noch Verlag können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

5 4 3 2 1 0

<b>1</b>	<b>Einführung</b> .....	<b>1</b>
	Virtualisierung im Allgemeinen .....	1
	Die Technik virtueller Maschinen .....	3
	Hardwareausstattung .....	7
	Virtualisierung mit VMware .....	8
<b>2</b>	<b>Die Bestandteile von vSphere</b> .....	<b>11</b>
	Komponenten der vSphere-Umgebung .....	11
	Die Editionen im Vergleich .....	14
<b>3</b>	<b>Der Hypervisor</b> .....	<b>19</b>
	Embedded oder Installable .....	19
	ESXi-Hardwareanforderungen .....	21
	ESXi-Hardwareempfehlungen .....	22
	ESXi interaktiv installieren .....	23
	Alternative Installationsmöglichkeiten .....	32
	Den ersten ESXi-Host verwalten .....	35
	Den Host-Client konfigurieren .....	36
	Weitere Konfigurationen des Hosts .....	40
	Hardwareeinstellungen des ESXi-Servers .....	40
	Verwalten – System – Erweiterte Einstellungen .....	43
	Das Kontextmenü unter ESXi .....	61
	VMware Remote Console (VMRC) .....	65
<b>4</b>	<b>Der vCenter Server</b> .....	<b>69</b>
	Funktionen des vCenter Servers .....	70
	Die technischen Voraussetzungen für einen vCenter Server .....	78
	Den vCenter Server installieren .....	82
	vCenter Server-Lizenzen .....	93
	Logdateien des vCenter Servers .....	96

<b>5</b>	<b>Die virtuelle Maschine</b> .....	<b>103</b>
	Eine virtuelle Maschine erstellen .....	103
	Betriebssystem installieren .....	115
	VMware Tools installieren .....	117
	Virtuelle Maschinen optimieren .....	130
	Gasthardware ändern .....	134
	Gasthardware hinzufügen .....	151
	Optionen der virtuellen Maschine .....	156
	Ressourcenkontrolle der VM .....	163
	BIOS-Einstellungen der virtuellen Maschine .....	168
	EFI-Einstellungen der virtuellen Maschine .....	171
	Dateien der virtuellen Maschine .....	172
	VMs umbenennen .....	181
	Die MAC-Adresse der VM .....	183
<b>6</b>	<b>Netzwerkconfiguration</b> .....	<b>185</b>
	Netzwerkkonzepte .....	185
	Internet Protocol Version 6 .....	189
	Netzwerkdienste .....	191
	VLAN .....	192
	vNetwork-Standardswitch .....	196
	Netzwerkconfiguration des VMkernels .....	199
	Konfiguration von Management Network .....	202
	vSwitches optimieren .....	212
	Empfehlungen zu Netzwerkoptimierungen .....	215
	Fehlerbehebung auf der Konsole .....	217
<b>7</b>	<b>Storage-Konfiguration</b> .....	<b>229</b>
	Allgemeine Richtlinien .....	229
	iSCSI-Speicher anschließen .....	231
	NFS v3-Speicher anschließen .....	246
	NFS v4.1-Speicher anschließen .....	247
	Fibre-Channel-Storage .....	250
	Storage Alignment .....	251
	Gegenüberstellung: NFS, iSCSI und Fibre Channel .....	253
<b>8</b>	<b>Snapshots</b> .....	<b>269</b>
	Was ist ein Snapshot? .....	269
	Einen Snapshot erstellen .....	271
	Den Snapshot-Manager verwenden .....	274

<b>9</b>	<b>Arbeiten auf der Kommandozeile</b> .....	<b>283</b>
	Dienste und Konfigurationsdateien .....	286
	Updates und Patches manuell einspielen .....	291
	Die Kommandozeile, wichtige Dateien und Befehle .....	293
	Skripte .....	305
	Weitere Tools .....	308
	Eigene Skripte schreiben .....	312
	PowerCLI .....	315
	Beispielbefehle für virtuelle Maschinen .....	319
	Allgemeines zu Skripten .....	326
<b>10</b>	<b>Ein Cluster erstellen</b> .....	<b>335</b>
	Wie funktioniert HA? .....	336
	Wie funktioniert vMotion? .....	336
	Wie funktioniert DRS? .....	337
	Wie funktioniert DPM? .....	338
	Wie funktioniert FT? .....	339
	Wie funktioniert EVC? .....	339
	Clusterkonfiguration für vSphere HA .....	339
	Hostisolierungsreaktion richtig einstellen .....	344
	VM-Komponentenschutz .....	347
	VM-Außerkräftsetzungen .....	349
	Clusterkonfiguration für DRS .....	350
	Cluster-Zusammenfassung .....	359
	DPM einrichten .....	360
	Fault Tolerance einrichten .....	361
	Fehlertoleranz einschalten .....	364
	Cluster-Registerkarten .....	366
<b>11</b>	<b>vSphere Client und Fernzugriff auf virtuelle Maschinen</b> .....	<b>369</b>
	vSphere Client .....	369
	Fernzugriff auf VMs .....	373
<b>12</b>	<b>VMware Distributed Switches und vApp</b> .....	<b>381</b>
	vSphere Distributed vSwitch .....	381
	VMware vApp .....	386
<b>13</b>	<b>vVol, vSAN und Hostprofile</b> .....	<b>393</b>
	Hostprofil erstellen .....	393
	vSphere Auto Deploy .....	399
	vCenter High Availability .....	400
	Virtuelle Volumes und vSAN .....	403

<b>14 VMware Lifecycle Manager, Upgrade und Converter</b> .....	<b>409</b>
Konsolidieren .....	409
Lifecycle Manager .....	416
Einen Host über Baselines updaten .....	421
Ein Cluster über Image updaten .....	423
Upgrade der Umgebung .....	425
<b>15 Templates (Vorlagen für virtuelle Maschinen)</b> .....	<b>437</b>
Templates und ihr Nutzen .....	437
<b>16 vCenter Server-Konfiguration und Alarmer</b> .....	<b>447</b>
Einstellungen des vCenter Servers .....	447
Alarmer .....	453
<b>17 Datensicherung und -wiederherstellung</b> .....	<b>461</b>
Backup-Unterschiede zwischen den Welten .....	461
Sicherung des Hosts .....	462
Sicherung der VMs .....	463
Veeam Software .....	463
Erstkonfiguration der Umgebung .....	467
Backup-Jobs erstellen .....	471
Planen eines Replikationsjobs .....	480
Wiederherstellung einer VM .....	481
Arbeiten mit Veeam Explorer .....	486
<b>18 Sicherheit in der virtuellen Umgebung</b> .....	<b>493</b>
VMwares Architektur der Sicherheitsfeatures .....	493
Portabsicherung virtueller Switches .....	497
Benutzerkennwortbeschränkungen .....	499
Berechtigungen und Rollen .....	500
Sicherheit bei der VM .....	504
Allgemeine Sicherheitsempfehlungen .....	507
Firewall-Konfiguration im vCenter Server .....	510
<b>19 Ressourcen, Optimierung und Troubleshooting</b> .....	<b>519</b>
Ressourcenverwaltung .....	519
Virtueller Speicher der VMs .....	522
Ressourcenpools für VM-Gruppen .....	526
VM-Speicherprofil und Storage DRS .....	529
Optimierung von VMs .....	531

Performance überwachen .....	537
vSphere-7-Troubleshooting .....	543
An HA beteiligte Komponenten .....	550
Weitere Tools .....	556
<b>Index .....</b>	<b>561</b>



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 mit dem VMware-Produkt vSphere 7.0 los.

## 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. Eine solche Konstellation nennt man *Virtualisierung*. Den Computer, auf dem die Software installiert wird, nennt man *Host* oder *Wirt*, 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 bei Belieben anschließend wiederherstellen.

Ein Computer, auf dem beliebig viele unterschiedliche Betriebssysteme gleichzeitig laufen können, also unabhängige und verschiedene Rechner in Fenstern, ist der Traum jedes Entwicklers, Supporters oder auch versuchsfreudigen Anwenders. Programme von VMware, Microsoft, XEN, KVM 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 Gastsys-

teme). Eine VM verfügt wie jeder echte PC über die üblichen Hardwarekomponenten wie 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 dieser 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 dieser meist 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 oder Hypervisoren sind auch andere Betriebssysteme verwendbar, z. B. DOS, Novell, Unix, OS/2 oder Mac OS X.

## Warum virtualisieren?

Viele spezielle Anwendungen, gerade auf Serverbetriebssystemen, erfordern einen eigenständigen Rechner. Nur so verspricht der Hersteller einen reibungslosen Einsatz. Gerade bei 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 bei der Energieversorgung, der Hardware und Wartung sowie dem Platzbedarf für neue Server 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 ein 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, ein neuer Releasestand oder auch ein Servicepack für das Betriebssystem. Funktioniert alles bestens, kann dieser Zustand getrost übernommen werden. Geht etwas daneben oder funktioniert es nicht wie gewünscht, so kann jederzeit zu einem vorherigen Stand (Snapshot) 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 portiert werden. In einer virtuellen Maschine ist das kein Problem.

## Wann nicht virtualisieren?

Einzigste Ausnahme bei den installierbaren Betriebssystemen sind wohl Echtzeitsysteme wie QNX, RTOS und VXworks, bei denen es auch keinen Sinn macht, diese virtuell laufen zu lassen. Zeitgenaue Abfolgen bei Betriebssystemen oder Anwendungen sollten nicht virtuell laufen – dafür ist das Laufzeitverhalten der VM nicht genau genug. Ein ESXi-Server (Host) macht keine abrupten Zeitänderungen, sondern dehnt Sekunden aus oder verkürzt sie, um die richtige Zeit irgendwann zu erreichen – auch das wäre für Echtzeitanwendungen sehr schädlich. Auch bei manchen Linux-Systemen, gerade mit spezieller Software, ist von der Virtualisierung grundsätzlich abzuraten.

Außerdem wird nur eine Standardhardware zur Verfügung gestellt, sodass spezielle Komponenten wie Steuerungssysteme oder spezielle Bus-Karten usw. leider nicht emuliert werden können. Gängige PCI- und PCIe-Adapter wie z.B. ISDN-Karten können aber – zumindest unter ESXi auf einigen Plattformen – an die VMs durchgereicht werden (PCI-Passthrough bzw. DirectPath-I/O-Konfiguration).

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-, 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 Betriebs- und Dateisystem unabhängige Laufzeitumgebung, in der sich gegebenenfalls 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:

- Prozessor
- (A)PIC ((Advanced) Programmable Interrupt Controller)

- DMA (Direct Memory Access)
- IDE- oder SATA-Controller, gegebenenfalls 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- und Host-Bus 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:

- 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 Rechners. 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 primäres 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 RVI bzw. Intel VT-x und lässt sich im BIOS des Servers aktivieren.

Die AMD- und Intel-Architektur der 32- und 64-Bit-CPU's bietet vier verschiedene Privilegien an, mit denen dem Betriebssystem, Treibern und Programmen unterschiedliche Rechte zugewiesen werden können, was Sie in der Abbildung 1-1 se-

hen können. Normalerweise laufen OS (Operating System, Betriebssystem) 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.

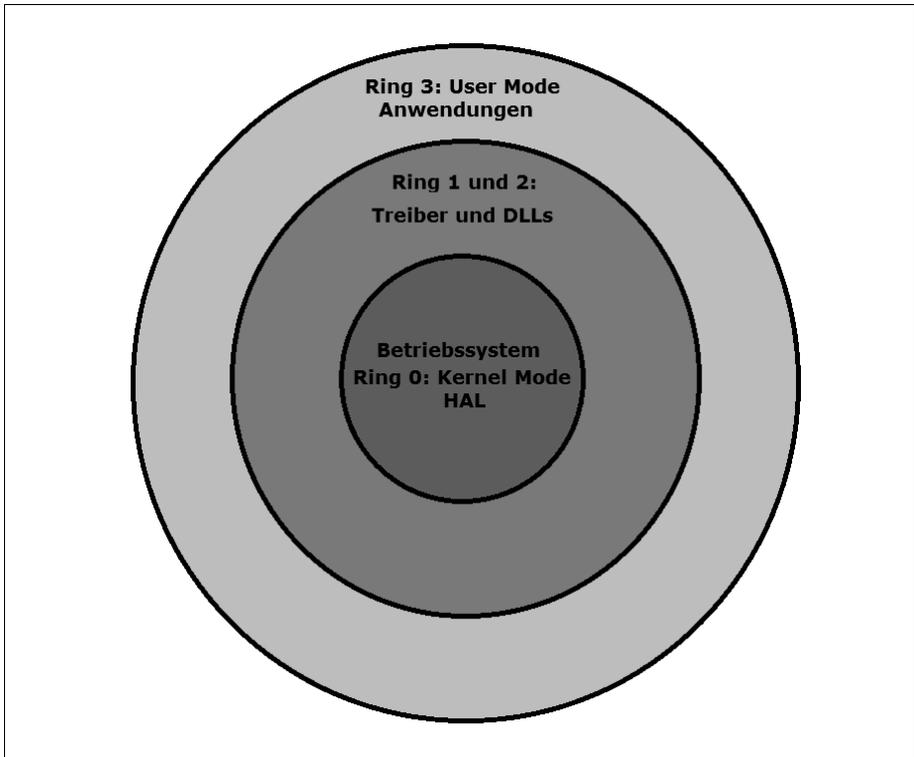


Abbildung 1-1: Die Ring-Modi eines Betriebssystems

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 Descriptor 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. Der x86 behandelt die LGDT-Anweisung (Load Global Descriptor Table) auch als

privilegiert. Allerdings führt SGDT (Store Global Descriptor Table) 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 beispielsweise 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 hierbei 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 (Logical Unit Number) im SAN (Storage Area Network), und Direct Passthrough, z. B. bei Netzwerkkarten. Dazu erfahren Sie später ebenfalls mehr.

Meistens wird die virtuelle Festplatte mit einer Datei auf dem Hostbetriebssystem realisiert. Die Virtualisierungssoftware 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 immer in einem definierten Zustand starten und kritische Tests ausführen. Beim nächsten Start befindet sich die VM wieder im Originalzustand.

Als virtuelles CD-/DVD-ROM-Laufwerk kommen meist ISO-Images zum Einsatz, die als Datei auf der lokalen Platte des Hosts, einer Freigabe im Netzwerk oder einem angeschlossenen NAS (Network Attached Storage) oder SAN (Storage Area Network) liegen. Das Betriebssystem in der VM erkennt diese als »echte« optische Medien, wobei die Zugriffe und Übertragungsraten dort erheblich höher als bei realen Laufwerken sind.

# Hardwareausstattung

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

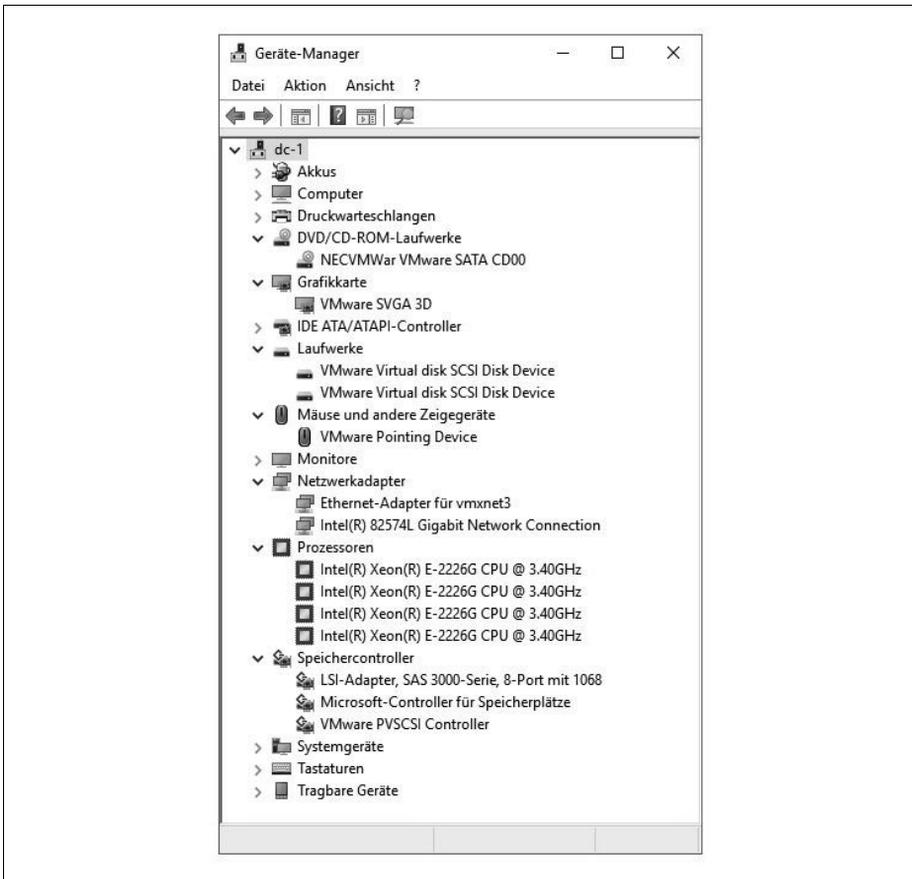


Abbildung 1-2: Gerätemanager unter Windows Server in der VM

Zu den notwendigen Komponenten der VM gehören unter anderem der Chipsatz des Motherboards (z.B. Intel 440BX), BIOS (AMI oder Phoenix) oder EFI, Festplatte sowie Grafik-, Sound- und Netzwerkkarte. Während Motherboard und Festplatte meistens mit den generischen Treibern der Betriebssysteme laufen, muss für die Gra-

fikkarte ein angepasster Treiber installiert werden. VMware übergibt zum Beispiel der VM eine spezielle SVGA-II- oder sogar 3D-Karte, Microsoft bevorzugt hier meist eine Trio 32/64. In den VMware Tools enthaltene Treiber sollten für den korrekten Zugriff nach der Installation des Betriebssystems noch installiert werden.

Als Netzwerkkarte wird bei VMware unter anderem eine AMD-PCnet-PCI-II- oder Intel-LAN-Pro-Karte (PCI oder PCIe), 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 LSI Logic, für die 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. 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 -3.1-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 ist die Rede, 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 einen Tag über 19 Milliarden US-Dollar Gewinn. Mittlerweile gehört EMC und damit auch die Tochterfirma VMware zu Dell.

## VMware-Produkte

Als erstes Produkt brachte VMware die WORKSTATION heraus, die heute immer noch das bekannteste Produkt ist und mittlerweile in der Version 15 vorliegt. Das Produkt heißt mittlerweile »VMware Workstation Pro«. Diese Applikation wird auf einem bestehenden Betriebssystem (Windows oder Linux) installiert. Ähnlich verhielt es sich mit dem kostenlosen Nachfolger des ehemaligen GSX-Servers, dem VMware SERVER, der aber nicht weiterentwickelt wird. 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 10 oder einen Server handelt.

Weiterhin gibt es für den nicht kommerziellen Gebrauch den kostenlosen VMware PLAYER, der eigentlich nur vorhandene virtuelle Maschinen abspielen konnte. Seit der Version 3.0 ist man aber damit ebenfalls in der Lage, neue VMs zu generieren, aktuell liegt er in der Version 15 vor und nennt sich »VMware Workstation Player«. Der Player läuft unter 32-Bit-Betriebssystemen nur allein, unter 64 Bit auch mit Server oder Workstation zusammen, wobei es dann auf die Installationsreihenfolge und die Versionen der beiden Anwendungen ankommt. Da die Konfigurationsmöglichkeiten hier eingeschränkter sind als beispielsweise bei VMware Workstation Pro, aber die Anwendung deutlich kleiner ist und weniger Ressourcen verbraucht, ist der Player durchaus dazu geeignet, als Ersatz für Workstation mit wenigen 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 dieses die einzige lauffähige Möglichkeit von VMware, denn weder Workstation und Server noch der Player können hier installiert werden. Fusion gibt es auch als Pro-Version, die deutlich mehr Funktionen mitbringt.

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

Als Desktop- und Anwendungs-Virtualisierungslösung gibt es bei VMware HORIZON (ehemals View), HORIZON CLOUD, HORIZON APPS und HORIZON FLEX jeweils in der Version 8. Die Namensgebung bei der Vorgängerversion, Virtual Desktop Infrastructure (VDI), war da schon aussagekräftiger. Der Sinn dieser Software ist es, komplette Arbeitsplatzrechner auf Hosts zur Verfügung zu stellen und nicht mehr 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. Bei HORIZON CLOUD (ehemals AIR DESKTOPS) liegt der Schwerpunkt auf VMware vCloud, wohingegen HORIZON FLEX eher die Unterstützung für Macs und Windows bietet.

Will man ähnlich wie bei virtuellen Maschinen nur eine Applikation zur Verfügung stellen, so 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 (Microsoft Software Installation) oder eine EXE-Datei zu packen und dann auf einem Server, dem Netzwerk oder einem USB-Stick teilweise ohne Installation zur Verfügung zu stellen.

VMware vSphere with Kubernetes (auch vSphere Integrated Container, VIC) ist das neue Highlight bei der aktuellen Version. Damit können Container statt ganzer VMs zur Verfügung gestellt werden. Somit muss nicht mehr für jede Applikation eine eigene VM bereitgestellt werden, sondern nur eine isolierte Umgebung innerhalb des Betriebssystems der VM – der Container.

Für mittelständische bis große Unternehmen war Virtual Infrastructure gedacht, das jetzt vSphere 7.0 heißt. Der große Unterschied zu den oben genannten Lösungen ist das Zusammenfassen von mehreren Servern zu einer Ressource, die Verwaltung von mehreren Virtualisierungsservern und virtuellen Maschinen von einem Rechner aus, die Ausfallsicherheit und viele weitere 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 vSphere. Viele Funktionen, die bei diesem System seit einigen Jahren verfügbar sind, werden bisher nicht von anderen Herstellern angeboten. Einen Vergleich braucht VMware bezüglich Funktionen, Sicherheit, Skalierbarkeit, Zuverlässigkeit etc. nicht zu scheuen. Auch die neue Version von Microsoft »Hyper-V« ist gegenüber vSphere in einigen Details noch eingeschränkt.

Häufig wird mir in Gesprächen gesagt, dass Hyper-V von Microsoft kostenlos ist. Der alleinstehende ESXi-Host ist ebenfalls kostenlos, erst wenn man einen vCenter Server einsetzen will und ein Datacenter braucht, muss man Lizenzen kaufen, und das ist bei dem Microsoft-Produkt genauso.

# Die Bestandteile von vSphere

In diesem Kapitel erhalten Sie einen groben Überblick über die einzelnen Bestandteile einer vSphere-7-Umgebung sowie ihrer Begrifflichkeiten und Funktionen. Außerdem 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 vSphere 7« besteht aus mehreren Komponenten, die z. T. unabhängig voneinander sind wie z.B. ein Betriebssystem und eine Anwendung. Mit einer Anwendung alleine 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 VMware vSphere: Es ist ein erweiterbares Paket mit Einzelteilen, die in einigen Fällen nur Sinn machen, 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 nur sehr bedingt eine virtuelle Maschine erstellen oder verwalten, dafür benötigt man eine weitere Anwendung, die z.B. auf einem Client installiert wird. Das ist dann der vSphere oder HTML5-Client. In Abbildung 2-1 sehen Sie, wie ein Client-PC auf den Host zugreift.

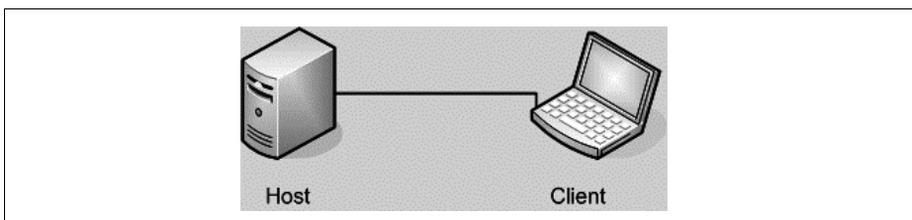


Abbildung 2-1: Hostzugriff über einen Client

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 Browsersitzung auch mehrfach starten kann, besteht die Möglichkeit, auch mehrere unabhängige Hosts gleichzeitig zu verwalten, wie in Abbildung 2-2 dargestellt. 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.

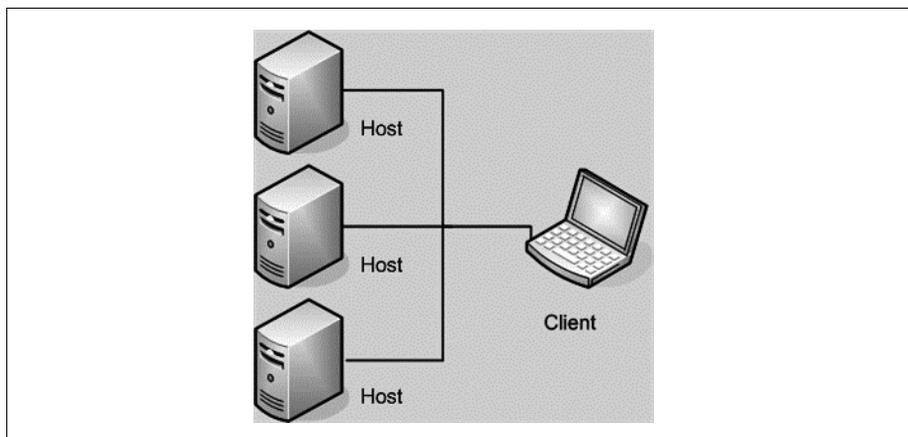


Abbildung 2-2: vSphere Client greift auf drei Hosts zu.

Ist einer unserer 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, so 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. 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.

Ein vCenter Server ist eine Anwendung, die als Dienst im Hintergrund läuft und über eine fertige Linux-VM (sogenannte Appliance), die man bei VMware herunterladen kann, zur Verfügung gestellt wird. Der Benutzer kann wie vorher mit dem Browser arbeiten und verbindet sich jetzt mit dem Management-Server. Nun bekommt er ein Fenster, in dem alle ESXi-Hosts und alle virtuellen Maschinen aufgelistet sind. Seit der Version vSphere 7.0 ist dies eine fertige virtuelle Maschine, die auf der Basis von Photon Linux die Aufgaben vom Windows vCenter Server voll-

ständig übernommen hat. Die Linux-Distribution Photon stammt direkt von VMware. Eine Anwendung, die unter Windows installiert werden kann, steht nicht mehr zur Verfügung.

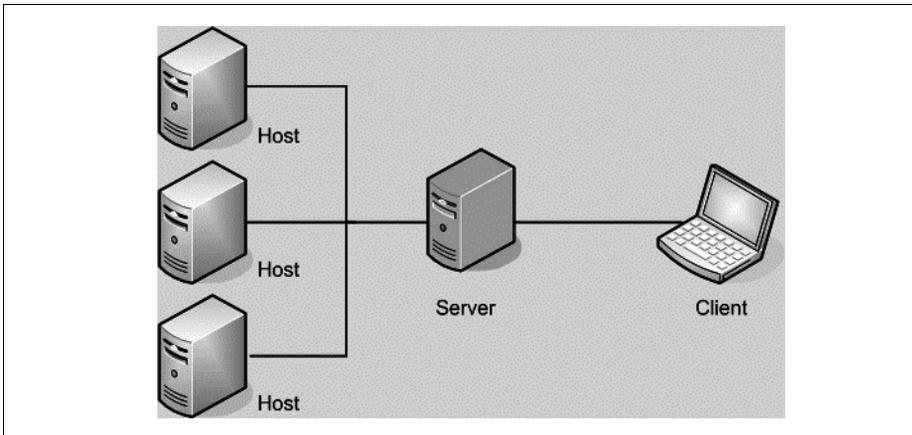


Abbildung 2-3: Zugriff des Clients über den vCenter Server

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 (High Availability, HA), 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.

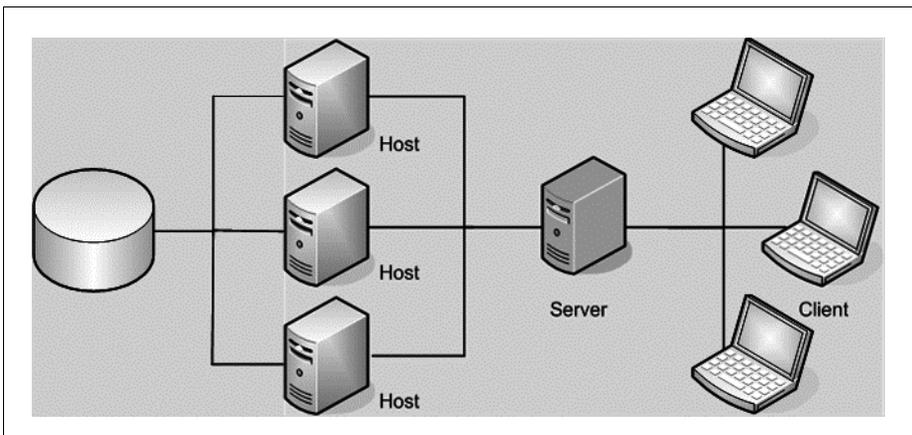


Abbildung 2-4: vSphere-7-Umgebung mit SAN oder NAS

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

## VMware Cloud-Betriebssystem

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 aus zugegriffen wird (wie auf die Internetseite mit dem 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.
- Welcher Host Arbeitsspeicher und CPU-Leistung zur Verfügung stellt, spielt keine Rolle.
- Wo sich der Festplattenplatz befindet, kann ebenfalls egal sein.

Deshalb nennt VMware vSphere 7 ein *Cloud-Computing-Betriebssystem*. Streng genommen handelt es sich hierbei um eine Private Cloud.

## Die Editionen im Vergleich

VMware bietet die Komponenten von vSphere 7 in verschiedenen Bundles und den kostenlosen ESXi-Server auch allein an. Je nach Version sind einige der in diesem Buch beschriebenen Funktionen enthalten. Die nachfolgende Tabelle zeigt einen Ausschnitt des aktuellen Angebots.

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

	Standard	Enterprise Plus	vSphere EP mit Operations Management
Übersicht	Serverkonsolidierung und Business Continuity	Ressourcenmanagement, verbesserte Verfügbarkeit und Performance von Anwendungen	Ressourcenmanagement, verbesserte Verfügbarkeit und Performance von Anwendungen
Produktkomponenten			
Lizenzberechtigung	Pro CPU	Pro CPU	Pro CPU
Kompatibilität für zentrales Management			
vCenter Server (separat erhältlich)	vCenter Server Standard	vCenter Server Standard	vCenter Server Standard
Cloud-API-Integration			
VMware Integrated OpenStack			Support für VMware Integrated OpenStack ist separat erhältlich.

→

Tabelle 2-1: VMware vSphere-Editionen mit zugehörigen Funktionen (Forts.)

	Standard	Enterprise Plus	vSphere EP mit Operations Management
<b>Business Continuity und Sicherheit</b>			
vMotion	ja (+ Cross vSwitch)	ja (+ Cross vSwitch)	ja (+ Cross vSwitch/Cross vCenter/Long Distance)
Storage vMotion	ja	ja	ja
High Availability	ja	ja	ja
Data Protection	ja	ja	ja
Fault Tolerance	4 vCPUs	8 vCPUs	8 vCPUs
vShield Endpoint	ja	ja	ja
vSphere Replication	ja	ja	ja
Hot Add	ja	ja	ja
<b>Priorisierung von Ressourcen und verbesserte Performance von Anwendungen</b>			
Virtual Volumes	ja	ja	ja
Storage Policy-Based Management	ja	ja	ja
Reliable Memory		ja	ja
Big Data Extensions		ja	ja
Virtual Serial Port Concentrator		ja	ja
Distributed Resources Scheduler (DRS), Distributed Power Management (DPM)		ja	ja
Storage DRS			ja
Storage I/O Control			ja
Network I/O Control			ja
Unterstützung von Single Root I/O Virtualization (SR-IOV)			ja
Flash Read Cache			ja
NVIDIA GRID vGPU			ja
<b>Automatisierte Administration und Bereitstellung</b>			
Content-Bibliothek	ja	ja	ja (+ Vorlagenbereitstellung)
Storage APIs for Array Integration, Multipathing		ja	ja
Distributed Switch			ja
Host Profiles und Auto Deploy			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 Gruppen von Unternehmen preiswertere Angebote, wie zum Beispiel für Akademien und Schulen.

Neu seit der Version 6 sind zwei Lizenzmodelle, bei denen die Anzahl der VMs (bis maximal 25) begrenzt ist und die sich offiziell vSphere Remote Office Branch Office Editions nennen. Deren Funktionen sind in der nachfolgenden Tabelle gelistet.

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

	<b>vSphere Remote Office Branch Office Standard</b>	<b>vSphere Remote Office Branch Office Advanced</b>
Übersicht	Servervirtualisierungsplattform für Remote-Standorte mit Funktionen für Business Continuity und Backup	Servervirtualisierungslösung für Remote-Standorte mit Funktionen für Business Continuity und Backup sowie die Standardisierung von Hostkonfigurationen
Produktkomponenten		
Lizenzberechtigung	Paket mit 25 virtuellen Maschinen	Paket mit 25 virtuellen Maschinen
Zentrale Managementfunktion		
vCenter Server (separat erhältlich)	vCenter Server Standard	vCenter Server Standard
Business Continuity und Sicherheit		
vMotion	ja	ja
Storage vMotion	ja	ja
High Availability	ja	ja
Data Protection	ja	ja
Fault Tolerance	2 vCPUs	4 vCPUs
vShield Endpoint	ja	ja
vSphere Replication	ja	ja
Hot Add	ja	ja
Standardisierung und Compliance		
Host Profiles und Auto Deploy		ja
Distributed Switch		ja

Häufig werden auch vSphere Essentials Kits angeboten. Diese gibt es dann üblicherweise in zwei verschiedenen Ausbaustufen, wie die nachstehende Tabelle 2-3 zeigt:

Tabelle 2-3: VMware vSphere Essentials Kits mit zugehörigen Funktionen

	Essentials Kit	Essentials Plus Kit
Übersicht	Servervirtualisierung und -konsolidierung mit zentralem Management	Servervirtualisierung und -konsolidierung mit Business Continuity
Zentrales Management	vCenter Server Essentials	vCenter Server Essentials
Lizenzberechtigung	3 Server mit jeweils bis zu 2 Prozessoren	3 Server mit jeweils bis zu 2 Prozessoren
Funktionen	vSphere Hypervisor	vSphere Hypervisor, vMotion, High Availability, vShield Endpoint, vSphere Replication

## Kostenloser ESXi-Server

Einen alleinstehenden Host, der einige virtuelle Maschinen laufen lassen kann, erhält man bei VMware kostenlos. Diese Version ist allerdings gegenüber der lizenzierten deutlich eingeschränkt. So ist es nicht möglich, per Skripte (siehe Kapitel 9) etwas zu automatisieren oder diesen Host über einen vCenter Server zu managen. Hardwareseitig gibt es kaum Einschränkungen:

- Unbegrenzte Anzahl an Kernen pro Prozessor
- Unbegrenzte Anzahl an Prozessorsockeln
- VMs können maximal acht vCPUs bekommen.
- Alle Betriebssysteme werden wie in der Vollversion unterstützt.

Weitere Einschränkungen gibt es nicht.

## Lizenz-Resümee

Eine Faustregel, für welche Umgebung welche Edition sinnvoll oder angebracht ist, lässt sich nicht ableiten. 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 Einschränkungen in Kapitel 10 und die dort angegebenen unterstützten Betriebssysteme ansehen, wird schnell deutlich, dass man diese Ausfallsicherheit nur für wenige Maschinen nutzen wird. Das größte Manko war bisher, dass nur Einprozessormaschinen hierbei unterstützt wurden. Ab vSphere 6.7 sind es je nach Lizenz vier Kerne oder in der Enterprise-Plus-Variante acht Kerne. Die wichtigen Rechner, die möglichst immer zur Verfügung stehen sollen und von vielen Usern genutzt werden, haben häufig deutlich mehr CPUs nötig. Allerdings muss man gestehen, dass VMware die Einzigen sind, die das überhaupt anbieten.

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, benötigen Sie kein DRS. Wenn eine Trennung der LAN-Verbindung von maximal einer Sekunde nicht schlimm ist, brauchen Sie keinen Distributed vSwitch, usw.

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

---

# Der Hypervisor

Die erste Komponente, die man für eine vSphere-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 Red Hat-Linux-Betriebssystem (ESX) und eine Version ohne Betriebssystem (ESXi). Seit der Version 5.0 von vSphere gibt es nur noch den ESXi, der nunmehr auf der Internetseite von VMware generell als »Hypervisor« bezeichnet wird, aber auf fast allen Bildschirmen und Dokumentationen weiter als »ESXi« oder schlicht »Host« auftaucht.

Die physikalische Hardware des Hosts, auf der letztendlich die virtuelle Maschine später 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 oder noch zu beschaffender Komplettsysteme mit einzelnen Geräten überprüfen kann, und zwar unter:

<http://www.vmware.com/resources/compatibility/search.php>.

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 7.0 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), dazu erfahren Sie in Kapitel 10 mehr.

Der Begriff »ESX(i)« ist übrigens ein Name und keine Abkürzung, auch wenn im Internet teilweise etwas anderes behauptet wird, wie z. B. »Elastic Sky X (Integrated)«.

## Embedded oder Installable

Bei den Hypervisor-Versionen mit dem »i«, also *Embedded* oder *Installable*, gibt es keine Unterschiede mehr, lediglich in der Dokumentation von VMware und auf der grafischen Oberfläche tauchen diese beiden Begriffe auf.

Es ist zwar möglich, auf die Kommandozeile zu kommen und dort ein paar Befehle einzugeben, aber man wird wohl eher das *vSphere Remote Command Line Interface* (RCLI) oder PowerCLI als Erweiterung für die Windows Powershell dafür nutzen, das man sich bei Bedarf bei VMware herunterladen kann. 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. Es gibt auch fertige virtuelle Maschinen, sogenannte Appliances, die bereits das CLI lauffähig vorinstalliert haben. Auf beide CLI-Versionen gehe ich in Kapitel 9 näher ein.

Der ESXi ist ein sogenannter Bare-Metal-Hypervisor, der direkt auf der Serverhardware installiert wird bzw. bereits im Server – meist als USB-Stick oder (SD-)Speicherkarte – auf dem Motherboard steckt. Damit ist das Ressourcenmanagement für die virtuelle Maschine mit den vier Kernkomponenten (»Four-Core«: CPU, RAM, Storage und Netzwerk) rein als virtuelle Schicht anzusehen.



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

Der ESXi kann auch als kostenlose Version eingesetzt werden – beide Varianten (frei und nicht frei) haben übrigens die gleichen Hardwareanforderungen. 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 einem Datenträger (siehe unten) können dort ähnlich wie beim ehemaligen ESX-Server Befehle eingegeben werden. Dazu später mehr in Kapitel 9.

VMware bietet nur noch den ESXi als vSphere Hypervisor an und der Support der alten ESX- und ESXi-Versionen (bis 6.0) ist ausgelaufen, der Support für die Version 6.5 läuft nach fünf Jahren am 15.12.2021 und für 6.7 am 15.10.2022 aus.

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

- Die Konfiguration erfolgt am Server über eine Umgebung, die an ein BIOS erinnert (DCUI, Direct Console User Interface). Agenten können nur über einen CIM-Provider (Common Information Model) installiert werden. Die Konfiguration ist lediglich über die grafische Oberfläche oder das Remote CLI oder PowerCLI (Command Line Interface) möglich.
- Das Remote CLI kann auf einem Linux- oder Windows-PC oder als virtuelle Maschine installiert werden. Dabei handelt es sich meist um Pearl-Skripte, die eine Verbindung zum ESXi-Host aufnehmen.
- vSphere RCLI und PowerCLI haben bei der kostenlosen Version nur Lese-, aber keine Schreibberechtigungen.
- Die Installation über Kickstart-Skripte (z. B. USB oder CD) ist möglich.
- Booten über SAN wird bei ESXi auch unterstützt.