1 Virtualisierung

Dieses Kapitel bietet die Basis zum Verständnis der Virtualisierung. Ausgehend von der Begriffserklärung für *Virtualisierung* wird die Funktionsweise von Hypervisoren und virtuellen Maschinen vorgestellt. Darauf aufbauend folgt ein Vergleich zwischen den unterschiedlichen Virtualisierungsformen und ihrer praktischen Ausformungen bei aktuell gängigen Virtualisierungsprodukten. Insbesondere werden hierbei die beiden Virtualisierungslösungen Xen und VMware vorgestellt und separat betrachtet. KVM wird später in einem eigenen Kapitel detailliert dargestellt. Schließlich folgen noch Anmerkungen zum Einsatz und der Bedeutung der Virtualisierung in der gegenwärtigen Informationstechnologie.

1.1 Was ist Virtualisierung?

Virtualisierung gibt es im Bereich der Informatik schon seit Mitte der 60er-Jahre, als vor allem IBM mit Versuchssystemen unter anderem zur virtuellen Speicherverwaltung[1] die Grundlagen für ein hardwareunabhängigeres Design von Rechnersystemen legte. IBM entwickelte in den 90er-Jahren für seine Mainframe-Server (z.B. IBM System z) auch erstmals die Technik der *logischen Partitionierung* (engl. logical partition, LPAR), bei der die einfach vorhandenen Hardwareressourcen (CPUs, Arbeitsspeicher, Festplattenspeicher etc.) in mehrere Systeme – sogenannte *Partitionen* – aufgeteilt wurden. Deshalb spricht man in diesem Zusammenhang auch von *Serverpartitionierung* – im Gegensatz zu Virtualisierung, bei der etwas nachgebildet wird.

[1] Bei der virtuellen Speicherverwaltung wird den Prozessen ein vom physikalischen Hauptspeicher unabhängiger Adressraum, der *virtuelle Speicher*, zur Verfügung gestellt. Zugriffe auf den Hauptspeicher erfolgen nicht mehr direkt durch die Prozesse selbst; stattdessen werden die Speicheranforderungen von einem Speichermanager abgefangen und weiterverarbeitet. Dies ermöglicht Speicherschutzmechanismen zur Abtrennung der Adressräume von Prozessen sowie die Nutzung von Massenspeichern zur Auslagerung von Speicherinhalten, die sonst die tatsächlich vorhandene Speicherkapazität überschreiten würden.

Christoph Arnold / Michel Rode / Jan Sperling / Andreas Steil, KVM Best Practices, dpunkt.verlag, ISBN 978-3-89864-737-3

Die logische Partitionierung wird auf der Hardwareebene realisiert und hat daher kaum Performance-Einbußen zur Folge. Sie sorgt beispielsweise beim Arbeitsspeicher dafür, dass jeder Partition ein bestimmter Adressierungsbereich ohne Überschneidungen zugewiesen wird. Zur Prozessornutzung hatte in der Anfangsphase der logischen Partitionierung jede Partition ihre eigene Zentraleinheit (CPU); später dann konnte mit der Technik der *Mikro-Partitionierung* ein Prozessor mehrere logische Partitionen verwalten. Diese Techniken wurden im Laufe der Zeit auch in andere Großrechnerserien übernommen. Je nach Großrechnerserie können solche Systeme ihre Ressourcen auf 60 oder mehr logische Partitionen aufteilen. Aber nicht nur die Aufteilung von Rechnerressourcen, auch die Bündelung zu sogenannten *Clustern* hat der Virtualisierung neue Aufgabengebiete erschlossen. Statt teurer Großrechner wird für das Supercomputing immer mehr Standardhardware eingesetzt, deren Rechenleistung durch Virtualisierung zusammengefasst werden kann.

Im Laufe der Zeit haben sich weitere unterschiedliche Konzepte und damit verbundene Technologien – sowohl bei der Hardware als auch bei der Software – herausgebildet. Die Entwicklung hat sich – abgesehen von der Hardwareunterstützung (siehe Abschnitt 1.3.4, S. 10) – jedoch zunehmend in Richtung Software verschoben. Die heutigen Anbieter von Virtualisierungslösungen sind in den meisten Fällen Softwarefirmen.

So unterschiedlich die Lösungen virtueller Systemumgebungen auch sein mögen, sie alle dienen dem einen Zweck: vorhandene Systemressourcen effizient und sicher zu nutzen. Wenn es auch keine allgemeingültige Definition für *Virtualisierung*[2] gibt, so können doch alle diese Lösungen mit der folgenden Definition beschrieben werden:

Definition: Virtualisierung

Als Virtualisierung bezeichnet man Techniken, die Ressourcen eines Rechners aufteilen oder zusammenfassen und dabei das Funktionsverhalten der realen Maschine kapseln.

Unter Ressourcen versteht man im Zusammenhang mit der Virtualisierung Prozessor(en), Hauptspeicher sowie I/O-Ressourcen des Netz-

[2] Der Wortbedeutung nach ließe sich *Virtualisierung* (lat.: virtus = Mannhaftigkeit, Tüchtigkeit, Vermögen, Kraft; Tugend, ...) als *mit der Fähigkeit ausgestattet* oder *mit dem Vermögen ausgestattet* deuten.

werks und der Speichersysteme einschließlich Direct Memory Access (DMA)-Controller, die auch als *Core-Four* bezeichnet werden.

Diese Hardwareressourcen werden von einem Wirtsystem, dem *Host*, bereitgestellt und von der verwendeten Virtualisierungslösung transparent an die virtuellen (Gast-)Systeme verteilt.

Die Aufteilung der Ressourcen nennt man – wie schon bei LPAR – *Partitionierung*, wobei jede Partition ein eigenständiges Subsystem aus den vorhandenen Ressourcen darstellt, das dem virtuellen System zur Verfügung gestellt wird und eine Abstraktion der physikalischen Systembestandteile bildet. In diesem Sinne lässt sich Virtualisierung auch als eine Abstraktionsschicht beschreiben, die sich logisch zwischen Anwendung und Ressourcen einfügt.

1.2 Hypervisor und Virtual Machine Monitor

Möglich wird diese Ressourcenaufteilung durch eine logische Schicht zwischen dem Host- und dem virtuellen Gastsystem durch den sogenannten *Hypervisor*. Beim Hypervisor oder auch *Virtual Machine Monitor* (abgekürzt VMM) handelt es sich um eine Virtualisierungssoftware, die eine Ausführungsumgebung für virtuelle Maschinen schafft und ihre Steuerung ermöglicht. Der Hypervisor ist der Kern der meisten Virtualisierungsprodukte und erlaubt einem einzelnen physischen Rechner den gleichzeitigen Betrieb mehrerer virtueller Systeme. Die Gastinstanzen (engl. guests) teilen sich dann die Hardwareressourcen des Wirts (engl. host).

Für ein virtuelles System stellt sich diese Abstraktionsschicht wie eine normale Systemumgebung dar, auf die es exklusiven Zugriff hat. Der Hypervisor täuscht dem virtuellen System vor, dass es der alleinige Nutzer der entsprechenden Ressourcen ist.

Solch ein System wird – je nach Virtualisierungslösung – »virtuelle Maschine« (abgekürzt VM) oder »Container« genannt und stellt im Falle einer virtuellen Maschine meist eine komplette virtuelle Hardwareumgebung dar. Eine virtuelle Maschine meint in diesem Zusammenhang einen vollständigen Computer, der nicht aus Hardware besteht, sondern über Software abgebildet wird. Eine VM ist die Schnittstelle, die dem Gast (oder auch der Domain) vom Host bereitgestellt wird und auf der der Gast dann läuft.

Auf diesen Subsystemen können ganze Betriebssysteme oder auch nur Teile davon in einer Laufzeitumgebung gestartet werden.[3] Sich als Betriebssystem darstellende virtuelle Maschinen wiederum können voll-

[3] Eine Laufzeitumgebung ist ein durch Software realisiertes Modell eines Computers.

Christoph Arnold / Michel Rode / Jan Sperling / Andreas Steil, KVM Best Practices, dpunkt.verlag, ISBN 978-3-89864-737-3

ständig durch Software (z/VM), durch Software mit zusätzlicher Hardwareunterstützung oder allein durch Hardware (LPAR) realisiert werden.

Man unterscheidet zwei Typen von Hypervisor-Architekturen. Bei beiden Typen müssen Systemaufrufe eines Gastes, die direkt auf privilegierte Hardware (Speicher/CPU/Interrupts) zugreifen wollen, von der Hypervisor-Schicht abgefangen und interpretiert werden.[4]

Ein *Typ-1-Hypervisor* läuft ohne weitere Software direkt auf der Hardware und arbeitet dadurch recht ressourcenschonend. Der Hypervisor fängt privilegierte Operationen, die exklusiven Zugriff auf die Hardware brauchen, ab und ersetzt sie durch unprivilegierte Operationen. Typ-1-Hypervisoren sind sehr schlank und robust und gelten als die performantesten Servervirtualisierungsprodukte. Die virtuellen Maschinen nutzen die vom Hypervisor bereitgestellten Ressourcen. Allerdings muss der Hypervisor selbst die Treiber für die Hardware mitbringen. Bekannte Vertreter des Typ-1-Hypervisors sind beispielsweise IBM z/VM, Xen, VMware ESX oder Sun Logical Domains.

Ein *Typ-2-Hypervisor* dagegen setzt als Anwendung in Form der Virtualisierungssoftware auf ein vollwertiges (Host-)Betriebssystem auf und kann daher die Gerätetreiber des Betriebssystems, auf dem er läuft, nutzen. Im Wesentlichen funktioniert ein Typ-2-Hypervisor also wie ein Typ-1-Hypervisor, nur dass ein Hostbetriebssystem die Verwaltung der virtuellen Systeme übernimmt. Beispiele für den Typ-2-Hypervisor sind VMware Server/Workstation, Microsoft Virtual PC, QEMU, Parallels Workstation/Desktop.

Bei der x86-Architektur wurden entsprechende Funktionen ursprünglich über die Software des Hypervisors realisiert. Mit der Einführung der hardwareunterstützten Virtualisierung (siehe Abschnitt 1.3.4, S. 10) helfen spezielle Virtualisierungsfunktionen des x86-Prozessors (Intel-VT, AMD-V) bei der Ausführung solcher Systemaufrufe.

1.3 Virtualisierungstechniken

Mit der Zeit haben sich vier grundlegende Techniken zur Virtualisierung herausgebildet, die in den folgenden Abschnitten ausführlicher dargestellt werden: die Virtualisierung auf Betriebssystemebene, auch Prozessvirtualisierung genannt, die Vollvirtualisierung, die Paravirtualisierung und die hardwareunterstützte Virtualisierung.

[4] Näheres dazu findet sich in Abschnitt 1.3.4, Die Ringproblematik, S. 11ff.

1.3.1 Prozessvirtualisierung

Bei der Prozessvirtualisierung werden Prozesse auf Betriebssystemebene über unterschiedliche virtuelle Prozessräume verteilt. Den Prozessen wird dabei vorgespielt, sie könnten eine komplette Rechnerumgebung benutzen, sie sind aber tatsächlich isolierte Userspace-Instanzen (»Container« oder »Jails«) eines darunterliegenden Betriebssystems, weshalb auch der Begriff »Betriebssystemvirtualisierung« gebräuchlich ist. Dies geschieht auf Basis des bereits laufenden Kernels, es wird also kein neuer Kernel gestartet. Den einzelnen Prozessgruppen wird eine virtuelle Laufzeitumgebung innerhalb eines Containers zur Verfügung gestellt. Durch die unterschiedlichen Prozessräume innerhalb der Container entsteht der Eindruck mehrerer unabhängiger Systeme. Es gibt aber nur einen Prozessraum und dessen Kernel, der für eine strikte Trennung zwischen den einzelnen virtuellen Prozessräumen der Container sorgt. Durch die virtuellen Prozessräume lassen sich mehrere virtuelle Systeme logisch voneinander trennen.

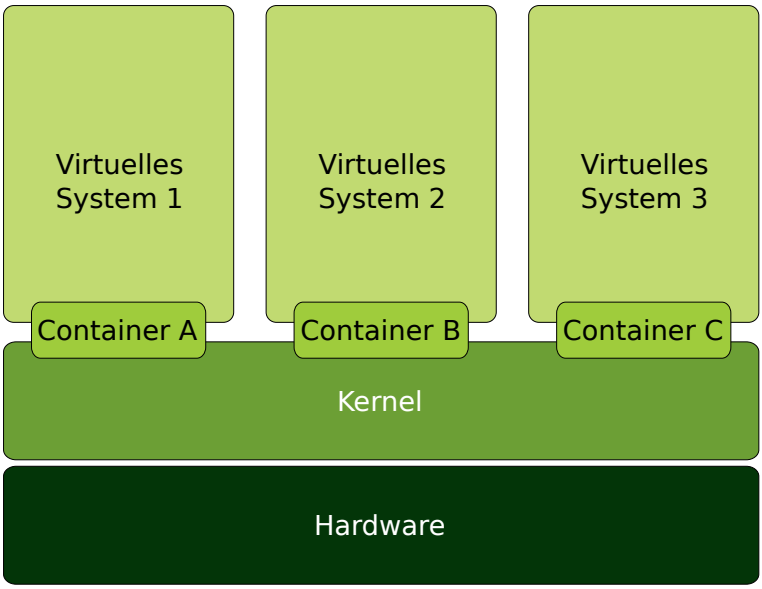

Abb. 1-1
Prozessvirtualisierung – ein Kernel für alle virtuellen Systeme

Da sich diese Art der Virtualisierung an Prozessen und Prozessgruppen orientiert, spricht man auch von Prozessvirtualisierung. Diese Technik wird überwiegend dazu verwendet, Anwendungen so voneinander zu isolieren, dass ein Angreifer, der die Kontrolle über so eine Anwendung erlangt hat, nicht ohne Weiteres Zugriff auf die anderen Container erlangen kann. Solaris Zones und FreeBSD jails sind die klassischen Vertreter für Prozessvirtualisierung, aber auch die Linux-Projekte

Christoph Arnold / Michel Rode / Jan Sperling / Andreas Steil, KVM Best Practices, dpunkt.verlag, ISBN 978-3-89864-737-3

VServer und OpenVZ fallen in diese Kategorie. Auch beim User Mode Linux kann man von Prozessvirtualisierung sprechen. Es nimmt aber eine Sonderstellung ein, da dort ein spezieller User-Mode-Kernel unter Kontrolle des Hostkernels läuft.

Da es nur eine Kernel-Instanz gibt, die bereits Bestandteil des verwendeten Betriebssystems ist, gestaltet sich der Einsatz dieser Virtualisierung sehr einfach. Sie lässt sich gut und ohne großen Aufwand in bestehende Systeme integrieren. Dabei sind keine großen Performance-Einbrüche zu befürchten, da durch die Nutzung einer einzelnen Kernel-Instanz kein Prozessoverhead entsteht. Durch die Verwendung eines Kernels ergibt sich aber der Nachteil, dass alle Container auf eben diesen angewiesen sind. Somit können keine unterschiedlich konfigurierten Kernel-Instanzen oder gar Betriebssysteme laufen. Auch ist es nicht möglich, Laufzeitparameter des Kernels aus den Containern heraus zu verändern. Darüber hinaus ist die Implementierung der Prozessvirtualisierung überaus komplex, da für autarke Systeme eine vollständige Trennung aller Prozesse notwendig ist.

1.3.2 Vollvirtualisierung

Bei der Vollvirtualisierung (engl. full virtualization) wird die logische Schicht zwischen dem Host und dem Gast durch eine Softwarekomponente realisiert, die sich *Hypervisor* oder *Virtual Machine Monitor* (VMM) nennt. Dieser bildet das Bindeglied zwischen dem virtualisierten Gastsystem und dem Hostsystem, indem er die Hardwarezugriffe der virtuellen Maschine über den Host an die physikalische Hardware weiterreicht.

Mittels Vollvirtualisierung gelang es erstmals, beliebigige x86-Betriebssysteme virtuell auf der Intel-Architektur laufen zu lassen. Diese kann somit als *Urahn* der Intel-Virtualisierung bezeichnet werden. Bei der Vollvirtualisierung sind die Gastsysteme und deren Kernel ohne weitere Anpassung in der virtuellen Umgebung lauffähig. Ein Gastsystem benötigt lediglich die passenden Treiber der emulierten Hardware. Dabei ist man im Vergleich zur Prozessvirtualisierung nicht auf das auf dem Host laufende Betriebssystem beschränkt. Diese Freiheit wird durch die Emulation der Hardwarekomponenten erreicht. Im Unterschied zur vollständigen Emulation (siehe Abschnitt 1.3.5, S. 15) werden CPU-Befehle aber ohne weitere Übersetzung an die physikalischen Prozessoren des Hosts durchgereicht.
Als verdeutlichendes Beispiel sei hier der Zugriff auf den Arbeitsspeicher genannt.[5] Der physikalisch vorhandene Arbeitsspeicher wird innerhalb vom Virtual Machine Monitor durch eine *Shadow Page Table*

[5] Diese Erklärung trifft beim Einsatz von *Nested Page Tables* (NPT) nicht mehr zu. Mehr dazu in Abschnitt 1.3.4, S.10

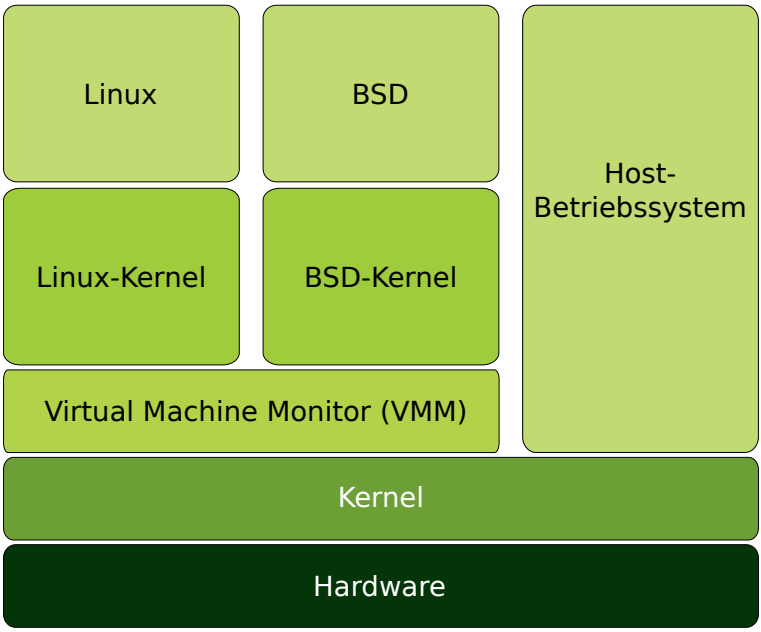

Abb. 1-2
Vollvirtualisierung – der VMM als Bindeglied zwischen Gast- und Host-Kernel

dargestellt. Mit deren Hilfe wird der Arbeitsspeicher einer virtuellen Maschine auf den des Hostsystems abgebildet, ohne dass diese einen direkten Zugriff darauf erhält. Am einfachsten kann man sich die Shadow Page Table als eine Tabelle vorstellen, in der der Speicherbereich X einer virtuellen Maschine dem Bereich Y im realen Arbeitsspeicher zugeordnet wird. Das Gastsystem sieht immer nur den Bereich X und erst der Virtual Machine Monitor setzt Zugriffe auf diesen Bereich in den realen Bereich um. Das Gastsystem kann nicht beurteilen, ob es in einer virtuellen Maschine läuft oder auf realer Hardware, weshalb diese Zugriffe als *transparent* bezeichnet werden. Alle Zugriffe auf reale Hardware werden über den Virtual Machine Monitor gesteuert.

Die Vollvirtualisierung hat den Vorteil, dass – wie bereits erwähnt – keine Anpassungen am zu virtualisierenden System nötig sind. Dies macht diese Virtualisierungslösung sehr einfach anwendbar. Das Prinzip, nach dem bei der Vollvirtualisierung gearbeitet wird, lässt sich auf jede moderne Prozessorarchitektur anwenden. Dadurch dass keinerlei Anpassung auf Betriebssystemebene notwendig ist und eine Umwandlung der Hardwarezugriffe über eine Softwarelösung realisiert wird, hat die Vollvirtualisierung den Nachteil, einen sehr großen Overhead zu erzeugen, der sich entsprechend in der Performance niederschlägt.[6]

[6]Durch den Einsatz von paravirtualisierenden virtio-Treibern (siehe Abschnitt 2.3, S. 31) kann die Performance einer Vollvirtualisierung jedoch enorm gesteigert werden.

Christoph Arnold / Michel Rode / Jan Sperling / Andreas Steil, KVM Best Practices, dpunkt.verlag, ISBN 978-3-89864-737-3

Die Vollvirtualisierung ist weit verbreitet mit entsprechend bekannten Produkten aller derzeit relevanten Virtualisierungsanbieter: So nutzen neben VMware beispielsweise die VirtualBox von Oracle oder auch Microsofts Virtual PC eine Vollvirtualisierung mit Hardwareunterstützung. Auch Xen gehört in diese Reihe, wobei Xen zusätzlich noch Paravirtualisierung beherrscht.

1.3.3 Paravirtualisierung

Bei der Paravirtualisierung wird die Implementierung der Virtualisierung in einen host- und einen gastspezifischen Teil aufgeteilt. Dabei wird vom Hostsystem eine Schnittstelle bereitgestellt, die vom Gastbetriebssystem unterstützt werden muss.[7] Durch die entsprechende Implementierung dieser definierten Schnittstellen ist es dem Gast möglich, alle privilegierten Aufgaben aktiv an den Virtual Machine Monitor (Hypervisor) durchzureichen. So entfällt dessen Aufgabe, den Gast zu überwachen. In den virtuellen Maschinen kommen dazu Frontend-Treiber zum Einsatz, die jeweils mithilfe eines korrespondierenden Backend-Treibers in einem privilegierten System die Hardware direkt ansprechen (siehe Abb. 1-3). Die Kommunikation zwischen Front- und Backend findet über einen gemeinsam genutzten Speicherbereich, den *Event-Channel*, statt.

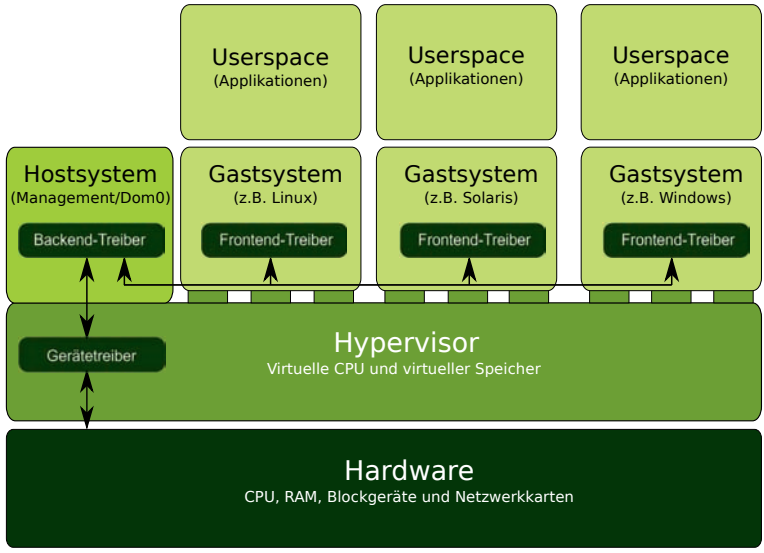

Abb. 1-3
Paravirtualisierung – angepasste Gastsysteme

[7] *Para* (griechisch: neben, bei, ...) bedeutet in diesem Zusammenhang so viel wie *miteinander*.

Die Schnittstelle zwischen den Host- und Gastsystemen wird durch eine Erweiterung des CPU-Befehlssatzes in Form sogenannter *Hypercalls* realisiert. Dazu muss der Kernel des Gastbetriebssystems modifiziert werden: Alle Bereiche des Kernelcodes, die privilegierte Befehle aufrufen, müssen so umgeschrieben werden, dass diese als Hypercalls die Funktion des Hypervisors nutzen. Hypercalls sind Funktionsaufrufe, die an den Hypervisor weitergeleitet werden, und funktionieren analog zu Systemaufrufen: So wie Systemaufrufe es Prozessen im Userspace gestatten, privilegierte Operationen über den Kernel aufzurufen, ermöglichen Hypercalls es dem Gastkernel, privilegierte Operationen über den Hypervisor aufzurufen.[8] Der Virtual Machine Monitor verschiebt sich vom Userspace in den Kernelspace und wird im Zusammenhang mit der Paravirtualisierung meist *Hypervisor* genannt. Durch die Verschiebung in den Kernelspace wird das Hostbetriebssystem selbst zu einem virtuellen System, das lediglich mehr Privilegien als die Gastsysteme hat. Auch die im System vorhandenen Ressourcen lassen sich dadurch hardwarenah partitionieren. Die partitionierte Hardware kann durch das angepasste Gastsystem mithilfe der neuen Befehlssätze angesprochen werden. Dadurch entfällt die performancelastige Emulation der entsprechenden Hardware. Das Gastsystem ist sich durch die Anpassung auch darüber bewusst, in einer virtuellen Umgebung zu laufen, und der Hypervisor muss diese nicht überwachen, sondern stellt nur eine Laufzeitumgebung bereit, die es dem Gast erlaubt, auf die partitionierte Hardware zuzugreifen.

Dieses System bezeichnet man bei Xen als Dom0.

Somit wird, im Vergleich zum Virtual Machine Monitor bei der Vollvirtualisierung, der Aufgabenbereich umgekehrt. Der Virtual Machine Monitor sorgt nicht mehr dafür, dass privilegierte Operationen abgefangen und auf das Hostsystem umgeleitet werden, sondern der Gast meldet solch eine Operation beim Hypervisor an und kann dank des erweiterten Befehlssatzes direkt auf die entsprechenden Komponenten zugreifen. Dafür sind die schon erwähnten Hypercalls nötig. Durch die Befehlssatzerweiterung wird quasi eine neue Architektur definiert; so entsteht z.B. aus der x86-Architektur mit der entsprechenden Befehlssatzerweiterung für Xen die Architektur x86/xen.

Damit das Gastsystem in einer paravirtuellen Umgebung laufen kann, muss es erst einmal portiert werden, um die entsprechenden Befehlssätze zu beherrschen. Diese Anpassung benötigt wenige tausend Zeilen zusätzlichen Programmcode. Allerdings erzeugt man dadurch nicht mehr quelloffene Systeme (engl. closed source) und ist auf die Unterstützung des Herstellers angewiesen. Da aber nicht jeder Hersteller

[8] Um die Zahl der dabei entstehenden aufwendigen Kontextwechsel zu reduzieren, können diese Funktionsaufrufe gruppiert werden.

Christoph Arnold / Michel Rode / Jan Sperling / Andreas Steil, KVM Best Practices, dpunkt.verlag, ISBN 978-3-89864-737-3

entsprechende Änderungen vornehmen kann oder will, können nicht alle Betriebssysteme rein paravirtualisiert betrieben werden.[9]

Paravirtuelle Lösungen haben durch den Wegfall der Hardwareemulation den Vorteil einer hohen Performance. Dadurch, dass Gastsysteme auf die zu verwendende Lösung portiert werden müssen, um die nötige Unterstützung für die Befehlssatzerweiterungen zu bieten, muss man bei proprietären Systemen auf die Unterstützung des entsprechenden Herstellers zurückgreifen.

Auch wenn die Idee hinter der Paravirtualisierung schon älter ist, ist die entsprechende Umsetzung auf der x86-Architektur noch relativ jung. Am bekanntesten dürfte die Realisierung mittels Xen sein. Ob Xen in Zukunft das paravirtualisierte Modell zugunsten der hardwareunterstützten Virtualisierung aufgeben wird, kann momentan noch nicht beurteilt werden.

1.3.4 Hardwareunterstützte Virtualisierung

Was auf anderen Architekturen schon seit langer Zeit fest implementiert ist, wurde auf der x86-Architektur erst in den letzten Jahren umgesetzt. Die Rede ist von der Implementierung der Virtualisierung in der CPU, der *hardwareunterstützten Virtualisierung* (engl. hardware assisted full virtualization, auch *Native Virtualisierung*). Eines der bekannteren Beispiele ist das schon eingangs erwähnte *Locigal Partitioning* (LPAR) auf der System-p- und System-z-Architektur von IBM. Bei LPAR wird eher eine Art Paravirtualisierung auf Hardwareebene realisiert, was sie zu der momentan performantesten Virtualisierungslösung macht. LPAR ist allerdings nicht auf x86-Systemen verfügbar. Für diese wurde eine Hardwareunterstützung für die Vollvirtualisierung jeweils eigenständig von den Firmen Intel und AMD entwickelt. Die Entwicklung von Intel trug dabei den Codenamen *Vanderpool* und wird jetzt *Intel Virtualization Technology for x86*, kurz VT-x, genannt. AMD entwickelte seine Lösung, die jetzt als *AMD Virtualization*, kurz AMD-V, bekannt ist, unter dem Codenamen *Pacifica*. Beide Hersteller präsentierten ihre Entwicklungen erstmals 2005. Die zwei Lösungen sind – trotz vieler Analogien – nicht zueinander kompatibel, d.h. eine Virtualisierungssoftware muss für AMD-V eine andere Unterstützung anbieten als für Intels VT-x.

[9] Umgehen lässt sich dieses Problem mit Prozessoren, die eine Hardwareunterstützung für die Virtualisierung bieten, in Kombination mit speziellen Treibern: Damit können unmodifizierte Betriebssysteme (z.B. Microsoft Windows), die keine Portierung anbieten, mit Xen oder VMware ESX Server paravirtualisiert laufen.

Eine Hardwareunterstützung verringert zwar den Prozess-Overhead der Virtualisierung selbst; dennoch ist ohne weitere Unterstützung mit großen Performance-Einbußen zu rechnen, die auf I/O-Einschränkungen zurückzuführen sind, da die Treiber für das Gastsystem emuliert werden müssen und somit den Flaschenhals bilden. Dieses Problem lässt sich entweder durch den Einsatz paravirtualisierter Treiber oder durch eine spezielle Hardwareunterstützung für die I/O-Virtualisierung umgehen. Besonders die Hardwareunterstützung hat in den letzten Jahren große Fortschritte gemacht. So sind in den letzten Jahren unter anderem Funktionen wie PCI Passthrough, Single Root I/O Virtualization (SR-IOV) und Hardware-Assisted Paging (HAP), auch als *Nested Page Tables* (NTP) bekannt, hinzugekommen. Bei PCI Passthrough, oder auch *I/O Memory Mapping Unit* (IOMMU), wird es den Gästen möglich, physikalische Geräte direkt zu verwenden. Auf Intel-Systemen wird diese Funktion VT-d (Virtualization Technology for Directed I/O) genannt und benötigt sowohl die Unterstützung durch die CPU als auch durch den Chipsatz. Auf AMD-Systemen heißt diese Funktion AMD-Vi und ist seit Version 3 Bestandteil vom Hypertransportprotokoll und benötigt ebenfalls unterstützende Prozessoren. Mit IOMMU kann jedoch das Gerät nur von einem Gast gleichzeitig verwendet werden. Diese Beschränkung wird durch SR-IOV umgangen, das eine Erweiterung des PCI Express Standard ist. Es ist auf Intel-Systemen auch Bestandteil der *Virtualization Technology for Connectivity* (VT-c).

Bei *Nested Page Tables* (NPT) wird den Gästen direkter Zugriff auf den physikalischen Speicher gewährt, sodass keine Shadow Page Table mehr notwendig ist. Dadurch entfällt ein Großteil des ansonsten notwendigen Virtualisierungs-Overheads. Bei Intel wurde dieses Feature *Extended Page Tables* (EPT) genannt und ist auf der Nehalem-Architektur verfügbar. Bei AMD wurde diese Technik als Rapid Virtualization Indexing (RVI) mit Prozessoren der Barcelona-Reihe eingeführt.

Allen Ansätzen gemeinsam ist die Rolle des Hypervisors, der immer mit der höchsten Privilegienstufe (siehe Abschnitt 1.3.4 »Die Ringproblematik«) ausgeführt wird und stets die virtuellen Betriebssysteminstanzen und deren Zugriff auf die Ressourcen kontrolliert.

Die Ringproblematik

x86-kompatible CPUs enthalten vier unterschiedliche Privilegienstufen für den Speicherzugriff und den Umfang des nutzbaren CPU-Befehlssatzes. Diese Privilegienstufen werden *Domains* genannt und als Ringe (Ring 0 bis Ring 3) dargestellt (siehe Abb. 1-4).

Christoph Arnold / Michel Rode / Jan Sperling / Andreas Steil, KVM Best Practices, dpunkt.verlag, ISBN 978-3-89864-737-3

Der innerste Ring 0 verfügt im sogenannten *Supervisor Mode* über alle Rechte der CPU. Privilegierte Prozessoranweisungen, die den Prozessorzustand verändern und die direkte Zugriffe auf die Register, den Arbeitsspeicher und die übrige Hardware ausführen, können nur in Ring 0 abgearbeitet werden.

So läuft auf Ring 0 normalerweise der Kernel eines Betriebssystems, weshalb er auch als *Kernelspace* bezeichnet wird. Nach außen hin werden die Rechte immer weiter eingeschränkt. Während also der Betriebssystem-Kernel privilegierte Prozessoranweisungen im Ring 0 verwenden darf, sind die Anwendungen auf den Benutzermodus – den *Userspace* – von Ring 3 beschränkt.[10] Die Kommunikation zwischen den Ringen erfolgt über sogenannte *Gates*, definierte Schnittstellen, die Aufrufe und deren Rückmeldungen weiterreichen.

Ein Prozess kann grundsätzlich nur innerhalb eines einzelnen Rings ausgeführt werden. Er kann sich nicht selbst in eine andere Privilegienstufe versetzen.

Will nun ein Prozess eines weniger privilegierten Rings eine privilegierte Operation ausführen, muss der Prozess eine *Exception* erzeugen, die diese Operation abfängt und in einem höher privilegierten Ring ausführt.

Der Prozess veranlasst dazu mittels eines *Systemaufruf*s (engl. system call) einen *Kontextwechsel*, bei dem er die Kontrolle über den Prozessor vorübergehend an den Kernel übergibt. Nachdem die Anfrage abgearbeitet wurde, gibt der Kernel die Kontrolle über den Prozessor wieder an den Prozess des Benutzermodus zurück. Der kann dann im Programm dort weitermachen, wo er vor dem Kontextwechsel gestoppt wurde.

Der Userspace-Prozess verlässt dabei niemals den nichtprivilegierten Ring und kann so auch nicht Gefahr laufen, andere Prozesse oder gar die Stabilität des Systemkerns selbst zu gefährden, da nur vertrauenswürdiger Code aus dem Kernel im privilegierten Modus ausgeführt wird.

Zweck dieser Ringarchitektur ist es, die Stabilität und Sicherheit des Systems zu gewährleisten, indem Prozesse auf ihren erlaubten Kontext beschränkt und so davon abgehalten werden, sich gegenseitig unerwünscht zu beeinflussen. Vor allem die Prozesse des Betriebssystem-Kernels selbst bleiben so vor Anwendungsprogrammen im Benutzer-

[10] Die Ringe 1 und 2 finden kaum Verwendung und spielen in diesem Zusammenhang keine Rolle. Ring 1 und Ring 2 wurden bei der x86-Architektur gelegentlich zum Priorisieren von Gerätetreibern eingesetzt. Die meisten aktuellen Prozessorarchitekturen unterscheiden nur zwei Ringe, weshalb die gängigen Betriebssysteme aus Portabilitätsgründen auf die Nutzung von Ring 1 und Ring 2 verzichten.

modus geschützt. Es wird stets nur vertrauenswürdiger Code aus dem Kernel im privilegierten Modus ausgeführt.[11]

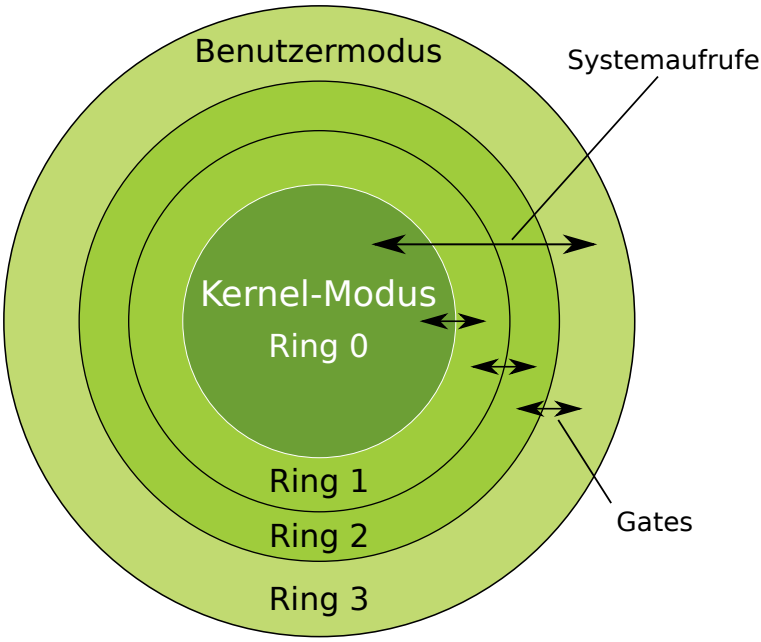

Abb. 1-4
Ringarchitektur – Systemaufrufe müssen vom Hypervisor im Ring 0 abgefangen werden.

Bei nicht virtualisierten Systemen arbeiten der Kernel (und die Hardwaretreiber) also im Ring 0 und die Anwendungen im weniger privilegierten Ring 3. Wenn eine Anwendung einen privilegierten Befehl ausführen will, muss der Befehl an den Kernel in Ring 0 übergeben werden.

Daraus ergibt sich bei der Virtualisierung aber die sogenannte »Ringproblematik«: Sollen mehrere Gastsysteme unmodifiziert laufen, müssten sich diese alle Ring 0 teilen, was bei gleichzeitigen Zugriffen unmöglich wäre.

Für die Virtualisierung auf x86-Prozessoren wird zur Steuerung der virtuellen Maschinen folglich eine eigene Virtualisierungsschicht unterhalb der Gastsysteme benötigt, die diese Zugriffe steuert. Dazu läuft der Virtual Machine Monitor im Ring 0. Ring 0 steht dadurch dem Betriebssystem einer virtuellen Maschine nicht mehr zur Verfügung. Privilegierte Prozessoranweisungen eines Gastsystems müssen nun vom Virtual Machine Monitor erkannt, abgefangen und – mit entsprechendem Performance-Verlust – weiterverarbeitet werden.

[11] Kann eine Exception nicht abgefangen werden, entsteht ein *General Protection Fault* (GPF) und der auslösende Prozess stürzt ab; bei einem Kernel – das virtualisierte Gastsystem läuft einschließlich Kernel im weniger privilegierten Ring 3 – wäre das ganze System betroffen …

Christoph Arnold / Michel Rode / Jan Sperling / Andreas Steil, KVM Best Practices, dpunkt.verlag, ISBN 978-3-89864-737-3

Aktuelle CPU-Generationen von Intel und AMD[12] bieten auf Basis der x86-Architektur eine direkte Hardwareunterstützung für die Virtualisierung, die diese privilegierten Befehlsaufrufe verarbeiten kann.

Die wesentliche Neuerung dabei ist die sogenannte *Hypervisor-Schicht*, die durch ein Aufsplitten von Ring 0 gebildet wurde. Die Ausführung des Virtual Machine Monitor (Hypervisors) wird in eine neue Schicht unterhalb von Ring 0 – auch *Ring -1* genannt – verschoben und läuft dann in einem speziellen, privilegierten Modus, dem *Root Mode Privilege Level*. Dadurch ist es möglich, einen nicht modifizierten Gastkernel im Kernelspace von Ring 0, jedoch in einem weniger privilegierten *Non Root Mode*, laufen zu lassen und ihm die Ausführung nichtkritischer Systemaufrufe zu erlauben.

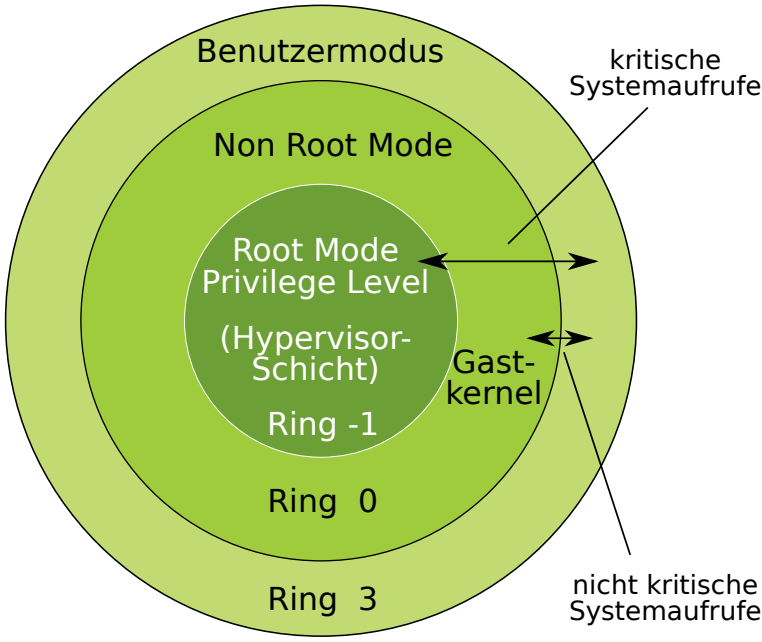

Abb. 1-5 *Ringarchitektur mit Hardwareunterstützung und Hypervisor im Ring -1*

Systemaufrufe bedürfen so nicht mehr in jedem Fall des Einschreitens des Hypervisors; solange keine kritischen Zugriffe[13] erfolgen, kann ein Gastsystem die Systemaufrufe für Anwendungen des Userspace selbst ausführen. Sobald ein Gastsystem versucht, einen kritischen Befehl auszuführen, greift die Hardwareunterstützung des Prozessors ein. Sie fängt diesen Befehl ab und übergibt ihn an den Hypervisor, der den Be-

[12] Prozessoren vom Typ VT-x (Intel) und AMD-V (AMD) sind seit 2006 erhältlich.

[13] Kritisch sind alle Aufrufe, die exklusiven Hardwarezugriff erfordern, wie Schreibvorgänge auf die Festplatte, die einen Interrupt auslösen.

fehl im Kernel-Modus weiterverarbeitet. Der Hypervisor sorgt dabei für einen kontrollierten Zugriff der Gäste auf die Ressourcen des Hostrechners. Durch diese Aufteilung können privilegierte Befehle von Gastsystemen sauber von anderen Gastsystemen und vom Hostsystem getrennt und gegebenenfalls störende Auswirkungen eines privilegierten Befehls in unschädlichen Grenzen gehalten werden. Den Gastsystemen wird dabei stets das ordnungsgemäße Verhalten eines unabhängigen Rechners vorgespielt. Es entfällt die Notwendigkeit, den Kernel der Gäste für eine Hypercall-Unterstützung zu patchen oder zu paravirtualisieren.

Dadurch, dass virtuelle Maschinen ohne den Umweg über Software auf Ring 0 zugreifen können, wird ein erheblicher Performance-Gewinn gegenüber einer reinen Softwarelösung erzielt. Darüber hinaus bringt diese Technik auch eine erhöhte Sicherheit mit sich, da die Ausführung der Gäste weit weniger Emulation durch Software erfordert. Eine geringere Fehleranfälligkeit ist die Folge.

1.3.5 Emulation

Während bei der Virtualisierung die Befehle einer virtuellen Maschine größtenteils direkt auf der CPU ausgeführt werden, werden bei der *Emulation* die Befehlssätze einer kompletten Architektur durch Software auf einer anderen Architektur nachgebaut (*emuliert*). Jedes Stück Hardware – auch die CPU – wird also durch Software nachgebildet. Prinzipiell können beliebige Architekturen emuliert werden. Eine komplette Hardwareemulation ermöglicht es sogar, ein nicht modifiziertes System, das für eine andere Prozessorarchitektur als die des Hostsystems geschrieben wurde, zu betreiben.

Im Unterschied zur Virtualisierung können bei der Emulation die Zugriffe aber nicht vom Gast zum Prozessor durchgereicht werden, sondern müssen umständlich und rechenintensiv umgeschrieben werden. Das führt zwar einerseits zu einer sauberen Trennung von Host- und Gastsystemen und bietet die Möglichkeit der Verwendung von grundsätzlich beliebigen Hardwaretreibern, erfordert andererseits aber viel Rechenleistung und stellt hohe Anforderungen an den Emulator. Vorteil der Emulation ist also ihre Flexibilität, Nachteil die geringe Performance. Performance. Eine komplette Emulation der Hardware ist daher für den Produktivbetrieb nicht geeignet.

In der Virtualisierung wird die Emulation dennoch in Teilbereichen eingesetzt: Zum einen, um einem Gastsystem spezielle Hardware, beispielsweise eine bestimmte Netzwerk- oder Soundkarte, bereitstellen zu können, die sich, aus welchen Gründen auch immer, nicht virtualisieren lässt. Zum anderen können Komponenten zur Verfügung gestellt wer-

Christoph Arnold / Michel Rode / Jan Sperling / Andreas Steil, KVM Best Practices, dpunkt.verlag, ISBN 978-3-89864-737-3

den, die für jedes System einmalig und exklusiv vorhanden sein müssen, wie beispielsweise der *Watchdog*[14].

Benötigt ein virtuelles System solch eine Systemkomponente, dann wird diese Komponente derart nachgebildet, dass sie aus Sicht der virtuellen Maschine wie ein tatsächlich vorhandenes physikalisches Gerät arbeitet.

Die bekanntesten Vertreter zur Emulation von x86-Prozessor-Architekturen sind Bochs und QEMU. QEMU ist insbesondere deshalb erwähnenswert, weil Teile aus dem QEMU-Projekt bei der Virtualisierung mit KVM genutzt werden, um bestimmte Hardwarebauteile zu emulieren. Darum ist QEMU im folgenden Kapitel auch ein eigener Abschnitt (siehe Abschnitt 2.2, S. 27) gewidmet.

1.4 Virtualisierungsprodukte

Fast alle heute relevanten Virtualisierungsanbieter nutzen primär eine Vollvirtualisierung mit Hardwareunterstützung. Im praktischen Einsatz wird unterschieden zwischen Desktop-Virtualisierung (VMware Workstation, VirtualBox, Virtual PC u.a.) und Servervirtualisierung (XEN, VMware ESXi Server, OpenVZ, Virtuozzo, Windows Server Hyper-V u.a.). KVM ist für beide Einsatzbereiche geeignet.

Hervorzuheben sind VMware und Xen, denen aufgrund ihrer Bedeutung und weiten Verbreitung jeweils ein eigener Abschnitt gewidmet wird.

1.4.1 VMware vSphere Hypervisor (ESXi)

www.vmware.de

Im Vergleich zu den bereits genannten Vollvirtualisierungslösungen wie z.B. Virtual PC geht VMware mit vSphere einen anderen Weg. Der ESXi-Server von VMware setzt eine Methode ein, die auch als *Full Virtualization with Binary Translation* bezeichnet wird.

Dabei wird die Virtualisierung des Userspace durch die Verwendung eines eigenen Kernels in den Kernelspace verschoben. Durch den Wegfall eines Hostbetriebssystems und der damit verbundenen Hardwarenähe kann VMware im Vergleich zu anderen Lösungen weitaus effektiver arbeiten. Der Virtual Machine Monitor muss aber weiterhin eine Emulationsschicht für die Hardware bieten, um den Gästen den exklusiven Zugriff auf die Hardware vorspielen zu können. Der Virtual Machine Monitor läuft im privilegierten Ring 0 und wird durch einen

[14] Ein Watchdog sorgt dafür, dass der Kernel regelmäßig ein lebenserhaltendes Signal erhält, das den voreingestellten System-Reset des Kernels unterbindet.

Mikrokernel realisiert. Infolge seiner Hardwarenähe kann er die Ressourcen sehr performant aufteilen. Mit dieser Implementierung bewegt sich der Overhead etwa im gleichen Rahmen wie bei einer Paravirtualisierung.

Ursprünglich wurde ESX als Virtual Machine Monitor verwendet. Dieser musste ein angepasstes Red Hat Linux mit einem stark angepassten Kernel starten, um ein Konfigurationsmanagement zu bieten. Der seit vSphere 4 eingesetzte ESXi-Kernel stellt selbst eine entsprechende API bereit. Durch den Wegfall des separat notwendigen Konfigurationssystems entfällt auch die Pflege eines eigenen Kernel-Tree, da dieser ja immer wieder an den proprietären Mikrokernel angepasst werden musste.

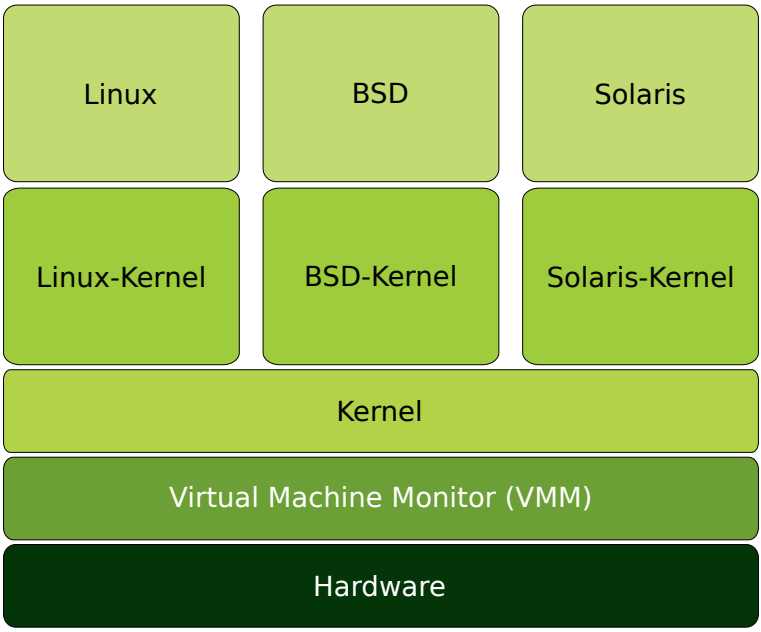

Abb. 1-6
VMware vSphere: Mikrokernel ohne Hostsystem

1.4.2 Xen

`www.xen.org`

Xen entstand ursprünglich an der britischen Universität Cambridge und wird unter der GPL entwickelt. Xen fand prominente Unterstützer wie Microsoft, Oracle, Intel und AMD, IBM, HP, Novell/SUSE und bis 2008 auch Red Hat. Um Xen zum Industriestandard zu machen, gründeten die Entwickler die Firma XenSource Inc., die 2007 von dem US-Unternehmen Citrix Systems übernommen wurde. Seitdem verantwortet Citrix das »Xen Open Source Hypervisor«-Projekt. Aktuell liegt Xen in der Version 4.1 vor.

Christoph Arnold / Michel Rode / Jan Sperling / Andreas Steil, KVM Best Practices, dpunkt.verlag, ISBN 978-3-89864-737-3

Xen ist ein klassischer Typ-1-Hypervisor, der direkt auf einer Hardware läuft, mit einer hardwarenahen Implementierung des Paravirtualisierungskonzepts und der daraus resultierenden sehr guten Performance. Die erste Domäne – so werden virtuelle Maschinen im Xen-Jargon bezeichnet –, die von Xen gestartet wird, hat eine besondere Funktion: Als privilegierte *Dom0* sorgt sie für die Interaktion mit dem eigentlichen Hypervisor und dient der Verwaltung aller weiteren unprivilegierten Domänen, den *DomUs*. Diese Verwaltungsfunktionalität muss in das Betriebssystem integriert werden, das in der Dom0 läuft. Dazu wird ein speziell angepasster Linux-Kernel eingesetzt. Auch die Kernel der Gastbetriebssysteme in den DomUs müssen angepasst und um die Hypercalls (siehe Abschnitt 1.3.3) erweitert werden. Die Auswahl an Gastarchitekturen und Emulatoren war daher eher beschränkt, Xen unterstützt aber auch Windows, Solaris und BSD als Gastbetriebssysteme.

Erforderte dieses Verfahren bislang die Pflege eines eigenen Kernel-Tree, so wurden die Erweiterungen für Xen mit Linux-Kernel 3.0 in die Linux Standard Base (LSB) aufgenommen, sodass es zukünftig nativ unterstützt wird. Durch ein neues Storage-Backend erhält die Dom0 in Verbindung mit dem Xen-Hypervisor zusätzlich direkten Zugriff auf die Hardware. Mit Kernel 3.1 kommen weitere Funktionen wie das *Xen-PCI-Backend*, das es dem Dom0-Kernel ermöglicht, PCI- und PCIe-Geräte an Xen-DomUs durchzureichen, und SR-IOV für paravirtualisierte Gäste hinzu.

www.linuxfoundation.org

Wird Xen auf einem Host mit Hardwareunterstützung (etwa AMD-V oder Intel-VT) betrieben, können die Betriebssysteme in den Domänen völlig unmodifiziert, also vollvirtualisiert laufen. Für eine solche Domäne – die sogenannte *Hardware Virtual Machine* (HVM) – ist Xen komplett transparent.

Xen gilt als sehr ausgereift und stabil und findet Einsatz in Rechenzentren und Private und Public Clouds (u.a. Amazon EC2).

Die kommerzielle Variante *XenServer* von Citrix hat einen höheren Funktionsumfang (sie unterstützt beispielsweise *Suspend to RAM*) und bietet unter anderem ein Managementtool zur zentralisierten Verwaltung der virtualisierten Systeme (*XenCenter*), ein Live-Migrationswerkzeug (*XenMotion*) sowie eine Anbindung an bestehende Storage-Systeme. Weiterhin setzt Citrix die Software als Kernbestandteil seiner Plattform zum Virtualisieren, Verwalten und Verteilen von Windows-Anwendungen ein (*XenApp*). Das Produkt *Citrix Essentials* ergänzt *XenServer* um Features wie Hochverfügbarkeit und dynamische Provisionierung.

Auch Oracles Virtualisierungsprodukt *Oracle VM* basiert auf Xen.

1.4.3 Weitere Virtualisierungsprodukte

Zur besseren Einordnung von KVM in die große Anzahl der Virtualisierungsprodukte folgt eine kurze Übersicht über weitere gängige Produkte.

Emulation:

Bochs
ist ein auf hohe Portabilität ausgelegter Emulator für x86(32-Bit)- und AMD64(64-Bit)-Architekturen für DOS-, Windows-, Linux- und BSD-Gastsysteme. (Lizenz: LGPL)
Homepage: `www.bochs.sourceforge.net/`

Servervirtualisierung:

Citrix XenServer
basiert auf dem Open Source Xen-Hypervisor und bietet als kommerzieller Ableger von Xen einen erweiterten Funktionsumfang. (Lizenz: Proprietär)
Homepage: `www.citrix.com/`

LXC
bietet eine Container-Virtualisierung unter Linux ('Linux Containers') und ist seit Version 2.6.29 Bestandteil des Linux-Kernels. (Lizenz: GPL v2) LXC kann sowohl einzelne Prozesse als auch ein komplettes Betriebssystem virtualisieren.
Homepage: `lxc.sourceforge.net/`

OpenVZ
ist ebenfalls eine Implementierung des Container-Konzepts mit der Virtualisierung auf Betriebssystemebene. (Lizenz: GPL v2)
Homepage: `www.openvz.org/`

Parallels Plesk/Virtuozzo
sind kommerzielle Weiterentwicklungen von OpenVZ mit eigener Verwaltungskonsole und u.a. erfolgreich bei Hosting-Providern und Anbietern von Cloud-Diensten. (Lizenz: Proprietär)
Homepage: `www.parallels.com/`

Windows Server Hyper-V
ist eine Implementierung des Paravirtualisierungskonzepts und setzt Windows Server 2008 voraus. Hyper-V unterstützt auch Linux (offiziell RHEL und SLES). (Lizenz: Proprietär)
Homepage: `www.microsoft.com/`

Christoph Arnold / Michel Rode / Jan Sperling / Andreas Steil, KVM Best Practices, dpunkt.verlag, ISBN 978-3-89864-737-3

Desktop-Virtualisierung:

Citrix XenApp
ist das bekannteste Produkt von Citrix (früher: Citrix Presentation Server, Citrix Metaframe) und eigentlich eine Terminalanwendung zum Zugriff auf das Unternehmensnetz. XenApp ermöglicht es mithilfe des Citrix-ICA-Clients, von jedem Rechner aus auf die Unternehmenssoftware zuzugreifen, ohne dass diese auf dem verwendeten Rechner lokal installiert sein muss. Dadurch können auch Anwendungen, die sonst auf einem Rechner etwa mangels Hardwareressourcen oder wegen eines veralteten Betriebssystems nicht laufen würden, verwendbar gemacht werden. (Lizenz: Proprietär)
Homepage: `www.citrix.com/`

Oracle xVM
ist der Xen-basierte Nachfolger von Suns xVM-Hypervisor und Bestandteil des Betriebssystems Solaris, unterstützt aber auch Microsoft Windows und Linux als Gastbetriebssystem. (Lizenz: Proprietär)
Homepage: `www.oracle.com/`

Parallels Desktop für Mac
ist eine Speziallösung für Mac OS X, vor allem um Windows-Programme auf Apple-Hardware laufen zu lassen. (Lizenz: Proprietär)
Homepage: `www.parallels.com/`

Parallels Workstation
bietet Desktop-Virtualisierung für Linux- und Windows-Hosts und wirbt mit seiner Benutzerfreundlichkeit. (Lizenz: Proprietär)
Homepage: `www.parallels.com/`

VirtualBox
ist eine Implementierung des Vollvirtualisierungs-(Typ-2-) Konzepts. Ursprünglich von der deutschen Firma innotek entwickelt, dann von Sun Microsystems aufgekauft, gehört sie mittlerweile Oracle. Unterstützt Windows, Mac OS X und Linux (ab Kernel 2.4) als Hostsystem, als Gastsysteme zusätzlich u.a. DOS-basierte Betriebssysteme, Linux (ab Kernel 2.2), Solaris, NetWare und verschiedene BSD-Derivate. (Lizenz: Die abgespeckte VirtualBox-Open-Source-Edition (OSE-Version) wurde unter der GPL v2 veröffentlicht. Die volle Version mit speziellen Enterprise-Features wie iSCSI- und USB-Unterstützung sowie Unterstützung des Remote Display Protocol (RDP) ist proprietär.)
Homepage: `www.virtualbox.org/`

Virtual PC
gehört zum Funktionsumfang von Windows 7 und ist eine Implementierung des Vollvirtualisierungs-(Typ-2-)Konzepts. (Lizenz: Proprietär)
Homepage: `www.microsoft.com/windows/virtual-pc/`

1.5 Bedeutung der Virtualisierung

Der Einsatz der Servervirtualisierung bietet wesentliche Vorteile:

Serverkonsolidierung
Durch den massiven Zuwachs von Prozessorleistung und Arbeitsspeichergrößen entstanden zunehmend Situationen, in denen ein Gutteil der Rechnerkapazität ungenutzt blieb. Mit der Virtualisierung können Rechnerressourcen gezielt einzelnen virtuellen Betriebssysteminstanzen nach Bedarf zugewiesen und so optimal genutzt werden. Überkapazitäten lassen sich vermeiden, die vorhandenen Ressourcen können besser ausgelastet und Einsparungen bei Beschaffung, Infrastruktur und Unterhalt von Hardware erreicht werden, unter anderem durch Senkung der Anschluss-, Strom- und Wartungskosten. Moderne Stromsparkonzepte – Stichwort *Green IT* – in Rechenzentren werden so erst möglich. Darüber hinaus wird die Serverstruktur übersichtlicher und lässt sich besser verwalten.

Hardwareunabhängigkeit
Das Deployment und Provisioning von Servern wird durch die Hardwareunabhängigkeit virtueller Systeme wesentlich erleichtert. Unterschiede in der Systemarchitektur der verschiedenen Serverplattformen verlieren – zumindest für die Gastsysteme – weitgehend an Bedeutung. Das virtuelle System ist in einer Datei gekapselt, die leicht gesichert, verteilt und verschoben werden kann. Hardwareausfälle ziehen dadurch seltener eine Neuinstallation nach sich und haben – wie auch anstehende Wartungsarbeiten – geringere Ausfallzeiten zur Folge.

Schließlich sei noch eine (Nischen-)Anwendung erwähnt: Spezielle Legacy-Anwendungen, die nur auf einem inzwischen veralteten und sonst nicht mehr eingesetzten Betriebssystem laufen, können bei Bedarf immer noch in einer virtuellen Maschine ausgeführt werden.

Sicherheit
Lässt man Serverdienste isoliert voneinander in unterschiedlichen virtuellen Maschinen laufen, können die Prozesse nicht aus ihrer

Christoph Arnold / Michel Rode / Jan Sperling / Andreas Steil, KVM Best Practices, dpunkt.verlag, ISBN 978-3-89864-737-3

virtuellen Umgebung ausbrechen und andere beeinflussen. Die Auswirkungen eventueller Sicherheitsmängel bleiben auf eine virtuelle Maschine beschränkt und greifen nicht auf andere Dienste über.
Auf der anderen Seite können durch den Einsatz zusätzlicher Software in Form des Virtual Machine Monitor neue Sicherheitslücken entstehen, da der VMM ja Systemaufrufe der virtuellen Rechner weiterleitet und somit einen weiteren Angriffspunkt darstellt.

Verfügbarkeit durch Ausfallsicherheit

Wird ein Cluster mehrerer Rechnersysteme mit einer oder mehreren virtuellen Maschinen betrieben, kann der Ausfall von physikalischen Rechnersystemen abgefedert werden. Virtuelle Systeme können leicht auf ein anderes Rechnersystem verschoben werden, durch eine Live-Migration selbst bei laufendem Betrieb. Ebenso einfach können sie kopiert oder – etwa wenn Spitzenlasten auftreten – um weitere ergänzt werden. Gerade im Bereich der Hochverfügbarkeit (High Availability, HA) ist die Virtualisierung daher eine Schlüsseltechnologie.

So findet man Virtualisierung überall da, wo es auf Optimierung von Rechenleistung, Ausfallsicherheit, Flexibilität und Verwaltbarkeit auch großer Umgebungen ankommt, u.a. in Rechenzentren, bei Testsystemen und immer mehr in den neuen IT-Wolken, dem Cloud Computing.