

Der Computer als Applikation

Roland Herbst
herbst@cms.hu-berlin.de

Die Idee ist nicht neu

Die Technologie von virtuellen Maschinen wurde Ende der 60er Jahre eingeführt, um die Hardware der IBM-Mainframe-Großrechnersysteme zu partitionieren und somit für verschiedene Applikationen gleichzeitig nutzen zu können. Moderne Multitasking-Systeme wie z. B. UNIX standen zu diesem Zeitpunkt noch nicht zur Verfügung. Sie warteten noch auf ihre Entwicklung. In den 80er Jahren bis in die 90er Jahre hinein wurde die Mainframe-Architektur in Industrie- und Bildungseinrichtungen von UNIX-Servern oder Servern auf Basis von IBM-kompatiblen PCs verdrängt. Virtualisierung war in dieser Zeit nicht gefragt und somit geriet in diesen Bereichen das Thema in Vergessenheit.

Mit dem Aufkommen immer kostengünstigerer Hardware und der damit steigenden Performance am Arbeitsplatz wurde auf den PCs der Nutzer zunehmend Rechenleistung verschenkt. Gleichzeitig wurden die Systeme immer komplexer und waren damit schwerer zu administrieren. Durch diese steigende Komplexität und die zunehmende Nutzung von Internet-Technologien in den Applikationen wurden die Systeme immer anfälliger gegenüber Programmierfehlern.

Um dieser Entwicklung zu begegnen, besann man sich in den 90er Jahren deshalb zunächst innerhalb eines Forschungsprojektes an der Stanford University auf die Technologie der Virtualisierung. Die Ergebnisse dieser Forschungsarbeiten führten im Jahr 1998 zur Gründung der Firma VMware. Diese hat es sich zur Aufgabe gemacht, eine

Technologie der Virtualisierung für IBM-kompatible PCs zur Verfügung zu stellen.

Virtualisierungsprinzip

Unter Virtualisierung versteht man allgemein die Entkopplung des Betriebssystems von der darunter liegenden Hardware. Dieses wird dadurch erreicht, dass man zwischen Hardware und Betriebssystem eine Abstraktionsschicht schiebt, die dem Betriebssystem in den installierten Gastsystemen das Vorhandensein von echter Hardware vortäuscht (Abb. 1).

Man spricht von einem *Virtual Machine Monitor (VMM)*. Bisher ist diese Funktion komplett in Software implementiert, zukünftig wird sie in der Hardware der Prozessoren unterstützt werden. Da bekannte Angriffe, die auf Buffer Overflows basieren, von prozessorinternen Funktionen abgefangen werden, ergibt sich eine Erhöhung der Sicherheit des VMM.

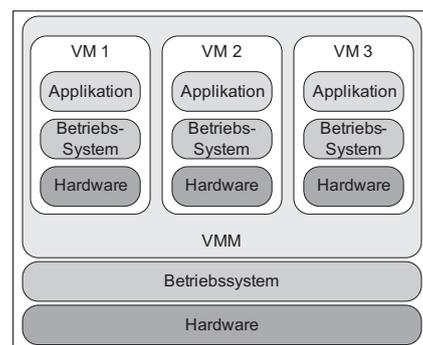


Abb. 1: Eine virtuelle Maschine ist eine spezielle Applikation. Diese wird Virtual Machine Monitor (VMM) genannt. In der Anwendung wird die Hardware eines IBM-kompatiblen PCs emuliert. In die virtuellen Maschinen hinein werden die Gastsysteme installiert.

Virtuelle Maschinen geraten immer mehr in den Mittelpunkt des Interesses der Anbieter und Nutzer von IT-Dienstleistungen. Was sind virtuelle Maschinen und wie funktionieren sie? Ist diese Frage beantwortet, folgt gleich die nächste: Lassen sich diese Technologien auch für die Anwendungen im Verwaltungsnetz einsetzen?

Die Produkte der Firmen *VMware* und *Microsoft* emulieren die Hardware eines IBM-kompatiblen PCs. Durch die Virtualisierung werden die Voraussetzungen geschaffen, dass auf einer Hardware verschiedene heterogene Betriebssysteme parallel und unabhängig voneinander genutzt werden können. Jede virtuelle Maschine besitzt dabei ihre eigene Hardware-Ausstattung (z. B. CPU, RAM, Netzwerkkarte). In diese virtuelle Maschine hinein wird das Gastsystem installiert. Das Gastsystem sieht dabei immer die Hardware eines IBM-kompatiblen PCs.

Was wird durch Virtualisierung erreicht?

Partitionierung

- Auf einem physikalischen System können gleichzeitig verschiedene Applikationen und Betriebssysteme genutzt werden, ohne dass sich die einzelnen Installationen gegenseitig beeinflussen können.
- Es besteht die Möglichkeit, verschiedene Server-Installationen zu konsolidieren.
- Die Rechenkapazität wird gebündelt und kann auf Anforderung kontrolliert den virtuellen Maschinen zur Verfügung gestellt werden.

Isolation

- Die virtuellen Maschinen sind vollständig vom Host-System und den anderen virtuellen Maschinen entkoppelt. Wenn eine Maschine abstürzt, sind die anderen nicht von diesem Crash betroffen.
- Zwischen den einzelnen virtuellen Maschinen gibt es keinerlei Datenverbindungen. Werden diese dennoch benötigt, kann man Verbindungen über das Netzwerk konfigurieren.

Verkapselung

- Die gesamte Umgebung der virtuellen Maschine wird in Dateien abgespeichert, sodass man diese leicht bewegen, kopieren und sichern kann.

Die virtuellen Maschinen werden auf dem Datei-System abgebildet. Dadurch

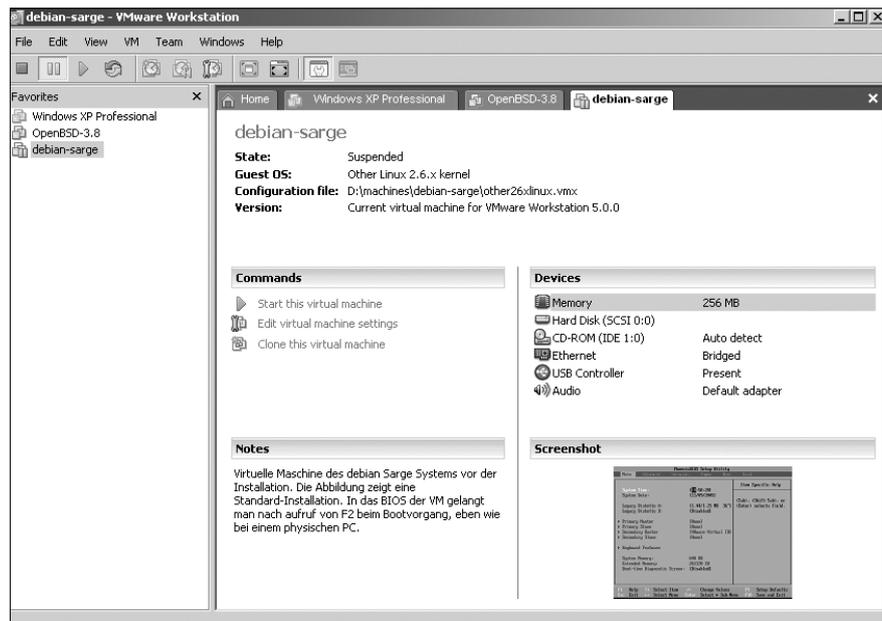


Abb. 2: VMware Workstation Version 5 in Aktion. Der Bootvorgang der virtuellen Maschine wurde angehalten (Pausen-Schalter im oberen Bereich der Abbildung). Dabei entsteht zur späteren Orientierung automatisch ein Snapshot des Bildschirmzustandes.

ist es sehr leicht möglich, Installationsstände zurückzusetzen, Systeme zu sichern und auf andere Maschinen zu transferieren, um sie anderen Nutzern zugänglich zu machen. Möglich wird dadurch die eigene Benutzer-Umgebung auf dem USB-Stick als virtuelle Maschine zum Mitnehmen.

VMware

VMware Workstation

Das wohl bekannteste Produkt dieser Entwicklung ist die *VMware Workstation*. Es handelt sich hier um eine PC-Applikation, die auf einer x86-Hardware laufend einen x86-PC emuliert. Die Installation dieser Software unterscheidet sich nicht von einer anderen Applikation. Der einzige Unterschied dabei ist, dass die Hardware eines x86-PCs emuliert wird (Abb. 2).

Wird eine solche virtuelle Maschine z. B. von einem dem Virenschanner unbekanntem Wurm oder Virus befallen, kann sie auf einfache Weise vom Netz genommen und heruntergefahren werden. Danach setzt man das System auf den Zustand vor dem Virenbefall zurück und beseitigt die Sicherheitslücke z. B. durch das Einspielen von Sicherheits-Patches

oder die Veränderung der Konfiguration der lokalen Firewall. Ist das System wieder okay, kann es mit dem nächsten Mausklick wieder mit dem Netzwerk verbunden werden und steht zur weiteren Nutzung bereit.

VMware GSX Server

Ein weiteres Produkt dieser Reihe ist der *VMware GSX Server*. Wie der Name schon vermuten lässt, ist diese Virtualisierungsanwendung stärker auf die Installation von Servern optimiert. Über die *VMware Virtual Machine Console* erhält der Administrator die Möglichkeit, die Server-Systeme remote zu administrieren. Dadurch wird die zentrale Administration von ganzen Server-Farmen von einem Arbeitsplatz aus ermöglicht.

Weitere Produkte sind der *VMware ESX Server*, das darauf aufbauende *VMware VirtualCenter* und *VMware ACE*, die hier nur erwähnt werden sollen. Weitere Informationen dazu findet man unter <http://www.vmware.com/>.

Virtualisierung im Verwaltungsnetz

Auch im Verwaltungsnetz wird diese Technologie seit Längerem angewendet. Am Beginn stand die Nutzung von

VMware Workstation am Arbeitsplatz. Diese ermöglicht es den Administratoren, neue Installationen zu entwickeln und zu erproben, ohne die eigentliche Arbeitsplatzumgebung verändern zu müssen. Es ist auf diese Weise möglich, auf einer x86-Hardware Windows- und Linux-Systeme gleichzeitig zu betreiben. Unter den Administratoren des CMS gehört diese Technologie mittlerweile zum Standard bei der Evaluierung von Anwendungen bzw. der Installation und Anpassung von Betriebssystemen. Zunehmend werden Server auf der Basis von virtuellen Maschinen realisiert (Abb. 3). Momentan kommt VMware GSX Server zum Einsatz, der Umstieg auf die ESX-Technologie wird derzeit evaluiert.

In Vorbereitung auf die Einführung des Windows-Netzwerkes der Verwaltung wurde eine Testumgebung benötigt. Die Realisierung erfolgte mit virtuellen Maschinen auf Basis eines VMware GSX Servers. Benötigt man eine weitere Testumgebung, so kann man diese durch Aufsetzen weiterer virtueller Server realisieren. Hierdurch erhält man die Möglichkeit, neue Software zu evaluieren und nur im Falle der Fehlerfreiheit auch auf den Produktionssystemen zu installieren. Ohne die Technologie der virtuellen Maschinen wäre ein solcher Testaufbau zu Hardware- und damit zu kostenintensiv. Ein weiterer Vorteil der Nutzung von virtuellen Maschinen besteht in der Möglichkeit, den Installationszustand zu einem bestimmten Zeitpunkt einzufrieren. Man spricht hier von der Erstellung eines Snapshots. Diese Snapshots sind gewöhnliche Dateien

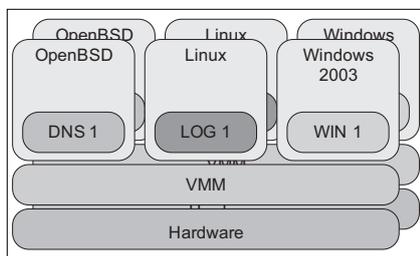


Abb. 3: Durch Nutzung von VMware GSX Servern können Anwendungen redundant zur Verfügung gestellt werden. Die einzelnen Systeme sind komplett voneinander abgeschottet. Verbindungen zwischen den Servern müssen wie bei Verwendung von separater Hardware über das Netzwerk konfiguriert werden.

und können deshalb auf andere Partitionen der Systeme kopiert und in ein Backup- oder Archiv-System übertragen werden. Bei Letzterem muss man den zu erwartenden Datenumfang beachten, da man mit solchen Snapshots die Kapazität der am Sicherungsvorgang beteiligten Systeme leicht überfordern kann. Dies betrifft insbesondere die Netzwerk-Anbindung. Es hat sich als sinnvoll erwiesen, die Server der VMM-Systeme mit Hardware-RAID auszustatten, entsprechend zu partitionieren und eine lokale Sicherung auf die Backup-Partition durchzuführen.

Das Xen-Projekt

Neben den kommerziellen Lösungen von VMware und Microsoft ist eine Reihe von Projekten im Open-Source-Bereich entstanden. Das momentan vielleicht interessanteste ist das Xen-Projekt. Dieses Projekt wird von einer Reihe namhafter Hersteller unterstützt und die Lösung steht unter der *GNU General Public License (GPL)*.

Xen ist ein *Virtual Machine Monitor* für x86-kompatible Computer, der an der Universität Cambridge entwickelt wird. Auch auf diesem VMM können x86-basierte Systeme parallel und voneinander unabhängig ausgeführt werden. Als Gastsysteme können momentan Linux, NetBSD, Plan 9 und FreeBSD genutzt werden. Die Gastsysteme müssen in den Quellen verfügbar sein, da sie an den Xen-Kernel speziell angepasst werden müssen, um die Virtualisierungsfunktionen zu unterstützen. Wie VMware kann Xen virtuelle Maschinen in einer sicheren Umgebung ausführen. Momentan unterstützt Xen auf Grund von lizenzrechtlichen Beschränkungen Microsoft Windows noch nicht direkt, eine Unterstützung der moderneren Windows-Systeme (XP, 2003) ist jedoch für die Zukunft geplant, wenn Virtualisierungstechnologien vom Prozessor direkt unterstützt werden. Will man Installationen mit Linux-Systemen virtualisieren, ist Xen schon zum jetzigen Zeitpunkt eine Alternative zu den im Artikel vorgestellten Beispielen. Man darf gespannt in die Zukunft schauen.

VMware Player

Das Argument zu hoher Kosten für Virtualisierungslösungen bei Desktop-Systemen verringert sich in zunehmendem Maße. Kurz vor dem Schreiben dieses Artikels wurde der VMware *Player* veröffentlicht. Er stellt die Basisfunktionen von virtuellen Maschinen zur Verfügung und ist für die Betriebssysteme Windows und Linux verfügbar. Genau wie die umfangreichere Workstation-Lizenz wird der VMware Player auf einem Windows- oder Linux-System installiert. Die Installation ist in wenigen Minuten erledigt und eine vorhandene virtuelle Maschine kann damit gestartet werden. Durch einen einfachen Mausklick ist es möglich, das Netzwerk-Interface der virtuellen Maschine vom Netzwerk zu trennen.

Die Abbildung 4 zeigt ein System bestehend aus einem VMware Player, in dessen Umgebung wiederum ein Xen-basierender VMM läuft. Zugegeben, dies ist ein eher akademischer Ansatz, aber er zeigt, dass in beiden VMM-Umgebungen die Virtualisierung konsequent umgesetzt worden ist.

Bei Beachtung der Lizenzbedingungen für die Gast-Systeme ist es nunmehr möglich, Anwendern virtuelle Maschinen fertig konfiguriert zur Verfügung zu stellen. Interessant ist diese Situation im Zusammenhang mit der Ausstattung von PC-Pools. Die Administratoren können z. B. für Lehrgänge fertig vorkonfigurierte virtuelle Maschinen installieren. Bisherig notwendige Lizenzen für die VMware Workstation entfallen dadurch.

Ausblick

Ein nächster Schritt wird die Unterstützung von Virtualisierungstechnologie im Prozessor sein. Ist der Virtual Machine Monitor bereits in der Hardware integriert, muss diese ressourcenintensive Operation nicht mehr in Software durchgeführt werden. Von AMD und Intel gibt es hierzu schon genaue Vorstellungen zur Umsetzung. Die ersten Modelle sollen in naher Zukunft verfügbar sein. Bei AMD läuft diese Technologie unter dem Codenamen »Pacifica« und Intel spricht

direkt von der »Virtualization Technology«.

Damit wird die komfortable Virtualisierung auf Servern und Arbeitsplatz-PCs ermöglicht. Microsoft hat in seiner Lizenzpolitik auf diese Entwicklung reagiert und kündigt an, dass die Serverlizenz der Enterprise-Version zukünftig nicht nur auf einem Server gilt [1].

Dadurch ergeben sich neue Möglichkeiten, die Sicherheit der Systeme zu erhöhen. Installationen verschiedener Sicherheitsstufen auf einer PC-Hardware können durchgeführt werden. Die Kommunikation zwischen den einzelnen Maschinen kann nur über Netzwerkverbindungen erfolgen. Ein weiteres Einsatzgebiet für lokale Firewall-Systeme deutet sich damit an.

Die Grenze zwischen den IT-Anwendungen und der Virtualisierung verschwimmt immer mehr. Schon bald werden Nutzer von PC-Systemen ganz normal mit virtuellen Maschinen umgehen, so wie es jetzt schon mit Textverarbeitung oder Webbrowser der Fall ist.



Abb. 4: Der Startvorgang des VMware Players unterscheidet sich nicht von der Workstation. Im oberen Bereich des Screenshots sind die unterstützten Geräte zu sehen.

Literatur

- [1] <http://www.microsoft.com/presspass/features/2005/oct05/10-rovirtualizationlicensing.mspix>
- [2] <http://enterprise.amd.com/Enterprise/serverVirtualization.aspx>
- [3] <http://www.cl.cam.ac.uk/Research/SRG/netos/xen/index.html>
- [4] <http://www.intel.com/technology/computing/vptech/index.htm>
- [5] <http://www.microsoft.com/windowsserversystem/virtualserver/default.mspix>
- [6] <http://www.vmware.com/>
- [7] <http://www.virtualization.info/>