Diplomarbeit

"Server- Virtualisierungslösungen im Vergleich"

ausgeführt zum Zweck der Erlangung des akademischen Grades einer/eines

„Diplom-Ingenieurin/Diplom-Ingenieurs für technisch-wissenschaftliche Berufe“

am Masterstudiengang Telekommunikation und Medien

der Fachhochschule St. Pölten

unter der Erstbetreuung von

DI Hans Mühlehner

Zweitbegutachtung von

DI Grischa Schmiedl

ausgeführt von

Christoph Lang-Muhr

tm071034

Ort, Datum

Unterschrift

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.

- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter oder einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Diese Arbeit stimmt mit der von den Begutachter/inne/n beurteilten Arbeit überein.

....

Ort, Datum Unterschrift

Zusammenfassung:

Durch die fortschreitende Entwicklung der Virtualisierungstechniken und dem Bestreben der Wirtschaft ihre Serverlandschaft effektiver auszunutzen, liegt Server- Virtualisierung momentan voll im Trend.
Es gibt eine Vielzahl von Lösungen zur Server-Virtualisierung auf dem Markt und es kommen laufend Neue dazu. Eine große Anzahl von Firmen und Open-Source-Projekten versucht die Aufmerksamkeit der Käufer bzw. Nutzer auf sich zu lenken.
Die Frage ist, welches Produkt für welche Anforderung der Server-Virtualisierung besser geeignet ist.

Diese Arbeit versucht diese Frage zu lösen indem sie Informationen über die Funktionsweise von Server- Virtualisierungslösungen gibt und auf spezielle Produkte eingeht.

Es wird dann im Speziellen auf die Virtualisierungslösungen:

- VMware ESXi
- Citrix XEN / Open Source XEN
- Microsoft Hyper -V

eingegangen. Die Produkte werden sowohl theoretisch als auch mittels einer exemplarischen Implementierung verglichen. Der praktische Teil der Arbeit soll es ermöglichen zusätzlich einen Vergleich der Leistung der einzelnen Systeme mit Hilfe der Durchführung von Benchmarks anzustellen.
Basierend auf diesen Ergebnissen wird eine Bewertung der Produkte abgegeben.

Abstract:

Through the progressive development of virtualization technologies and the desire of the economy to operate their servers more effectively, server virtualization is an upcoming market.

Today there is a wide variety of virtualization products on the market and new ones are constantly occurring. A large number of companies and open-source projects tries to catch the attention of the buyers and users.
The question is, which product meets the requirements of the server virtualization best.

This diploma thesis tries to solve this issue by providing information on the functioning of server virtualization solutions and looks into some specific products.

These products are:

VMware ESXi

Citrix XEN / Open Source XEN

Microsoft Hyper -V

The products were compared theoretically and via an exemplary implementation. The practical part of the document should allow a comparison of the performance of the individual systems. The practical comparison is done with benchmark programs.
Based on these results, an evaluation of the products will be made.

Inhaltsverzeichnis

1 Einleitung....1
1.1 Motivation....2
1.2 Ziel der Arbeit....3
2 Virtualisierung auf x86 Architekturen....4
2.1 Probleme beim Virtualisieren der x86 Architektur....6
2.2 Binary Rewriting (Full Virtualization)....8
2.2.1Funktion:....8
2.3 Paravirtualization....9
2.3.1Funktion....9
2.4 Hardware-Assisted Virtualization....11
2.4.1Funktion....11
2.5 Emulation....12
2.6 Virtualisierung auf Betriebssystemebene....14
3 Virtualisierung mittels eines Virtual Machine Monitor....17
3.1 VMM Type 1....18
3.2 VMM Type 2....20
4 Microsoft Server 2008 Hyper-V....22
4.1 Systemanforderungen und Features....23
4.2 Aufbau....28
4.2.1Parent Partition....29
4.2.2Hypervisor aware bzw. Enlightment....30
4.2.3Virtual Hard Disk (VHD)....33
4.2.4Netzwerk....34
4.3 Lizenzierung....35
5 VMware ESXi....36
5.1 Systemanforderungen und Features....37
5.2 Aufbau....41
5.2.1Vmkernel....42
5.2.2Prozesse außerhalb des Vmkernels („User World“)....44
5.2.3VMware Tools....45
5.2.4Prozessor und Hauptspeicher Zugriffe....46
5.2.5Netzwerk....47
5.2.6Massenspeicherzugriff....48
5.3 Lizenzierung....50
6 Citrix XenServer....52
6.1 Systemanforderungen und Features....53
6.2 Aufbau....56
6.2.1Domain 0....57
6.2.2Domain U....59
6.2.3HVM (Hardware Virtual Machine) Gast....60
6.2.4Netzwerk....61
6.2.5Storage....61
7 Vergleich der Produkte....63
7.1 Theoretischer Vergleich anhand der Funktionen....64
7.2 Aufbau der Testumgebungen....67
7.2.1Testhardware....68
7.2.2Konfiguration der VM's....69
7.2.3Benchmarks....69
7.3 Testumgebung des Microsoft Servers 2008 Hyper-V....74
7.3.1Installation....75
7.3.2Erstellen der virtuellen Maschinen....76
7.3.3Benchmarks ermittleln....78
7.4 Testumgebung des Vmware ESXi Servers....80
7.4.1Installation....80

7.4.2Erstellen der virtuellen Maschinen....83
7.4.3Benchmarks ermitteln....87
7.5 Teststellung des Citrix Xen Servers....89
7.5.1Installation....89
7.5.2Erstellen der virtuellen Maschinen....91
7.5.3Benchmarks ermitteln....95
7.6 Teststellung der nativen Systeme....96
7.6.1Auswertung der Benchmarks....96
7.7 Vergleich der Benchmarkergebnisse der Virtualisierungslösungen....98
8 Bewertung....101
9 Anhang....102
9.1 Anhang A: Literaturverzeichnis....102
9.2 Anhang B: Quellenangaben aus dem Internet....104
9.3 Anhang C: Abbildungsverzeichnis:....104
9.4 Anhang D: Verzeichnis der Tabellen....105

1 Einleitung

Server- Virtualisierung ist eine Software- oder Hardware-Technik die es ermöglicht, mehrere Instanzen eines oder verschiedener Betriebssysteme auf einem einzigen physikalischen Rechner gleichzeitig nebeneinander zu betreiben. Bei diesen Techniken können die Hardwareressourcen des Rechners auf die verschiedenen Instanzen nach Belieben aufgeteilt werden.
Die einzelnen Instanzen werden als virtuelle Maschine (im weiteren Dokument mit VM abgekürzt) oder Gast-System bzw. Gäste bezeichnet. Die VM verhalten sich in der virtuellen Umgebung identisch zum nativen Betrieb direkt auf der Hardware.

Der Gast wird von der Hardware abgekoppelt und kann somit wie ein Softwareobjekt flexibel und unabhängig von der physikalischen Hardware behandelt werden.

Die Virtualisierungslösung stellt der VM die Ressourcen, die für den Betrieb nötig sind zur Verfügung. Bei den Ressourcen, die auf die Gäste aufgeteilt werden, geht es vor allem um die vier Kernkomponenten

- CPU
- Hauptspeicher
- Festplattenspeicher
- Netzwerkanbindung

Diese zentralen Ressourcen werden in der Literatur auch „Core-Four“ genannt.

1.1 Motivation

Moderne Server haben oft viel mehr Rechenkraft als sie für ihre Aufgabe benötigen und daher ist die Auslastung des Systems meist sehr gering. Um diesen Umstand zu verbessern und die Server in den Betrieben besser auszulasten, steigen viele Firmen auf Server- Virtualisierung um. Der primäre Ansporn dieser Firmen ist es ihre Kosten zu senken.
Die wichtigsten Vorteile der Server- Virtualisierung :

- Reduzierung der Kosten durch weniger Server:
    - Bessere Ausnutzung der Rechner durch den Betrieb mehrerer Server auf einem physikalischen Server.
    - Es wird nicht mehr für jedes unterschiedliche Betriebssystem ein eigener Server benötigt.
- Schutz der Umwelt und Reduzierung der Kosten durch einen geringeren Stromverbrauch der IT- Infrastruktur.
- Es können eine große Anzahl an Testmaschinen für die Mitarbeiter einfach und schnell erstellt werden. Das ist ein wichtiges Argument für Entwickler die für verschiedene Plattformen entwickeln.
- Testen von Updates und Patches zuerst in einer VM bevor sie ins Produktiv System eingespielt werden.
- Günstige Alternative „one service per machine“ (ein Service pro Maschine) zu ermöglichen. Es muss nicht mehr für jeden wichtigen Dienst (z.B.: Mail- Server) ein eigener Server angeschafft werden. Jedes Service bekommt eine eigene VM und ist somit von allen anderen komplett isoliert. Durch diese Vorgehensweise steigt auch die Sicherheit, da man unsichere Dienste so auf eine eigene VM isolieren kann.
- Konsolidierung (=Vereinfachung und Flexibilisierung der Infrastruktur): der VM werden genau die für eine bestimmte Aufgabe benötigten Ressourcen zugewiesen. Ändern sich die Anforderungen werden die Ressourcen darauf angepasst, ohne die Hardware verändern zu müssen.

Aufgrund dieser Vorteile wird das Feld der Server- Virtualisierung immer wichtiger und in den nächsten Jahren wird eine Vielzahl von Betrieben einen großen Anteil ihrer IT-Infrastruktur auf Basis von Virtualisierung umstellen.

1.2 Ziel der Arbeit

Auf dem Markt gibt es zurzeit viele Lösungen zur Server-Virtualisierung und es kommen laufend Neue dazu. Eine große Anzahl von Firmen und Open-Source-Projekten bemühen sich um die Aufmerksamkeit der Käufer bzw. Nutzer.

Die Frage ist, welches Produkt für welche Anforderung der Server-Virtualisierung besser geeignet ist. Die vorliegende Arbeit versucht diese Frage zu lösen indem sie Informationen über die Funktionsweise von Server- Virtualisierungslösungen gibt und auf spezielle Produkte eingeht.

Diese Arbeit gibt zuerst eine Einführung in die Thematik der Server-Virtualisierung mittels Softwaretechniken und deren Funktionsweise. Es wird nur auf die Virtualisierung der x86 Architektur eingegangen, da sie die am weitesten verbreitete Technologie ist.
Nach der Einführung und Erläuterung der Technologien werden die folgenden 3 Virtualisierungslösungen im Speziellen untersucht:

- VMware ESXi
- Citrix XenServer
- Microsoft Hyper -V

Die Produkte werden sowohl theoretisch als auch mittels einer exemplarischen Implementierung verglichen. Der praktische Teil der Arbeit soll es ermöglichen zusätzlich einen Vergleich der Leistung der einzelnen Systeme mit Hilfe der Durchführung von Benchmarks anzustellen. Basierend auf diesen Ergebnissen wird eine Bewertung der Produkte abgegeben.

Das Ziel ist es zu zeigen welches Produkt für welche Anforderung der Server-Virtualisierung, nach den aufgestellten Kriterien, besser geeignet ist.

(vgl. itwissen 13.1.2009, 1, Server- Virtualisierung, http://www.itwissen.info/definition/lexikon/Servervirtualisierung-server-virtualization.html)
(vgl.: Rudolph 27.3.2008, 1, Virtualization 101, http://www.linux-mag.com/id/5508)
(vgl.: Robert Warnke, et al. 2008, S. 17)
(vgl.: Hantelmann 2007, S.104f)

2 Virtualisierung auf x86 Architekturen

X86 Architektur bezeichnet den Aufbau des Prozessors. Diese Architektur wurde von Intel Ende der 1970er Jahre eingeführt. Diese Art der Prozessoren wird heute in Desktops über Server, bis hin zu mobilen Geräten verwendet. Aufgrund ihrer weiten Verbreitung ist sie auch für die Virtualisierung interessant.

Es gibt mehrere Techniken zur Server- Virtualisierung, im Speziellen zur Prozessor Virtualisierung. Diese Techniken werden in diesem Kapitel näher beleuchtet. Zu Beginn dieses Kapitels wird die Speichervirtualisierung, Device und I/O Virtualisierung erläutert, denn ein Computer besteht nicht nur aus dem Prozessor alleine („Core Four“). Danach beschäftigt sich das Kapitel mit dem x86 Prozessor, welche Problem es gibt wenn man ihn virtualisieren will (siehe Kapitel 2.1 Probleme beim Virtualisieren der x86 Architektur, S. 6) und die Techniken zur Lösung dieses Problems.

Unabhängig von der eingesetzten Technik müssen Server- Virtualisierungslösungen folgende Anforderungen erfüllen (Popek und Goldberg 1974):

- Äquivalenz: Das virtualisierte System muss exakt dasselbe Verhalten an den Tag legen wie bei der Ausführung auf der physikalischen Hardware.
- Isolation: Die Isolation der virtualisierten Systeme (VM) muss untereinander gewährleistet sein, so dass Datensicherheit, Vertraulichkeit und Konsistenz von Daten und Zuständen garantiert werden kann. Eine instabile VM darf eine andere VM nicht zum Absturz bringen.
- Kontrolle: Die Hardwareressourcen müssen auf kontrollierte Weise den virtuellen Maschinen einzeln zugewiesen werden können.
- Effizienz: Die VM darf aufgrund der Virtualisierung keinen unangemessenen Overhead produzieren, sondern sollte annähernd so schnell laufen wie auf der physikalischen Hardware.

Aufgrund der Effizienzanforderung wurden viele sehr unterschiedliche architektonische Ansätze entwickelt, die unterschiedlichen Eigenschaften und verschiedene Leistungsfähigkeiten haben.

(vgl.: itwissen 13.1.2009, 1, Server- Virtualisierung, http://www.itwissen.info/definition/lexikon/Servervirtualisierung-server-virtualization.html)

Speichervirtualisierung

Speichervirtualisierung wird benötigt um den physikalischen Speicher des Hosts (Rechner auf dem die Virtualisierungssoftware läuft) auf die virtuellen Maschinen aufzuteilen, und wenn nötig, dynamisch zuzuteilen. Speicher zu virtualisieren ist relativ einfach. Der Speicher wird in die benötigten Teile partitioniert und wenn ein Speicherzugriff aus einer virtuellen Maschine erfolgt wird dieser Befehl auf den reservierten Bereich umgeleitet. Aus Sicht der virtuellen Maschine hat diese einen zusammenhängenden Adressraum zur Verfügung, der aber im physikalischen Speicher irgendwo liegen kann. Die Virtualisierungsschicht kümmert sich um die Übersetzung der internen Adressen des Arbeitsspeichers auf die realen Adressen des physikalischen Arbeitsspeichers und umgekehrt.

(vgl.: VMware 2007, S. 6f)
(vgl.: David Chisnall 2007, S. 5)

Device und I/O Virtualisierung

Wie bei der Speichervirtualisierung wird versucht die Hardware auf die virtuellen Maschinen aufzuteilen. Die Befehle der virtuellen Maschinen an die Hardware (Festplatten, Netzwerkkarten, Grafikkarten, usw.) werden abgefangen und an die reale Hardware weitergeleitet.

Es werden 2 Methoden verwendet:

- Für die virtuelle Maschine wird eine Standard Hardwarekomponente emuliert. Wenn sie darauf zugreift übernimmt die Virtualisierungsschicht die weiteren Schritte und stellt die benötigten Daten zur Verfügung. Ein Vorteil dieser Methode ist, dass man diese Maschine auf jedem beliebigen Host laufen lassen kann, da die Hardware für sie immer gleich ist. Nachteil der emulierten Hardware ist natürlich die niedrige Performance.
- Die zweite Methode ist „direct pass-through“. Dabei werden die Befehle direkt an eine reservierte Ressource durchgereicht.

(vgl.:: VMware 2007, S. 7)
(vgl.: David Chisnall 2007, S. 5f)

2.1 Probleme beim Virtualisieren der x86 Architektur

Ein x86 Betriebssystem ist ausgelegt direkt auf der Hardware zu laufen. Daher nimmt es auch an, dass die komplette Hardware ihm alleine zur Verfügung steht. Die x86 Architektur hat 4 Sicherheitsstufen für den Zugriff auf die Hardware. Die Sicherheitsstufen werden Ring 0, 1, 2 und 3 genannt, wobei Ring 0 (auch Kernel Mode genannt)die meisten Privilegien hat und diese bis Ring 3 (ab Ring 0 auch User-Mode genannt) immer weiter beschränkt werden (*siehe Abbildung 1*). Das Betriebssystem wird normalerweise im Ring 0 ausgeführt, da es direkten Zugriff auf Speicher und sonstige Hardware benötigt. Applikationen laufen meist im Ring 3.

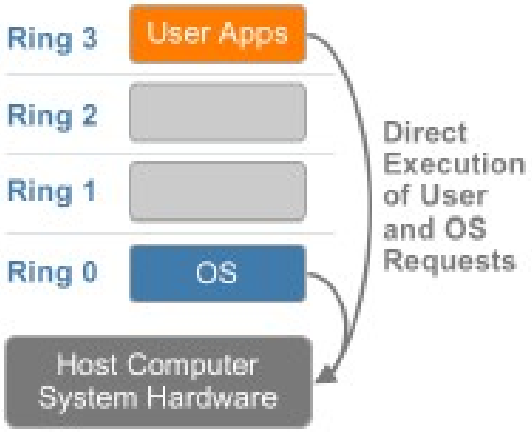

Abbildung 1: Schema der Ringarchitektur (vgl.: Vmware 2007, S 3)

Wenn man die x86 Architektur virtualisieren will, muss man versuchen, eine Virtualisierungsschicht unter dem Betriebssystem einzuziehen, welches dann aber noch immer glaubt, dass es im Ring 0 läuft. Diese Schicht ist dann für die Erstellung und Verwaltung der virtuellen Maschinen und die Verteilung der Hardwareressourcen verantwortlich.

Das Schwierige daran war die Befehle der Virtuellen Maschinen abzufangen und in der Laufzeit so zu verändern, dass es das Gast Betriebssystem nicht merkt. Alle Befehle, die die Konfiguration einer Ressource verändern, müssen im Ring 0 ausgeführt oder abgefangen werden. Es gibt einige Befehle (z.B.: einige Speicher Funktionen) die nicht abgefangen werden können, ohne dass das Gast Betriebssystem etwas merken würde.

Es haben sich primär 3 Lösungen entwickelt

- Binary Rewriting
- Paravirtualisierung
- Hardware- Assisted Virtualization

Diese Lösungen werden nachfolgend näher behandelt.

Sie finden vor allem in den Virtualisierungslösungen mittels Virtual Machine Monitor (VMM) Anwendung. (siehe 3.Virtual Machine Monitor, S. 17)

Weiters gibt es auch andere Lösungen die aber andere Ziele haben als speziell die x86 Architektur zu virtualisieren, daher sind die beschriebenen Probleme dort nicht zu finden. Aber aufgrund der Verbreitung dieser Lösungen sollten sie in diesem Dokument erwähnt werden.

- Emulation
- Virtualisierung auf Betriebssystemebene

(vgl.: David Chisnall 2007, S. 9)
(vgl.: VMware 2007, S. 3)

2.2 Binary Rewriting (Full Virtualization)

Diese Technik wurde vor allem von der Firma VMware verbreitet .In der Literatur wird sie auch „Binary Translation“ oder „Native Virtualization“ genannt. Sie erlaubt, dass ein Großteil der virtuellen Umgebung im User- Mode laufen kann. Es treten aber Geschwindigkeitseinbusse im Vergleich zum nativen Betrieb auf.

2.2.1 Funktion

Bei dieser Technik werden die Befehle des Gast Betriebssystems von der Virtualisierungsschicht gescannt und Befehle die im Kernel Mode ausgeführt werden müssen heraus gefiltert werden. Die restlichen User Mode Befehle werden direkt am Prozessor ausgeführt um die Performance zu steigern.
Befehle für den Ring 0 werden dann so umgeschrieben, dass sie den erwarteten Effekt auf die virtuelle Hardware des Gastes haben.

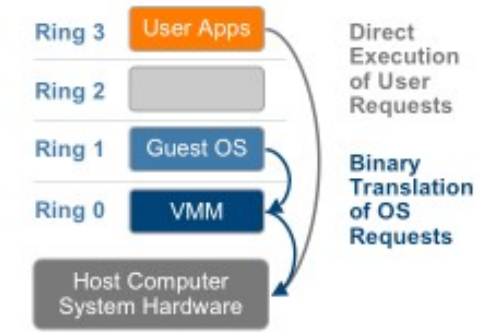

Abbildung 2: Binary Rewriting (vgl.: VMware 2007, S. 4)

In der Abbildung 2 kann man erkennen, dass die Befehle des Gast Betriebssystems zuerst in der Virtualisierungsschicht umgewandelt werden (in der Abbildung 2 VMM genannt) und von dieser dann erst an die eigentliche Hardware weitergegeben werden. Ein Systemcall (Befehl an die Hardware) wird vom Guest OS (Gast Betriebssystem) ausgeführt. Dieser Befehl wird dann von dem VMM abgefangen, wenn er einen kritischen Bereich der Hardware betrifft und in einen anderen Befehl umgewandelt. Nach der

Ausführung dieses Befehls, der vom VMM ausgeführt wurde, erhält das Guest OS die angeforderten Daten seines Befehls.
Ebenfalls ersichtlich ist die direkte Ausführung von Befehlen aus dem User- Mode.

Die Virtualisierungsschicht stellt jedem Gast Betriebssystem alle Services eines physikalischen Systems zur Verfügung. Dabei sind ein virtuelles BIOS, virtuelle Devices und virtuelles Speichermanagement enthalten.

Das einzige Problem ist, dass die Performance unter dieser Technik leidet. Vor allem I/O intensive Anwendungen sind dadurch merklich langsamer als im nativen Betrieb des Betriebssystems. Die Geschwindigkeit liegt meist zwischen 80-97%.

Durch die Kombination von Binary Rewriting und Direct Execution wird die virtuelle Maschine komplett von der darunter liegenden Hardware, durch die Virtualisierungsschicht, abstrahiert. Das Gast Betriebssystem weiß nicht, dass es in einer virtuellen Umgebung läuft und daher benötigt es keine Modifikationen um virtualisiert zu werden. Ein großer Vorteil dieser Technik ist, dass sie ohne Hardware Unterstützung seitens des Prozessors auskommt.

(vgl.: David Chisnall 2007, S. 10)
(vgl.: VMware 2007, S. 4)

2.3 Paravirtualization

Bei der Technik der Paravirtualisierung wird anders an das Problem herangegangen. Hier wird nicht die Frage gestellt „Wie kann man die x86 Architektur komplett virtualisieren?“, sondern: „Welches System, das man virtualisieren kann, ist dem x86 System am nächsten?“. Statt sich mit den problematischen Befehlen auseinanderzusetzen werden sie bei dieser Technik ignoriert.

2.3.1 Funktion

Bei dieser Technik muss der Kernel (=Betriebssystem- Kern) des Gast Betriebssystems angepasst werden. Er wurde in dieser Form angepasst, dass die Befehle, die zu Problemen, führen durch Hypercalls ersetzt wurden. Das Gast System läuft im Ring 1 anstatt im Ring 0. In diesem Ring darf es keine Befehle für den Kernel Mode ausführen, aber eben die Hypercalls. Ein Hypercall ist vergleichbar mit einem System Call (Befehl an des Betriebssystem der im privilegierten Modus, Ring 0, ausgeführt wird).

In der Abbildung 3 sieht man den Unterschied zwischen der Ausführung eines Befehls in einem nativ installierten Betriebssystem und im Gegensatz dazu in einer paravirtualisierten virtuellen Maschine.
Im nativen Betrieb geht der Befehl direkt an den Kernel des Betriebssystems und wird ausgeführt. Beim paravirtualisierten System geht der Befehl zuerst zur Virtualisierungsschicht (hier Hypervisor genannt), dann erst zum Kernel des Gast Betriebssystems.
Weiters gibt es auch noch die Möglichkeit direkte System Calls zu tätigen (Accelerateed System Calls in der Abbildung), die dann einen Hypercall auslösen. Aber dazu sind noch weitere Modifikationen im Gast Betriebssystem notwendig.

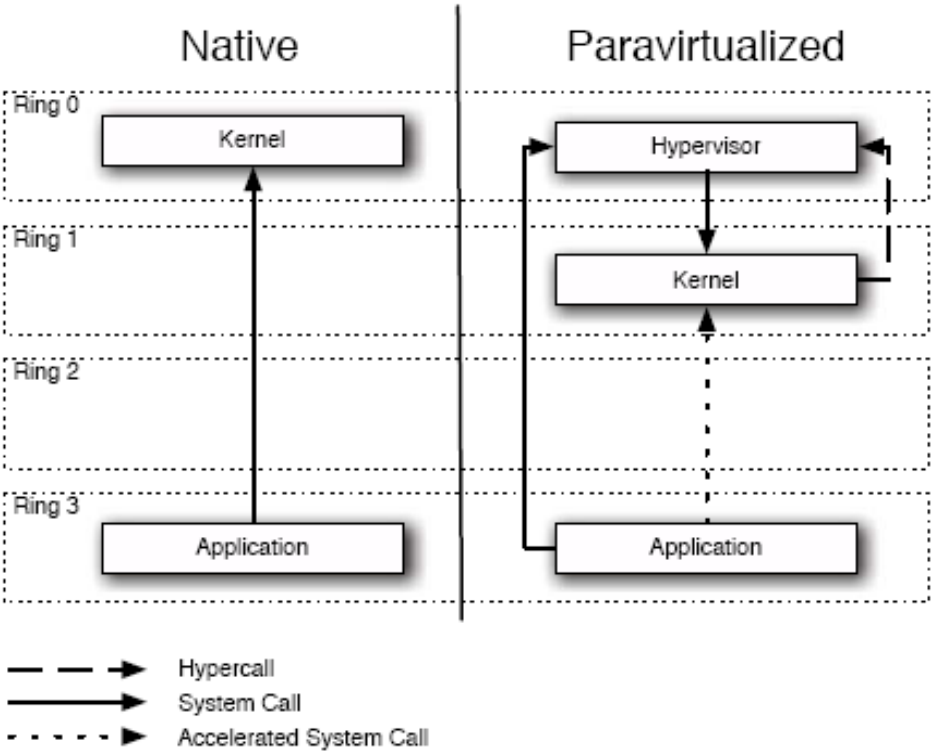

Abbildung 3: System call- Native versus Paravirtualiserten Umgebung (vgl.:Chisnall 2007, S 12)

Der Unterschied zum Binary Rewriting ist, dass bei dieser Technik das Gast Betriebssystem weiß, dass es in einer virtuellen Umgebung läuft. Ein großer Vorteil ist der kleinere Virtualisierungs- Overhead bei dieser Lösung. Es ist einfacher, ein Betriebssystem anzupassen, als das Binary Rewriting zu realisieren.

Ein Nachteil, der sich aus diesem Konzept ergibt, ist, dass keine unmodifizierten Gäste in dieser virtuellen Umgebung laufen können.

(vgl.: VMware 2007, S. 5)
(vgl.: David Chisnall 2007, S. 10f)
(vgl.: Hantelmann 2007, S.106)

2.4 Hardware-Assisted Virtualization

Die großen CPU Hersteller AMD und Intel haben ihren aktuellen Prozessoren (seit 2006) zusätzlich Funktionen hinzugefügt um Virtualisierung einfacher zu machen. Bei Intel wird die Technologie „Intel Virtualization Technology (VT-x)“ genannt und bei AMD „AMD-V“.

2.4.1 Funktion

Bei beiden Herstellern wurde eine neue Sicherheitsstufe eingeführt die unter dem Ring 0 liegt, man könnte sagen Ring -1. Dieser neue Ring beheimatet nun die Virtualisierungsschicht und erlaubt dem Gast Betriebssystem im Ring 0 zu laufen. Dadurch werden privilegierte Befehle der VM automatisch abgefangen und in der Virtualisierungsschicht verarbeitet, was den Gebrauch von Binary Rewriting und Paravirtualisation theoretisch unnötig macht. In der Abbildung 4 sieht man wie sich der neue Ring in die Struktur einfügt.

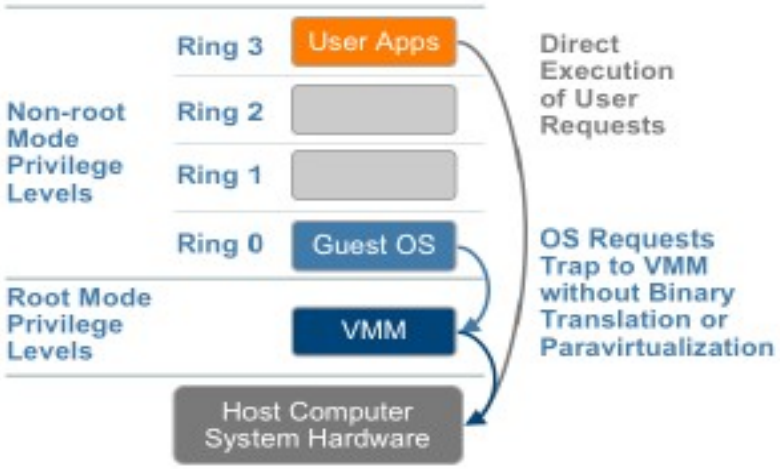

Abbildung 4: Hardware unterstützte Virtualisierung beim x86 (vgl.:VMware 2007, S6)

Der Weg eines Systemcalls geht bei dieser Technik vom Guest OS zum VMM und dann erst zur Hardware. Hier muss sich der VMM nicht um das Abfangen des Systemcalls kümmern, da er durch die geänderte Struktur automatisch abgefangen wird. Nachdem der VMM den Systemcall ausgeführt hat, liefert er dem Guest OS die angeforderten Daten.

Es gibt noch weitere Neuerungen in diesen Prozessoren z.B.: die „Virtual Machine Control Structures“ (VT-x) oder die „Virtual Machine Control Blocks“ (AMD-V). In diesen Strukturen können die Zustände der Gast Betriebssysteme gespeichert werden. Die meisten Virtualisierungslösungen verwenden bereits teilweise diese Technologie als Ergänzung zu ihren bestehenden und ausgereiften Technologien. Jetzt wird meist eine Hybridlösung eingesetzt aus Binary Rewriting oder Paravirtualisierung und der Hardware unterstützten Virtualisierung (z.B.: siehe 6 Citrix XenServer 5, S. 52)

(vgl.: VMware 2007, S 6)
(vgl.: David Chisnall 2007, S. 13f)

2.5 Emulation

Emulation bedeutet, dass eine komplette Rechnerhardware (einschließlich der CPU) simuliert wird. Dazu wird unter anderem der komplette Befehlssatz des Gast-Prozessors mit Hilfe des Host-Prozessors nachgebildet.

Durch diese simulierte CPU wird es möglich, Betriebssysteme und Anwendungen die für eine andere Hardware ausgelegt sind, auszuführen. Dies erlaubt die Ausführung eines x86-Betriebssystems wie z.B.: OS/2 auf einer anderen Architektur z.B.: SPARC.

(vgl. Hantelmann 2007, S. 105)

(vgl.: Robert Warnke, et al. 2008, S. 19)

Die Software-Schicht setzt dabei, wie jedes andere Programm auch, direkt auf das Betriebssystem auf. Diese Schicht emuliert die komplette Hardware für das Gast Betriebssystem. Von der Sicht des Gastes ist der Emulator die Hardware.

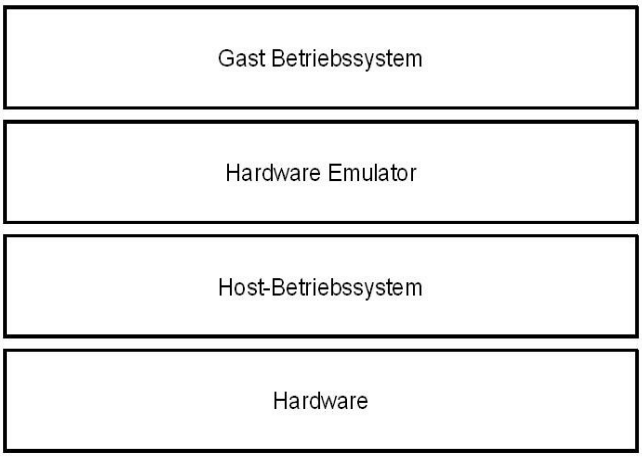

Abbildung 5: Darstellung der Schichten bei Verwendung einer Emulationssoftware

Vorteile:

Nur mit Hilfe der Emulation ist es möglich fremde Architekturen virtuell bereitzustellen. Dies wird teilweise verwendet um nicht mehr verfügbare Systeme nachzubilden. Ein weiterer Vorteil ist, dass man auch für eine andere Architektur Software entwickeln bzw. testen kann, ohne diese dabei als Entwicklungsrechner verwenden zu müssen. z.B.: Entwicklung einer Software für die Sparc Prozessoren auf einer handelsübliche x86 Hardware.

Nachteile:

Es wird eine vielfach höhere Systemleistung des Host-Systems benötigt als für das Gast-System notwendig wäre. Selbst bei günstigen Voraussetzungen erreicht ein emuliertes System nur 10% der Leistungsfähigkeit im Vergleich zur nativen Installation auf dem Host-System. Der Grund ist, dass jeder CPU-Befehl eines Gast-Systems in einen entsprechenden Befehl der CPU des Host-Systems übersetzt werden muss.
Bei der Emulation von älterer Hardware ist das meist kein Problem, da das emulierte System, aufgrund der aktuellen Hardware, meist schneller als das originale System ist.
Ein weiterer Nachteil ist, dass es keine dynamische Ressourcenverwaltung gibt. Daher ist die Konfiguration der emulierten Systeme starr, das bedeutet, während der Laufzeit können die Ressourcen den Gast-Systemen nicht variabel zugeteilt werden.

(vgl. Hantelmann 2007, S. 106)
(vgl.: Robert Warnke, et al. 2008, S. 18)

Die Emulation von kompletten Systemarchitekturen wird im Feld der Server-Virtualisierung nicht eingesetzt, da in erster Linie die Geschwindigkeit zu gering ist. Sie kann in diesem Anwendungsfeld auch nicht ihre Vorteile ausspielen, da der Großteil der Software für x86 Architektur vorhanden ist.

Beispiele für Emulatoren:

- Qemo: Es emuliert x86-, x86-64-, AMD64-, Power PC- und SPARC32/64-Architekturen. Weiterhin wird an der Unterstützung für Alpha, ARM, S390, IA-64, m68k und MIPS entwickelt.
- Bochs: Es emuliert x86- und AMD64 Architekturen

2.6 Virtualisierung auf Betriebssystemebene

In der Literatur wird auch oft der Begriff Betriebssystemvirtualisierung oder O/S Virtualization verwendet. Bei dieser Art der Virtualisierung wird nicht die vorhandene Hardware unter den Gästen aufgeteilt, sondern das Betriebssystem. Das bedeutet, dass sich mehrere Instanzen einen Kernel teilen. Bei dieser Technik wird also das Betriebssystem virtualisiert und nicht die Hardware. Es wird eine Abstraktionsschicht über das Host- Betriebssystem gelegt.

Diese Schicht erzeugt Instanzen des Host-Betriebssystems. Daher haben die Gast-Systeme den gleichen Kernel wie das Host-System. Man könnte sagen jeder Gast ist fast wie ein virtueller „Schnappschuss“ der Software des Hosts. Natürlich kann dann jeder Gast individuell angepasst werden.
Bei der Erstellung der Gäste werden nur die abweichenden Daten der Instanz von dem Host- System angelegt. Alle Betriebssystemdaten, z.B.: Bibliotheken des Betriebssystems, die alle Instanzen benötigen, werden vom Host-System den Gästen zur Verfügung gestellt. Die abweichenden Daten werden im Home- Verzeichnis der Instanz gespeichert. Diese Architektur hat folgendes zur Folge: Wenn man eine Datei auf dem Host- System ändert, werden zugleich alle mit ihr verknüpften Dateien innerhalb jeder virtuellen Maschine geändert. Bei der Betriebssystemvirtualisierung wird das gemeinsame Basisbetriebssystem zu einem Punkt zentraler Kontrolle für alle virtuellen Maschinen (Instanzen).

Aufgrund dieser Technik ist eine Instanz des Host- Systems sehr klein und besteht in der Regel nur aus wenigen Dateien. Daher verbraucht diese Art der Server-Virtualisierung deutlich weniger Festplatten- und Hauptspeicher als ein nativ (direkt auf der Hardware) installiertes Server Betriebssystem bzw. eine komplette Installation des Betriebssystems in einer virtuellen Maschine. Durch die Tatsache, dass keine Hardware emuliert werden muss, kann die Performance weiter gegenüber den anderen Arten der Virtualisierung gesteigert werden.

In der nachfolgenden Abbildung sieht man wo die Softwareschicht, die die weiteren Instanzen des Host- Betriebssystems erzeugt, liegt.

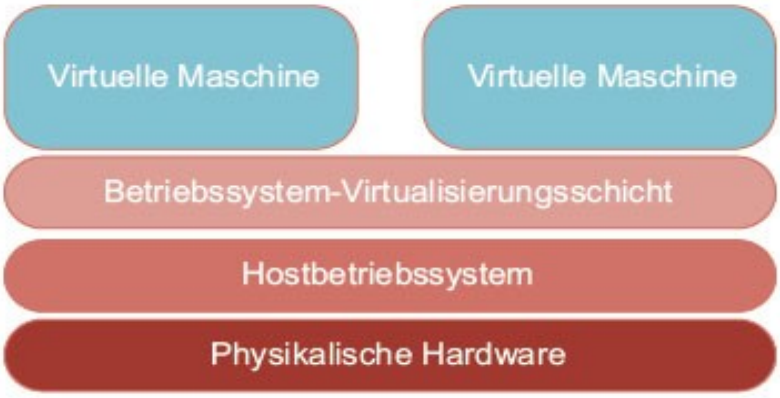

Abbildung 6: Darstellung der Schichten bei Verwendung von Virtualisierung auf Betriebssystemebene (vgl: Shields 2007, S 6)

Vorteile:

- Hohe Auslastung der Serverhardware durch eine große Anzahl an Gästen (größer Faktor zehn im Vergleich mit der Virtualisierung mittels VMM)
- Niedrige Leistungseinbussen durch Virtualisierung (nur 1% bis 3 %)
- geringe Systemressourcen pro Gast benötigt
- große Hardwareunterstützung (z.B.:Solaris oder Linux als Host- System)
- flexible Anpassung der Gasthardware möglich
- Nutzung von Teilen des Host-Betriebssystems
- optimierter Zugriff auf die virtuelle Hardware durch das Gast-Betriebssystem

Nachteile:

- Diese Technik lässt sich nur in homogenen Umgebungen anwenden, da alle Gast-Systeme gleich dem Host- System sind
- Aus dem Gast heraus können keine anderen Treiber oder Kernel geladen werden
- Ein Gast- System kann denn kompletten Server zum Stillstand bringen da das System nicht komplett isoliert ist.
- Eine Live-Migration (= Umzug der virtuellen Maschine auf einen anderen Host ohne Unterbrechung des Betriebs) ist nicht möglich, da der Kernel des Host-Systems nicht umziehen kann
- Betriebssystem-Updates des Hosts wirken sich auf den Gast aus

Beispiele für Virtualisierung auf Betriebssystemebene:

- Solaris-Zones
- BSD-Jails
- Linux-VServer
- Paralles (früher Virtuozzo)

(vgl.: Robert Warnke, et al. 2008, S. 19)
(vgl. Zimmer 7.1.2009, 1, FAQ- Virtualisierung,
http://wiki.computerwoche.de/doku.php/virtualisierung/faq-virtualisierung)
(vgl: Shields 2007, S 5f)

Diese Art der Virtualisierung wird in dieser Arbeit nicht mehr näher beleuchtet da sie zwar sehr interessant ist aber nur für spezielle Anwendungszwecke sinnvoll ist. Ein wichtiger Einsatzzweck dieser Technik ist die Bereitstellung von dezidierten- Servern in der Webhosting Branche (= Virtueller Webserver auf dem der Mieter alle Rechte hat). Diese Arbeit konzentriert sich aber, wie in der Einleitung bereits erwähnt, auf die Virtualisierung von unterschiedlichen Betriebssystemen.

3 Virtualisierung mittels eines Virtual Machine Monitor

In der Literatur wird der Begriff Virtual Machine Monitor (im weiteren Dokument mit VMM abgekürzt) auch unterschiedlich verwendet. Meist wird er als Synonym für den Begriff Hypervisor benutzt. Einige Quellen hingegen verwenden den Begriff Hypervisor nur für den VMM Type 1 (siehe 3.1 VMM Type 1, S.18).

Der VMM ist das am meisten genutzte Virtualisierungskonzept in der Praxis.
VMM wird die Abstraktionsschicht genannt die zwischen Gast- System und der Hardware liegt. Diese Schicht virtualisiert die Systemressourcen und stellt sie der VM zur Verfügung. Ebenso ist sie für die Steuerung der VM zuständig. Im VMM werden meist die Techniken Binary Rewriting, Paravirtualisierung und Hardware-Assisted Virtualization eingesetzt. Welche von den Techniken oder Kombinationen verwendet wird hängt vom jeweiligen Produkt ab.

Bei der Virtualisierung mittels VMM wird zwischen zwei unterschiedlichen Architekturen unterschieden, den Type 1 und den Type 2. Die Einteilung erfolgt über die Position der Schicht in Relation zur virtualisierten Hardware.

- Type 1 VMM läuft direkt auf der Hardware, es wird kein eigenes Host Betriebssystem benötigt.
- Type 2 VMM läuft auf einen Host- Betriebssystem das ihm verschiedene Services liefert wie z.B.: I/O Geräte, Speicher Management,...

(vgl.:Segor, 2008, S 128f)
(vgl.: IBM, 2005, S. 2f)

3.1 VMM Type 1

Der VMM vom Type 1 ist eine dünne Schicht die direkt auf der Hardware sitzt. Daher wird sie in der Literatur auch als „Bare Metal Hypervisor“ bezeichnet. Der VMM ist für die Aufteilung und Zuteilung der „Core Four“ und der restlichen Hardwareressourcen zuständig. Die VM laufen über dem VMM *siehe Abbildung 7*

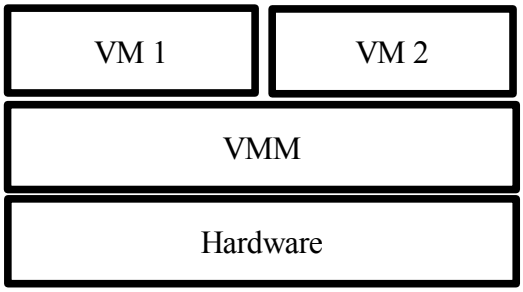

Abbildung 7: VMM Type 1

Es gibt 2 Arten dieses VMM:

- Microkernelized VMM
- Monolithic VMM

Der Unterschied liegt im Aufbau des VMM *siehe Abbildung 8*

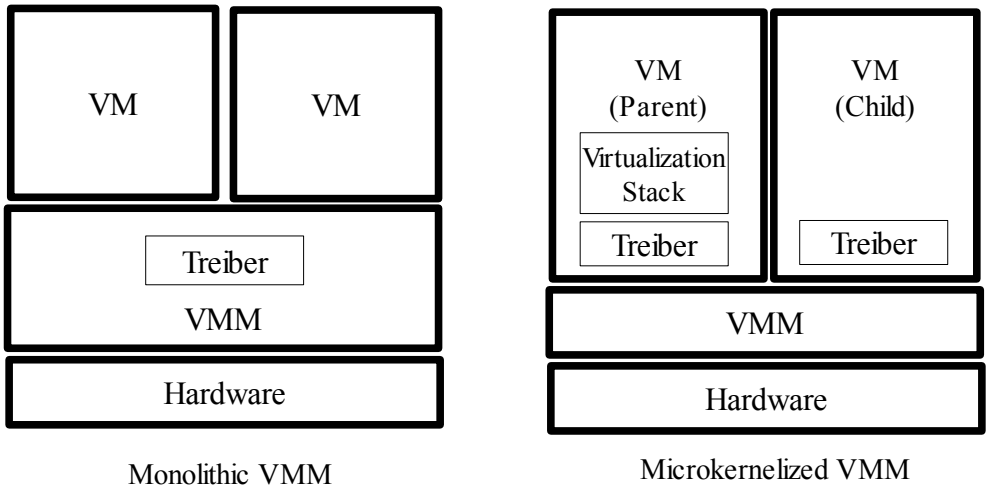

Abbildung 8: Monolithic VMM versus Microkernelized VMM

Beim Monolithic VMM liegen die Treiber die für die Kommunikation mit der Hardware notwendig sind direkt im VMM. Die Bereitstellung und Aufteilung der Hardwareressourcen übernimmt alleine der VMM. Diese Architektur bringt natürlich Vor- und Nachteile.

Vorteile:

- Durch diese Architektur können die VM direkt über den VMM auf die Hardware zugreifen, was aus Sicht der Performance eine gute Lösung ist.
- Es wird keine Parent VM (oder DOM 0 bei Xen) benötigt

Nachteile:

- Diese Treiber müssen speziell für den VMM geschrieben werden, daher wird nur eine kleine Anzahl an Hardware unterstützt.

Beim Microkernelized VMM gibt es immer eine Parent VM (VM mit höheren Privilegien). Die Treiber für die Hardware sind nicht in der VMM integriert sondern liegen in der Parent VM bzw. in den einzelnen VM's.
Aufgrund dieser Architektur ist der VMM nur für die Bereitstellung und Aufteilung des Prozessors und des Speichers zuständig. Er braucht sich nicht um andere Hardwareressourcen kümmern, wie z.B.: Festplatten, Ethernet,usw... . Diese Ressourcen werden von der Parent VM verwaltet und wenn notwendig an die anderen VM aufgeteilt bzw. als virtuelles Gerät bereitgestellt. Die Parent VM ist auch für die Verwaltung der VM's zuständig.

Die Implementation der Parent VM ist von Produkt zu Produkt unterschiedlich. Daher wird sie in diesem Dokument bei den jeweiligen Softwarelösungen erläutert.

Vorteile dieser Architektur:

- Es können Standard Treiber der Parent VM verwendet werden. Daher wird bei den meisten Produkten eine große Anzahl an Hardware unterstützt.
- Der VMM ist frei vom Code von Drittanbietern zur Unterstützung der Hardware, daher kleiner und sicherer.
- Es ist möglich die VM's direkt auf dem Server zu verwalten.

(vgl. Savill 2008, S 1285 f)
(vgl.: Chisnal 2008, S 19)

3.2 VMM Type 2

Dieser Typ wird in der Literatur auch „Hosted Virtual Machine Manager“ genannt. Bei diesem Typ liegt der VMM nicht direkt auf der Hardware sondern auf dem Host Betriebssystem, *siehe Abbildung 9.*

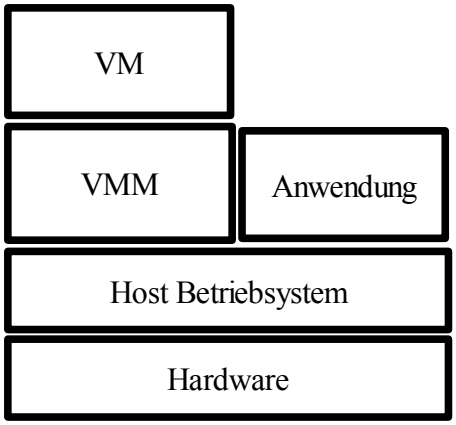

Abbildung 9: VMM Type 2

Der VMM läuft als Anwendung im Host Betriebssystem. Daher ist die Performance schlecht, denn jeder Hardwareaufruf der VM geht über den VMM, dann zum Host Betriebssystem, von diesem zum Device Treiber, dann zur Hardware und nach dieser Prozedur natürlich den ganzen Weg in umgekehrter Reihenfolge wieder zurück.
Der Unterschied zu einer Emulationssoftware ist, dass nicht alle Hardwarekomponenten emuliert werden, z.B.: der Prozessor. Beim VMM Type 2 werden nur einzelne Hardwarekomponenten wie Netzwerkadapter usw. emuliert.

Microsoft hat diesen Ansatz weiterentwickelt und den „Hybrid VMM“ geschaffen. Bei dieser Art des VMM Type 2. läuft der VMM nicht über dem Host Betriebssystem sondern daneben.

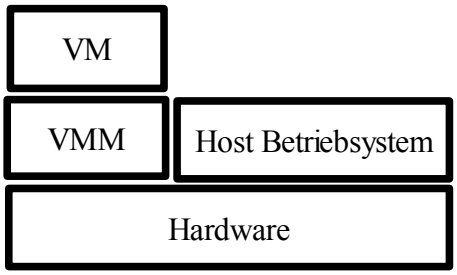

Abbildung 10: Hybrid VMM

Das Host System und der VMM laufen beide im Kernel Modus und haben so beide Anrecht auf die Hardwareressourcen. „Das letzte Wort“ bei der Vergabe der Ressourcen, hat aber das Host Betriebssystem, denn es kontrolliert die komplette Hardware.
Durch diese Architektur kann man den Performanceverlust ein wenig aufheben, aber es ist noch immer um ein Vielfaches langsamer als ein VMM vom Type 1.

(vgl. Savill 2008, S 1284 f)
(vgl.: Microsoft 2008, S 6)

Der VMM Type 2 wird vor allem für Testzwecke verwendet da die Virtualisierungslösung als Anwendung installiert wird und das Host Betriebssystem auch normal genutzt werden kann. Die Performance ist im Vergleich zum VMM Type 1 wesentlich geringer da der Overhead eines Host Betriebssystem gegeben ist. Daher wird dieser Type nur in Ausnahmezwecken zur Server- Virtualisierung verwendet. Die häufigste Anwendung findet er bei der Erstellung von Testumgebungen.

In der Dokumentation von Microsoft wird diese Art des VMM auch Hybrid VMM genannt, da sie den Ausdruck VMM Type 2 für Laufzeitumgebungen wie JVM (Java Virtual Machine) oder CLR (Common Language Rundtime) verwendet.

4 Microsoft Server 2008 Hyper-V

Windows Server Hyper-V ist die Hypervisor- basierte (VMM vom Type 1) Virtualisierungsfunktion von Microsoft und wurde im Juni 2008 veröffentlicht.
Die Virtualisierungssoftware ist ein Bestandteil von den meisten Windows Server 2008 Editionen und somit fast jedem Anwender des Betriebssystems unmittelbar zugänglich.
Die Installation erfolgt als Server-Rolle und das Management über die MMC (Microsoft Managment Console).

Als Alternative zum kompletten Windows Server 2008 gibt es seit 1.10.2008 den Hyper-V Server. Dieser kann kostenlos von der Microsoft Site heruntergeladen werden. Dahinter steckt ein abgespeckter Windows Server 2008 (Windows Server 2008 Core) auf dem die Hyper-V Rolle installiert ist. Er beinhaltet keine grafische Oberfläche und nur ein minimales Interface auf der Kommandozeile zum Verwalten des Servers.
Um mit der Virtualisierungsfunktion arbeiten zu können benötigt man ein „MMC Snap In“ (= Microsoft Management Console) auf einem Windows Server 2008 oder einen Rechner mit Windows Vista mit Servicepack 1 auf dem man die Mangament Console (als Download bei Microsoft erhältlich) installieren kann. Eine weitere Möglichkeit zur Administration ist der System Center Virtual Machine Manager von Microsoft. Dieser zielt aber aufgrund des Preises auf Firmen mit einer großen windowslastigen IT Infrastruktur ab. Mit dieser Management Lösung kann man nicht nur virtuelle Server sondern auch physische Server verwalten.

Mit Hyper-V im Windows Server 2008 und den kostenlosen Hyper-V Server will Microsoft die Anwender zur Virtualisierung ermuntern, wobei sie aber abhängig von der benutzten Version für virtuelle Windows- Rechner Lizenzkosten zahlen müssen. Bei der Standard-Edition vom Server 2008 ist es erlaubt eine weitere Installation in einer VM zu tätigen. Für weitere VM's mit Windows Server 2008 müssen Lizenzen erworben werden. Dadurch hofft Microsoft, dass Unternehmen für Virtualisierungslösungen keine anderen Systeme, wie etwa z.B.: XEN oder VMware, einsetzen.

(vgl.: microsoft, 30.11.2007, 1, Windows Server Hyper-V
http://www.microsoft.com/germany/windowsserver2008/virtualisierung.mspxvgl)
(vgl.: Hantelmann 2008, S.86)
(vgl.: Radonic 8.3.2008, 2, Hyper- V
http://wiki.computerwoche.de/doku.php/virtualisierung/microsoft/hyper-v)

4.1 Systemanforderungen und Features

Systemanforderungen:

Komponente	Anforderung
Prozessor	• x64 Prozessor • Hardware- Virtualisierung muss unterstützt werden (AMD- V oder Intel VT) • min.2 Ghz oder schneller • Hardware Data Execution (ein Sicherheitsfeature, welches einen Buffer-Overflow im RAM verhindern soll) muss verfügbar und aktiviert sein (Intel XD bit oder AMD NX bit)
Speicher	• Min. 1Gb • Empfohlen 2 Gb und mehr • Max. 32 Gb
Festplatten Speicherplatz	• Min. 10Gb • Empfohlen 40Gb und mehr
Netwerkkarten	• Min. 1 Netzwerkarte • Empfohlen 2 oder mehr
Laufwerke	• DVD Laufwerk
Bildschirm	• Super VGA (800x600) oder besser
Zeigegeräte	• Tastertur • Maus
Remote Management	Es wird beim Hyper-V Server ein zweites System für das Remote Management benötigt. Es kann sein: • Windows Server 2008 mit dem Hyper-V Manager MMC • Windows Vista SP1 mit dem Hyper-V Manager MMC • Microsoft System Center Virtual Machine Manager

Tabelle 1: Systemanforderungen Hyper-V (vgl.: microsoft 6.2.2009, 2, System Requirements, http://www.microsoft.com/servers/hyper-v-server/system-requirements.mspx)

Features:

Komponente	Unterstützung
Prozessoren Host	Bis zu physikalischen 4 Prozessoren (bei der Windows Server 2008 Enterprise und Datacenter Edition bis zu 64 Prozessoren
Prozessoren VM	Bis zu 4 virtuelle Prozessoren pro VM, 32bit und 64bit
RAM Host	Bis zu 32 GB RAM (bei der Windows Server 2008 Enterprise und Datacenter Edition bis zu 1TB RAM
RAM VM	Bis zu 31 GB RAM (bei der Windows Server 2008 Enterprise und Datacenter Edition bis zu 64GB RAM
Netzwerkkarten VM	Bis zu 12 Netzwerkkarten pro VM (8 „network adapter“, 4 „legacy network adapter“)
Storage Host	• Direct-attached storage: ◦ Serial Advanced Technology Attachment (SATA) ◦ external Serial Advanced Technology Attachment (eSATA) ◦ Parallel Advanced Technology Attachment (PATA) ◦ Serial Attached SCSI (SAS) ◦ SCSI ◦ USB ◦ Firewire • Storage area networks (SANs): ◦ Internet SCSI (iSCSI) ◦ Fibre Channel ◦ SAS technologies • Network-attached storage

Komponente	Unterstützung

Storage VM	• Virtual hard disks bis zu 2040 GB (fixed virtual hard disks, dynamically expanding virtual hard disks,differencing disks)
	• Virtual IDE devices: bis zu 4 IDE devices pro VM. Die startup disk muss ein IDE device sein.
	• Virtual SCSI devices. Bis zu 4 virtual SCSI controller, und pro controller bis zu 64 disks
	• Physical disks. Physical disks werden direkt an die VM weitergeleitet (“pass-through disks”), diese Art hat keine Limitierung der Größe (ausser durch das Gast Betriebssytem)
	• Komplette Storage Kapazität:
	  ◦ Virtual Hard Disks: 512 TB pro VM
	  ◦ Physical disks: Begrenzt durch das Gast Betriebssystem
	  ◦ Virtual machine snapshots:50 snapshots pro VM

Sonstige Hardware	• 1 DVD Laufwerk an einem der 4 IDE Controller • 2 virtuelle COM Ports pro VM • 1 Disketten Laufwerk pro VM
Lokales grafisches User Interfache	Nicht vorhanden beim Hyper- V Server 2008(bei den Editionen Windows Server 2008 Standard, Enterprise und Datacenter vorhanden
HA Clustering (Hochverfügbar-keits Cluster)	Nicht vorhanden beim Hyper- V Server 2008 und Standard Edition(bei den Editionen Windows Server 2008 Enterprise und Datacenter vorhanden
Backup	Live Backup mittels Volume Shadow Service möglich
Verschlüsselung	Verschlüsselung mittels Bitlocker
Quick Imigration (verschieben einer laufenden VM von einem Host zum Anderen mit minimaler Ausfallzeit	Nicht vorhanden beim Hyper- V Server 2008 und Standard Edition(bei den Editionen Windows Server 2008 Enterprise und Datacenter vorhanden

Komponente	Unterstützung
Möglichkeit zusätzliche Server Rollen hinzuzufügen	Nicht vorhanden beim Hyper- V Server 2008(bei den Editionen Windows Server 2008 Standard, Enterprise und Datacenter vorhanden
Unterstützte Gast Betriebssysteme	• Windows Server 2008 (32bit und 64bit) mit 1, 2, oder 4 virtuellen Prozessoren ◦ Windows Server 2008 Standard, Enterprise, Datacenter und Windows Server 2008 Standard, Enterprise, Datacenter without Hyper-V ◦ Windows Web Server 2008 ◦ Windows Server 2008 HPC Edition • Windows Server 2003 mit 1 oder 2 virtuellen Prozessoren ◦ Windows Server 2003 R2 Standard, Enterprise, Datacenter Edition with Service Pack 2 ◦ Windows Server 2003 Standard, Enterprise, Datacenter Edition with Service Pack 2 ◦ Windows Server 2003 Web Edition with Service Pack 2 ◦ Windows Server 2003 R2 Standard, Enterprise, Datacenter x64 Edition with Service Pack 2 ◦ Windows Server 2003 Standard, Enterprise, Datacenter x64 Edition with Service Pack 2 • Windows Server 2000 mit einem virtuellen Prozessor ◦ Windows 2000 Server with Service Pack 4 ◦ Windows 2000 Advanced Server with Service Pack 4 • Linux Distributionen mit einem Prozessor ◦ Suse Linux Enterprise Server 10 with Service Pack 1oder 2 (x86 edition) ◦ Suse Linux Enterprise Server 10 with Service Pack 1 oder 2 (x64 edition)

Komponente	Unterstützung
	• Windows Vista (32bit und 64bit) mit 1 oder 2 virtuellen Prozessoren ◦ Windows Vista Business, Enterprise, Ultimate mit Servicepack 1 • Windows XP ◦ Windows XP Professional with Service Pack 3 (mit 1 oder 2 virtuellen Prozessoren) ◦ Windows XP Professional und x64 Edition with Service Pack 2 (mit einem virtuellen Prozessor)

Tabelle 2: Features Hyper-V (vgl.: microsoft 6.2.2009, 3,Microsoft Hyper-V Server 2008 http://www.microsoft.com/servers/hyper-v-server/default.mspx vgl.: Microsoft Corporation 2008a, S. 3 f)

4.2 Aufbau

Der Microsoft Hyper-V Server 2008 ist ein Microkernelized VMM vom Type 1. In diesem Abschnitt werden die Komponenten des VMMs von Microsoft genauer erklärt. Bei genauerer Betrachtung sieht man eine sehr starke Ähnlichkeit im Aufbau zu den XEN basierenden Lösungen (Paravirtualisierung als Art der Virtualisierung).
Zuerst zur Erläuterung eine Abbildung auf der die wichtigsten Komponenten und ihre Lage im Aufbau des Servers dargestellt sind (siehe Abbildung 11). Danach folgen die Erklärungen der einzelnen Teile.

- Parent Partition
- Hypervisor aware bzw. Enlightened
- Virtual Harddisk
- Netzwerk

und wie diese zusammenspielen.

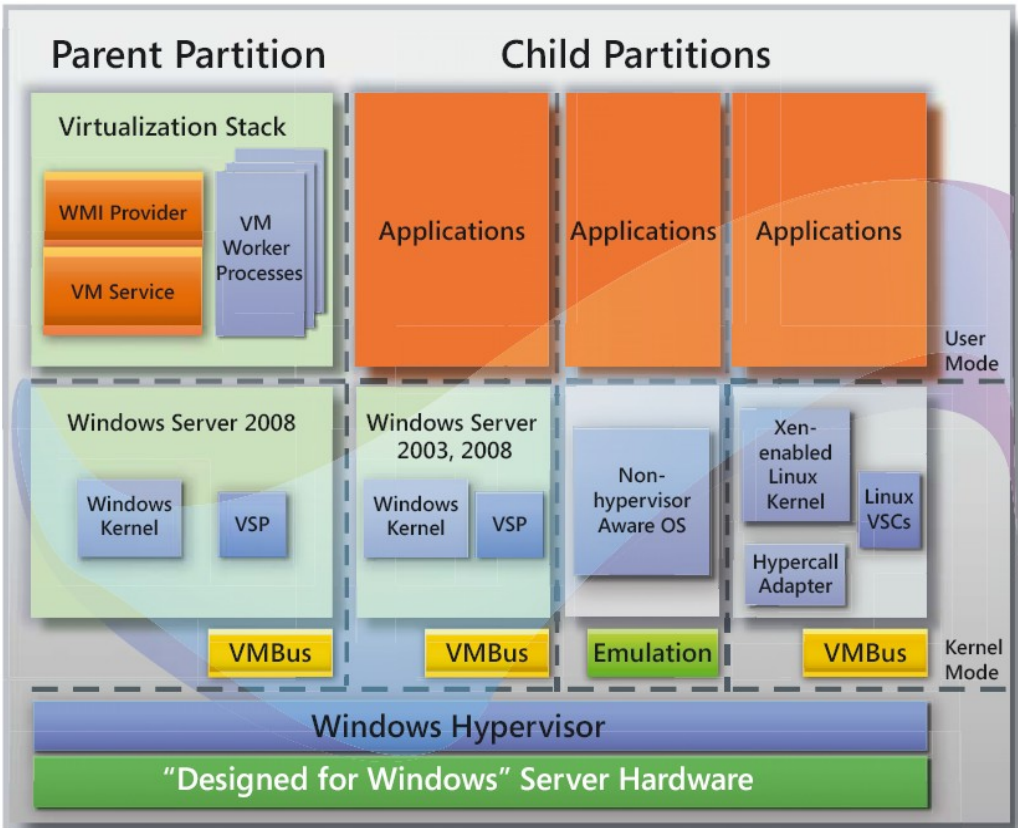

Abbildung 11: Aufbau Hyper-V (vgl.: Microsoft Corporation 2008b, S. 2)

So wie es bei dem VMM Type 1 üblich ist, der Kern vom Hyper-V der Windows Hypervisor. Er ist eine dünne Abstraktionsschicht zwischen der Hardware und den VM's. Es sind eine Parent Partition (Parent VM) und Child Partitions (Child VM's) vorhanden.

4.2.1 Parent Partition

In der Parent Partition läuft ein Windows Server 2008 (Variante Core Server, Standard Edition,usw....).
Als Anwendung in dieser privilegierten VM läuft der Virtualization Stack im User Mode. Er ist zuständig für die Management Komponenten (Virtual Machine Manager). Diese enthalten den Virtual Machine Service und den WMI Provider. Dieser Service managt die Virtual Machine Worker Prozesse. Für jede VM existiert einer dieser Prozesse. Sie überwachen und steuern die Zustände der Child Partitions (stop, run, start,usw.,...).
Der WMI Provider stellt die Schnittstelle zur Wartung der VM's bereit. Er wird nicht nur von dem lokalen Management - Tool verwendet sondern kann auch von anderen Programmen verwendet werden z.B.: System Center Virtual Machine Manager (SCVMM)
Im Kernel Mode läuft unter anderem der Virtual Machine Bus (VMBus).Dieser Bus ist für die Verbindung der VM's mit den Hardwareressourcen (bis auf Speicher und Prozessor) zuständig. Diese Verbindung erfolgt über die Virtual Service Provider (VSP) in der Parent Partition und die Virtual Service Consumers (VSC) in der Child Partition. Der VSP wird vom VMBus bereitgestellt, es gibt pro VSP einen VSC. Der VSC läuft in der Child Partition. Für jede Ressource gibt es ein Paar aus VSP und VSC, z.B.: für Festplattenzugriffe. Wenn die VM einen Hardwareaufruf macht sendet der VSC eine Anfrage an den VSP und wenn die Ressource zur Verfügung steht werden die Daten über den VMBus übertragen. Der VMBus wird zwischen den VM's nicht geteilt, es wird für jede Child Partition eine eigene Verbindung aufgebaut. Daher ist die Isolation zwischen den VM's gegeben.

In der *Abbildung 12* wird die Kommunikation über den VMBus und die Aufteilung der Ressourcen grafisch erläutert.

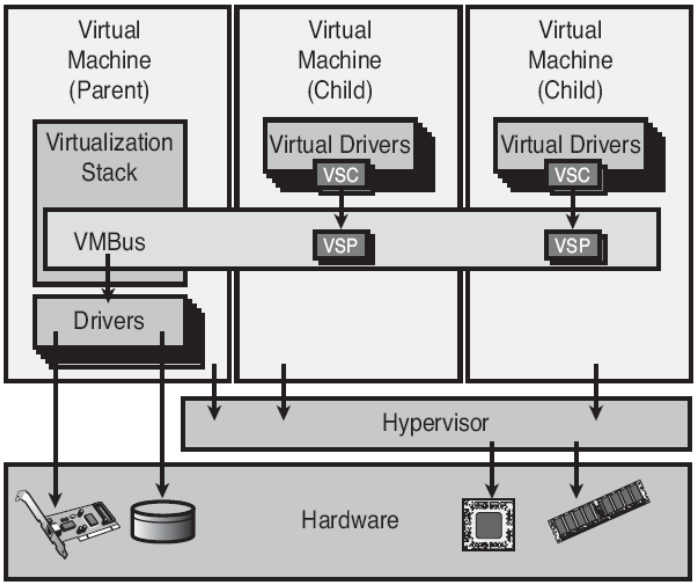

Abbildung 12: Hyper-V VMBus
(vgl.: Savill, John 2008 S1288)

4.2.2 Hypervisor aware bzw. Enlightment

Die unterstützten Gast Betriebssysteme werden in 2 Kategorien aufgeteilt, die „enlightened“ (Hypervisor- aware) und die „nonenlightend“ Child Partitions (Enlightment ist bei Microsoft der Ausdruck für Paravirtualisierung). Eine Child Partition ist dann „enlightened“, wenn sie weiß, dass sie in einer virtuellen Umgebung läuft.

Ein Betriebssystem kann „enlightened“ gemacht werden wenn es dafür die benötigten Treiber und Services gibt. Dieses Paket wird von Microsoft „Integration Components“ genannt.
Sie bestehen aus:

- Treiber für
  - Storage
  - Netzwerkanbindung
  - Grafik
  - Mouse
- Services
  - Betriebssystem shutdown
  - Zeitsynchronistation
  - Datenaustausch
  - Heartbeat
  - Online Backup

Betriebssysteme wie Windows Server 2008 und Windows Vista (mit installierten Integration Components) sind komplett „enlightened“. Während Windows Server 2000 nur zum teil enlightened“ ist, da es nicht für alle Ressourcen einen angepassten Treiber gibt.
Eine „enlightened“ Child Partition weiß, dass sie eine gewisse Anzahl an VSCs (Syntetic devices) hat mit denen sie auf Festplattenspeicher, Netzwerk, Video,... zugreifen kann.
Der VSC kommuniziert mit dem VSP der Parent Partition über den VMBus. Über diesen Weg kommt die Kommunikation zu den physikalischen Ressourcen zustande.
Eine Child Partition wird „nonenlightened“ genannt wenn sie nicht weiß, dass sie in einer virtuellen Umgebung läuft. Wenn sie nonenlightened“ ist kann die Kommunikation über den VMBus mittels VSC-VSP Paaren nicht verwendet werden. Stattdessen werden die Ressourcen der VM als emulierte Geräte (emulated devices) zur Verfügung gestellt.

Abbildung 13 zeigt eine Gegenüberstellung des Windows Gerätemanagers „Vor“ und „Nach“ der Installation der Integration Components.

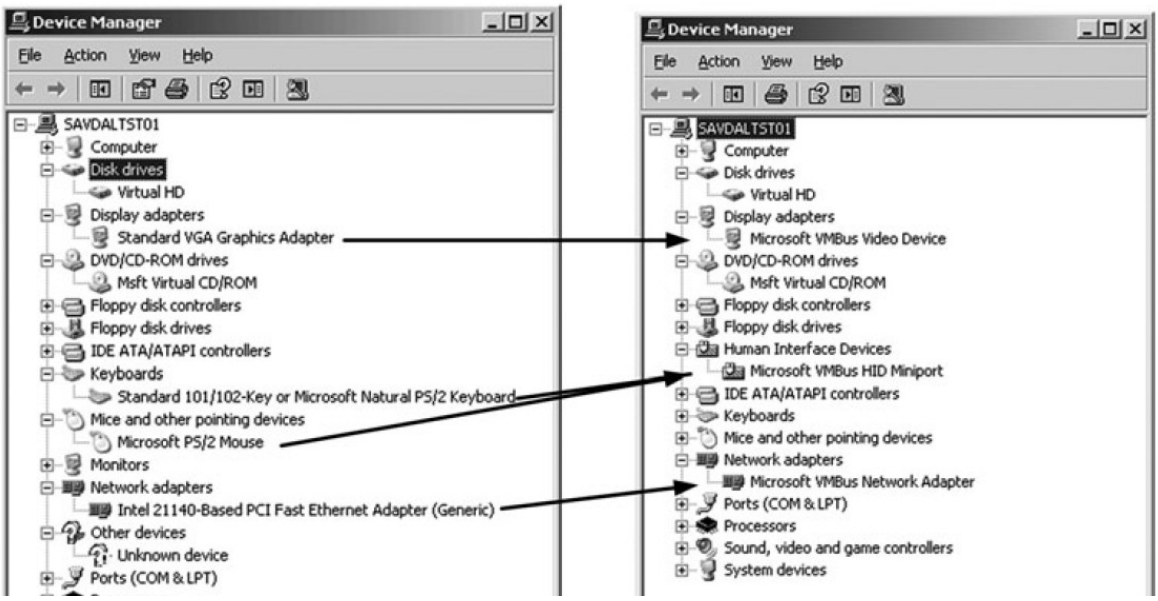

Abbildung 13: Integration Services (vgl.: Savill, John 2008 S. 1339)

Dieses Verfahren hat natürlich einen großen Einfluss auf die Performance, da das Betriebssystem in der VM einen normalen Hardwareaufruf tätigt, der dann vom Hypervisor abgefangen und an die Parent Partition zur Bearbeitung weitergegeben werden muss. Eine Netzwerk Operation würde bei einer emulierten Netzwerkkarte wie folgt aussehen:

User Mode in der Child Partition → Kernel Mode in der Child Partition → Kernel Mode Parent Partition (welcher das Gerät für die Child Partition emuliert) → User Mode Parent Partition – VM Worker Process (dieser erledigt dann den Hardwareaufruf).

Diese Prozedur ist um ein Vielfaches langsamer als die Aufrufe über den VMBus, aber dadurch können auch „nonenlightened“ Betriebssysteme vom Hyper-V unterstützt werden.

Auch eine Child Partition mit Linux als Betriebssystem kann „enlightened“ sein.
Das Linux muss einen Kernel mit den Xen – Erweiterungen verwenden. Danach müssen die Linux Integration Components installiert werden.
Diese beinhalten:

- Treiberunterstützung für synthetische Geräte (Kommunikation mittels VMBus)
- Hypercall- Adapter: eine dünne Softwareschicht die Xen-spezifische Aufrufe von Virtualisierungsfunktionen in Microsoft Hyper-V-Hypercalls übersetzt. Dadurch ergibt sich eine bessere Leistung des Linux- Gastes.
- Unterstützung für den Systemstart mit Fastpath: Startgeräte nutzen den Speicher-VSC um gesteigerte Leistung bereitzustellen.

Momentan werden von Microsoft zwei Linux Betriebssysteme mit Integration Components unterstützt:

- SUSE Linux Enterprise 10 SP2 x86
- SUSE Linux Enterprise 10 SP2 x64

4.2.3 Virtual Hard Disk (VHD)

Das VHD Format ist ein Container File welches die Festplatte für eine VM darstellt. Dieses Format wird vom Microsoft Server 2008 Hyer-V, Virtual PC und Virtual Server verwendet. In diesem File sind das Betriebssystem, Anwendungen und ihr momentaner Zustand gespeichert. Dieses File lässt sich auch direkt ohne Booten der VM ändern. Daraus ergeben sich einige Vorteile:

- Datenaustausch zwischen dem Host- System und dem VHD- File
- Leichtes Backup der Maschine (kopieren des VHD- Files)
- Anitvirus und Sicherheitstests
- Image Management und Patchen von Files
- Umwandlung von Festplatten in VHD und umgekehrt

Beim Hyper- V gibt es 3 Arten von VHD Files:

- Fixed VHD: Hier wird ein VHD- File mit einer fixen Größe erstellt, die nicht mehr variieren kann.
- Dynamic VHD: Die Größe des VHD-Files hängt vom Inhalt ab.
- Differencing VHD: Es werden nur die Änderungen zu einem Basis VHD- File gespeichert

Hyper- V kennt auch noch einen weiteren Typ einer Festplatte für eine VM: das pass-through drive. Bei dieser Art wird eine komplette physikalische Festplatte einer VM als virtuelle Festplatte zur Verfügung gestellt. Auf diese Festplatte kann die VM dann direkt zugreifen und muss nicht den Umweg über ein VHD- File nehmen. Dadurch ist die Performance höher als bei den VHD- Files.

Die VHD Files können auf jedem Datenspeicher den Microsoft Windows Server 2008 unterstützt abgelegt werden.

4.2.4 Netzwerk

Es stehen 2 Arten von virtuellen Netzwerkadaptern für die VM's zur Verfügung, der „network adapter“ und ein „legacy network adapter“. Der „network adapter“ funktioniert nur wenn man die Integration Components installiert hat. Der Vorteil von diesem Netzwerkadapter ist, dass er um ein Vielfaches schneller ist als der „legacy network adapter“. Wenn es für das jeweilige Betriebssystem keine Integration Components gibt, dann wird automatisch der „legacy adapter“ verwendet. Bei diesem wird ein „ Intel 21140-based PCI Fast Ethernet Adapter” emuliert. Er wird auch beim Netzwerkboot benötigt und es kann nur von ihm gebootet werden.

Bei der Netzwerkanbindung der VM's gibt es 3 verschiedene Möglichkeiten für verschiedene Anforderungen.

- External virtual networks: Dieser Typ wird verwendet wenn die VM mit der Parent Partition, den VM's am gleichen Host und mit dem normalen Netzwerk des Hostes kommunizieren soll.
- Internal virtual networks: Dieser Typ wird verwendet wenn die VM mit der Parent Partition und den VM's am gleichen Host kommunizieren soll.
- Private virtual networks: Dieser Typ wird verwendet wenn die VM nur mit anderen

VM's auf dem selben Host kommunizieren soll.

Bei der Erstellung eines external virtual network benutzt die Parent Partition eine neue virtuelle Netzwerkkarte um sich mit dem physikalischen Netzwerk zu verbinden. Der physikalische Netzwerkadapter kommuniziert mit dem neuen Virtuellen über das Microsoft Virtual Network Switch Protocol (VNSP). Ab dem Zeitpunkt der Verbindung wird der komplette Traffic über den virtuellen Switch geleitet.

Wenn eine Applikation in einer VM sich mit einem externen Ziel verbinden will, wird das Paket zuerst vom „virtual network adapter“ zum virtuellen Switch geleitet und dann von dort direkt zum physikalischen Netzwerkadapter ins externe Netz.

Microsoft unterstützt auch die Isolation von Netzwerken auf Layer 2 mittels Vlans. Um diese Funktion nutzen zu können benötigt man einen physikalischen Netzwerkadapter mit Vlan Unterstützung. Man kann dann jeden virtuellen Netzwerkadapter und den virtuellen Switch mit einer Vlan ID konfigurieren.

4.3 Lizenzierung

Theoretisch benötigt man für jede VM eine normale Lizenz wie für einen physikalischen Server, aber Microsoft hat hier aber ein paar Ausnahmen bei der Lizenzierung gemacht.

- Mircosoft Hyper-V Server 2008: jede VM mit Windows benötigt eine eigene Lizenz
- Windows Server 2008 Standard: diese Edition darf man auf einem physikalischen Server und einer VM gleichzeitig installieren.
- Windows Server 2008 Enterprise: diese Edition darf man auf einem physikalischen Server und 4 VM's gleichzeitig installieren.
- Windows Server 2008 Datacenter: diese Edition darf man auf einem physikalischen Server und einer unlimitierten Anzahl an VM's gleichzeitig installieren.

(vgl.: Microsoft 2008a, S 28f)
(vgl.: Gabe 11.3.2008, 1, Microsoft Windows Server 2008- Hyper-V solution overview, http://www.brianmadden.com/blogs/gabeknuth/archive/2008/03/11/microsoft-windows-server-2008-hyper-v-solution-overview.aspx)
(vgl. Savill 2008, S 1320 ff)

5 VMware ESXi

VMware ESXi ist eine Hypervisor – basierte (VMM vom Type 1) Virtualisierungslösung von VMware. ESXi ist eine abgespeckte Version vom VMware ESX Server und von der VMware Site kostenlos downloadbar.
Dieses Produkt ist im Vergleich zum Microsoft Hyper-V Server und Citrix Xen Server an kein Betriebssystem gebunden, da es selbst lauffähig ist (siehe Aufbau 5.2 S.41). Es wurde sehr kompakt designed um auf einer zertifizierten Hardware sehr schnell installiert und konfiguriert werden zu können.

Der Funktionsumfang des ESX Server und des ESXi Servers sind nahezu gleichwertig. Der gravierendste Unterschied liegt darin, dass der ESXi keine Linux basierende Service-Konsole besitzt. Dadurch konnte die Größe des Servers auf 32 MB reduziert werden (ESX: 2GB). Die einfachste Implementation eines ESXi Servers ist die Einbettung der Software direkt in einen Chip auf dem Mainboard des Servers. Dabei wird dann direkt von diesem Chip gebootet (erhältlich bei einigen Server Herstellern).

Möglichkeiten zum Managen des ESXI-Servers

- Virtual Infrastructure Client (VI Client): Hier handelt es sich um ein grafisches Windows User Interface um den Server zu managen.
- Remote command line interfaces: Durch diese Interfaces ist es möglich den Server mittels Skripten oder der Command Line von Linux und Windows Rechnern aus zu managen. Die Übertragung erfolgt über einen authentifizierten und verschlüsselten Kommunikationskanal.
- Anwendungen von Drittanbietern, die die dokumentierten APIs von VMware nutzen, wie die VIM API und die Common Information Model (CIM).
- VMware Infrastructure (VI): Mit dieser kostenpflichtigen Management Lösung lassen sich mehrere Server ESX und ESXi Server verwalten und spielen hier, dem Preis entsprechend, ihre Vorteile aus. (*siehe Features)*

Das Management des ESXi geht weg von der Konfiguration auf dem Host Rechner, direkt hin zur Konfiguration mittels Remote Werkzeugen.

(vgl.: Charu Chaubal 2007, S 3)
(vgl.: Charu Chaubal 2007a, S 3)

5.1 Systemanforderungen und Features

Systemanforderungen:

Aufgrund des Aufbaus des ESXi Servers gibt es keine allgemeinen Systemanforderungen. Laut VMware gibt es bestimmte Server von diversen Herstellern auf denen die Virtualisierungslösung installiert werden kann. Die Software unterstützt alle Hardwarekomponenten dieser Rechner.
Auf der Internet Site von VMware gibt es eine Liste in der alle unterstützten Server aufgelistet sind. Natürlich heißt das nicht ,dass der ESXi Server nur auf diesen Rechnern läuft, aber bei anderen Hardwarekomponenten kann man nur durch Testen herausfinden ob er funktioniert. Wenn man vor hat so ein System produktiv einzusetzen, sollte man sich an die Kompatibilitätsliste von VMware halten.

Ein paar Beispiele für kompatible Server:

- IBM Blade Center LS42; Quad core AMD Opteron 8376
- DELL PowerEdge 6650: 64-bit Intel Xeon Processor MP 64-bit
- HP ProLiant BL25p: Dual-Core AMD Opteron Processor Model 275
- Sun Fire X4200: Dual-Core AMD Opteron Processor Model 280
- Lenovo R630 G7: Quad Core Intel Xeon E73xx Series

Ein paar Beispiele für I/O Devices:

- Adaptec SCSI RAID 2120S
- Broadcom NetXtreme II BCM5706 1000Base-SX
- Qlogic QLA2310 (FiberChannel)

Ein paar Beispiele für Storage/SAN Devices:

- IBM DS3400 Fibechannel
- HP EAV4000 iSCSI
- DELL MD3000 SAS
- EMC Celerrra NSX NAS

(vgl.: http://www.VMware.com/resources/compatibility/search.php?action=base&deviceCategory=server)

Features:

Komponente	Unterstützung
Prozessoren Host	Bis zu physikalischen 32 Prozessoren
Prozessoren VM	Bis zu 4 Prozessoren pro VM
RAM Host	Bis zu 256 GB RAM
RAM VM	Bis zu 64 GB RAM
Netzwerk VM	Bis zu 4 Netzwerkkarten pro VM
Storage Host	• Direct-attached storage: siehe Kompatiblitätsliste auf der VMware Site • Storage area networks (SANs): siehe Kompatiblitätsliste auf der VMware Site • Network-attached storage: siehe Kompatiblitätsliste auf der VMware Site
Storage VM	• Virtual SCSI hard disks bis zu 2 TB • Virtual SCSI devices. Bis zu 4 virtual SCSI controller, und pro controller bis zu 15 devices
Sonstige Hardware	• 1 DVD Laufwerk • 4 virtuelle COM Ports pro VM • 2 virtuelle parallel Ports • 2 Disketten Laufwerk pro VM
Lokales grafisches User Interfache	Eingeschränke Funktionen: • Netzwerkeinstellungen • Setzen des Administrator Passworts • Keyboardeinstellungen • Logs lesen
HA Clustering (Hochverfügbar-keits Cluster)	Nur in Verbindung mit Virtual Infrastruktur 3 Standard und Enterprise Edition
Backup	Nur in Verbindung mit Virtual Infrastruktur 3 Foundation, Standard und Enterprise Edition (Consolidated Backup) Bei ESXi durch manuelles Kopieren der Datein

Komponente	Unterstützung
VMotion (verschieben einer laufenden VM von einem Host zum Anderen mit minimaler Ausfallzeit	Nur in Verbindung mit Virtual Infrastruktur 3 Enterprise Edition
Möglichkeit zusätzliche Server Rollen hinzuzufügen	Nicht vorhanden
Unterstützte Gast Betriebssysteme	• Windows Server 2008 32bit und 64bit • Windows Vista 32bit und 64bit • Windows Server 2003 32bit und 64 bit • Windows XP 32 bit und 64bit • Windows 2000 32bit • Windows NT 4.0 • CentOS 5.2 32bit und 64bit • Red Hat Enterprise Linux 5 32bit und 64bit • Red Hat Enterprise Linux 4 32bit und 64bit • Red Hat Enterprise Linux 3 32bit und 64bit • Red Hat Enterprise Linux 2.1 32bit • SUSE Linux Enterprise Desktop 10 32bit und 64bit • SUSE Linux Enterprise Server 10 32bit und 64bit • SUSE Linux Enterprise Server 9 32bit und 64bit • SUSE Linux Enterprise Server 8 32bit • Ubuntu Linux 8.04 LTS 32bit und 64bit • Ubuntu 7.10 Linux 32bit und 64bit • Ubuntu 7.04 Linux 32bit und 64bit • Netware 6.5 Server 32bit • Netware 6.0 Server 32bit

Komponente	Unterstützung
	• Netware 5.1 Server 32bit • Solaris 10 Operating System fpr x86 Platforms 32bit und 64 bit

Tabelle 3: Features ESXi (vgl.: VMware 2008, S 2
vgl: VMware 2009, S31f
vg.: VMware 2007a, S 11
vgl.: VMware 22.1.2009, 1, VMware ESXi Features,
http://www.vmware.com/products/esxi/features.html
vgl.: kb.vmware.com 4.12.2008, 1, Vmware ESX and ESXi Comparison,
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1006543)

5.2 Aufbau

Der VMware ESXi Server ist ein Monolithc VMM vom Type 1. In diesem Abschnitt werden die Komponenten des VMMs von VMware erläutert. VMware verwendet den Begriff Hypervisor für diese Art der Virtualisierung und der Begriff VMM wird nur für einen kleinen Teil des Hypervisors benutzt. Dieser ist für die VM's direkt zuständig.
Dieser Hypervisor beruht auf einem anderen Konzept als die Konkurrenten Microsoft Hyper-V und Citrix XEN. Aufgrund des Konzepts des Monolithic VMM gibt es hier nur die Hypervisor Schicht direkt auf der Hardware. Bei dieser Software wird keine Paravirtualisierung verwendet, sondern Binary Rewriting und Direct Execution.
In der folgenden Abbildung (siehe Abbildung 14) wird der Aufbau eines ESXi Servers gezeigt.

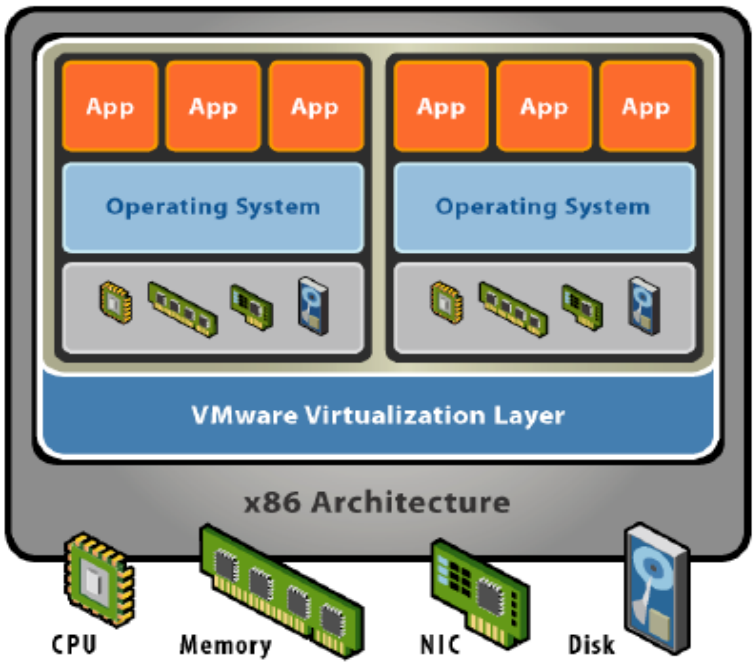

Abbildung 14: Aufbau ESXi (vgl.: VMware 2007 S 2)

Aus der Abbildung ist ersichtlich, dass es beim ESXi nur eine Virtualisationsschicht gibt die direkt auf der Hardware sitzt (bare-metal). Es wird keine Parent Partition benötigt da sich die Virtualisationsschicht um alles kümmert, wie die Ansteuerung der Hardware und ihre Aufteilung. Auf dieser Schicht sitzen die VM's welche von der darunter liegenden Schicht gesteuert werden.

Wie der Hypervisor intern aufgebaut ist sieht man in der Abbildung 15. Die Komponenten und wo diese im Aufbau der Virtualisierungsschicht untergebracht ist erkennbar.

Die Virtualisierungsschicht besteht aus dem Betriebssystem des ESXi, dem Vmkernel und Prozessen die auf ihm laufen. Der Vmkernel stellt die Ressourcen für alle Prozesse, inklusive der Management Anwendungen, der VM's, usw., zur Verfügung. Die Hauptprozesse die auf dem Vmkernel laufen sind:

- Direct Console Interface (DCUI): dient zur low-level Konfiguration des ESXi von der Command Line des Servers.
- Virtual Machine Monitor (VMM): ist ein Prozess der die Umgebung für die VM's mithilfe des VMX (Virtual Machine eXtensions) Prozesses erzeugt. Für jede VM gibt es einen VMM und einen VMX Prozess.
- Einige Agents die für das Management zuständig sind.
- Common Information Model (Cim) system: CIM ist ein Interface über das man den Server komplett über standardisierte APIs remote managen kann.

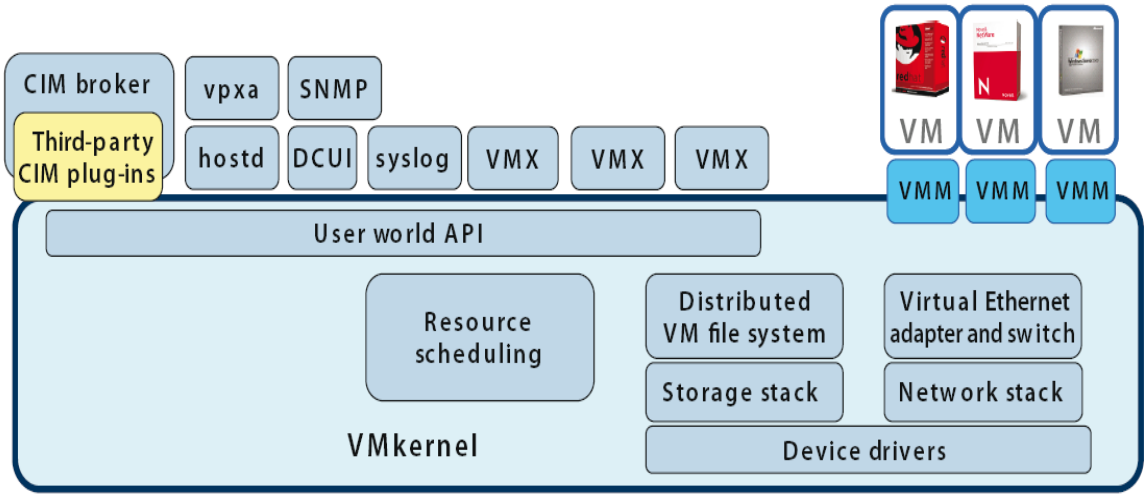

Abbildung 15: Aufbau Hypervisor ESXi (vgl.: Charu Chaubal 2007, S 3)

5.2.1 Vmkernel

Der Vmkernel ist eine Eigenentwicklung der Firma VMware. Er ist das Betriebssystem des ESXi Servers und wurde speziell für die Anforderungen der Virtualisierung designed. Dieser Kernel ist kein abgewandelter Linux Kernel. Daher ist es auch nicht möglich Linux Treiber für die Hardware zu verwenden um mehr Hardware zu unterstützen.
Durch den Vmkernel alleine ist keine Virtualisierung möglich, daher startet er weitere Prozesse, wie den VMM, um die Virtualisierung zu ermöglichen.

Die Hauptmerkmale des Vmkernels sind:

- Er ist ein für Virtualisierung optimiertes Betriebssystem
- Er läuft direkt auf der Hardware („bare metal“)
- Er kontrolliert alle Hardwareressourcen wie RAM, Prozessoren, Netzwerkadapter, usw. durch die „Device Drivers“
- Er besitzt einen Scheduler für die Hardwareressourcen
- Er besitzt voll funktionsfähige Netzwerk und Speicherstacks

Ressource Scheduling

- ist ein Prozess im Vmkernel
- ist für die Aufteilung der physikalischen Ressourcen zuständig
- erfasst alle Benutzereinstellungen die das Ressourcenmanagement betreffen

Virtual Machine Monitor:

- virtualisiert die Prozessoren
- verwaltet die gestarteten VM's
- gibt die Befehle aus den VM's an die Hardware weiter

Filesysteme

Der Vmkernel selbst benutzt ein simples Filesystem. Es liegt im Hauptspeicher (in-memory file system) um seine Konfigurations Files, log Files und Patches zu speichern.

Dieses Filessystem ist unabhängig vom VMware VMFS Filesystem, welches benutzt wird um VM's zu speichern. (siehe 5.2.6 Massenspeicherzugriff)

Über das Remote Command Interfaces ist ein Zugriff auf beide Filesysteme möglich. Der Zugriff wurde über https implementiert und wird über User und Groups die lokal am Server eingerichtet werden authentifiziert.

5.2.2 Prozesse außerhalb des Vmkernels („User World“)

Die Prozesse in der „User World“ haben einen wesentlich eingeschränkteren Befehlssatz zur Verfügung als Prozesse in einem normalen POSIX Kompatiblen Betriebssystem. Beispiele dafür sind:

- die Anzahl von verfügbaren Signals ist limitiert
- die System API ist nur ein kleiner Teil eines POSIX Betriebssystems
- das /proc Filesystem ist sehr beschränkt
- ein swap file ist für alle Prozesse vorhanden, wenn auch eine lokale Festplatte vorhanden ist. Wenn nicht kann der User manuell auf einem VMFS Datastore eine anlegen

Einige wichtige Prozesse laufen in dieser Umgebung:

Direct Console User Interface (DLCUI)

DLCUI ist das lokale User Interface das auf der Konsole des ESXi Server läuft. Der Zweck diese Management Tools ist die erste Konfiguration und Fehlersuche. Weitere Konfigurationen werden dann mittels der Remote Management Tools erstellt.
Mit der DLCUI kann man:

- das Administrationspasswort setzen
- den Netzwerkadapter konfigurieren
- einfache Netzwerktests durchführen
- Logs ansehen

- Agents neu starten
- Auf Werkseinstellung zurücksetzen

hostd Prozess

Dieser Prozess ist für die Authentifizierung und Erstellung von Usern und Gruppen zuständig. Über die Remote Management Tools lassen sich dann mittels dieses Prozesses die User und Gruppen anlegen bzw. überprüfen, welche Rechte die User der Remote Tools haben.

Weitere Prozesse:

- vpxa Prozess: wird verwendet zur Kommunikation mit einem Virtual Center
- syslog Prozess läuft wenn logging aktiviert ist. Es kann auch auf ein entferntes Ziel geloggt werden damit bei einem Neustart nicht die alten Logs verschwinden (in-memory filesystem)
- SNMP Prozess um den Server mittels SNMP zu überwachen
- Agents für Hochverfügbarkeit, wenn verfügbar

(vgl.: Charu Chaubal 2007, S 3f)
(vgl.: Zimmer, Dennis 2007, S 29f)

5.2.3 VMware Tools

Dieses Programm- Paket besteht aus Werkzeugen und Treibern die der VM neue Funktionen und eine bessere Performance ermöglichen. Diese Programme erweitern das Betriebssystem um einige Funktionen die an die virtuelle Umgebung angepasst sind. Die VMware Tools werden für eine Vielzahl von unterstützen Betriebssystemen angeboten.

Einige Funktionen der Tools sind:

- File transfer zwischen Host und VM (beim ESXi nicht so wichtig)
- Erhöhte Netzwerk Performance
- Besseres Speichermanagement
- Zeitsynchronisation zwischen Host und VM's

5.2.4 Prozessor und Hauptspeicher Zugriffe

Die Bereitstellung der virtuellen Hardwareressourcen wird nicht bei allen Komponenten gleich realisiert. Die Prozessor- und Hauptspeicheranfragen werden nahezu direkt an die physikalische Hardware weitergegeben. Alle anderen Ressourcen werden für die einzelnen VM's emuliert.

Bei der Prozessorvirtualisierung werden von VMware 2 Verfahren angewendet:

- Direct Execution: die Befehle werden direkt an den Prozessor weitergegeben und bearbeitet. Diese Art wird vorwiegend für Ring 3 Anfragen eingesetzt.
- Virtualization Mode (Binary Rewriting): die Befehle werden vom Hypervisor abgefangen und modifiziert. Diese Art wird vor allem für Ring 0 Anfragen verwendet.

Beim Zugriff auf den Hauptspeicher teilt der ESXi Server den vorhandenen Speicher laut den Konfigurationen der VM's auf. Die einzelnen VM's können nur den Speicher sehen der ihnen zugewiesen wurde. Der Hypervisor verwaltet den Speicher für die VM's, die VM kann nie direkt auf den Hauptspeicher zugreifen. Durch diese Mechanismen ist es dem ESXi Server möglich den sichtbaren Hauptspeicher der VM's zu begrenzen und zu verwalten.

Einige interessante Funktion in Verbindung mit dem Hauptspeicher besitzt der ESXi:

- „Memory Overcommitment“: Diese Funktion erlaubt es dem Server der VM bis zu 100% mehr Hauptspeicher zur Verfügung zu stellen als der Host besitzt. Diese Funktion wird mittels einer Swap- Datei gelöst.
- „Memory Allocation“: damit kann eingestellt werden, wie viel Hauptspeicher physikalisch bzw. mittles einer Swap Datei einer VM bereitgestellt wird.
- „Memory Idle Tax“: dabei wird versucht dem Gastbetriebssystem nur soviel Hauptspeicher zu geben wie es benötigt und nicht mehr
- „Memory Ballooning“: benutzt einen angepassten Speichertreiber der in der VM installiert werden muss. Diese Technik wird verwendet um belegten Speicher wieder zurückzugewinnen und nutzt dabei die Funktion des Betriebssystems Speicherinhalte auszulagern.
- „Transparent Page Sharing“: ermöglicht die Nutzung gleicher Hauptspeicherinhalte durch mehrere VM's.

5.2.5 Netzwerk

Das Netzwerk besteht beim ESXi Server aus mehreren Komponenten und nicht nur aus der virtuellen Netzwerkkarte. Die Netzwerkkomponenten sind virtuelle Netzwerkadapter, virtuelle Switches und die physikalischen Netzwerkadapter. In der folgenden Abbildung 16 werden alle Komponenten aufgezeigt und wie diese zusammenspielen.

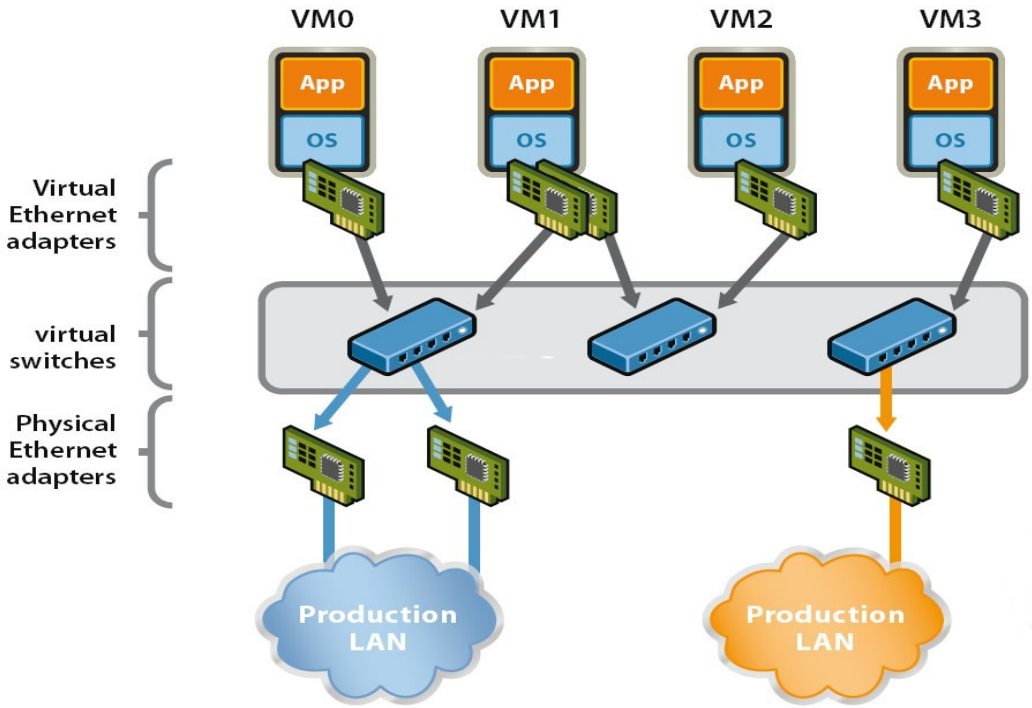

Abbildung 16: Netzwerkstruktur ESXi (vgl.: VMware 2007a, S 3 – angepasst)

Jede VM kann bis zu 4 virtuelle Netzwerkadapter besitzen. Es gibt 3 Arten von Netzwerkadaptern für die VM's.

- Vlance: Eine Emulation des AMD PCNet32 Netzwerkadapters. Diese Karte wird verwendet wenn keine VMware Tools installiert sind. Dieser Netzwerkadapter wird von den Treibern des Betriebssystems der VM angesteuert.
- Vmxnet: ist ein paravirtualisierter Netzwerkadapter der verwendet wird wenn die VMware Tools installiert sind. Dieser Adapter wurde für hohe Performance optimiert.
- E1000: Eine Emulation eines Intel E1000 Netzwerkadapters. Dieser wird vor allem für 64bit VM's verwendet. Der Netzwerkadapter wird von den Treibern des Betriebssystems der VM angesteuert.

Diese Netzwerkadapter werden mit einem virtuellen Switch verbunden. Es können pro physikalischen Host 248 virtuelle Switches erstellt werden. Die Aufgabe des Switches ist es, die VM's untereinander und mit den physikalischen Netzwerkadaptern zu verbinden.

Die Hauptfunktionen eines virtuellen Switches sind:

- Layer 2 forwarding
- VLAN Zuordnung (Vlan tagging)
- Layer 2 Security:

Weitere Funktionalitäten des ESXi Netzwerks sind Load Balancing und Failover Konfigurationen.
Beim Load Balancing kann der Traffic der VM's auf mehrere physikalische Netzwerkadapter aufgeteilt werden.
Die Failover Konfiguration wird verwendet um beim Ausfall einer physikalischen Verbindung zum Ziel einen anderen Weg über einen anderen physikalischen Netzwerkadapter zu aktivieren.

(vgl.: Zimmer, Dennis 2007, S 37)
(vgl.: VMware 2007a, S 3f)

5.2.6 Massenspeicherzugriff

Der VMkernel regelt alle Zugriffe auf sämtliche Massenspeicher mit seinem eigenen Storage-Stack. Es macht für die VM's keinen Unterschied ob ihre virtuelle Festplatte auf einer lokalen SCSI Platte oder auf einem entfernten Storage, z.B.: iSCSI liegt. Es kann aber auch über den VMkernel eigenen Netzwerk- Stack auf NFS Freigaben zugegriffen werden.

(vgl.: Zimmer, Dennis 2007, S29 f)

VMware verwendet für die virtuellen Festplatten der VM's das Virtual Machine Disk Format (VMDK). In diesem File sind das Betriebssystem, Anwendungen und ihr momentaner Zustand gespeichert.

Es gibt 3 Möglichkeiten um einer VM eine virtuelle Festplatte zur Verfügung zu stellen:

- Ein vmdk File im VMware Virtual Machine File System (VMFS)
- Raw Device Mapping (RDM)
- Ein vmdk File über eine NFS Freigabe

Jedes dieser Systeme hat Vor- und Nachteile, doch als Standard wird VMFS verwendet. VMFS wurde speziell zum Speichern von VM's entwickelt. Es ist ein High Performance Cluster- Dateisystem welches den konkurrierenden Zugriff mehrerer ESXi bzw. ESX Server auf Dateien erlaubt. Es wurde auf hohen Durchsatz und die Speicherung von großen Dateien (virtuelle Festplatten der VM's) optimiert. Durch dieses Dateisystem werden die Enterprise- Features (Vmotion, Hochverfügbarkeit,...) von VMware erst möglich.
In der Abbildung 17 sieht man eine typische Anwendung von VMFS.

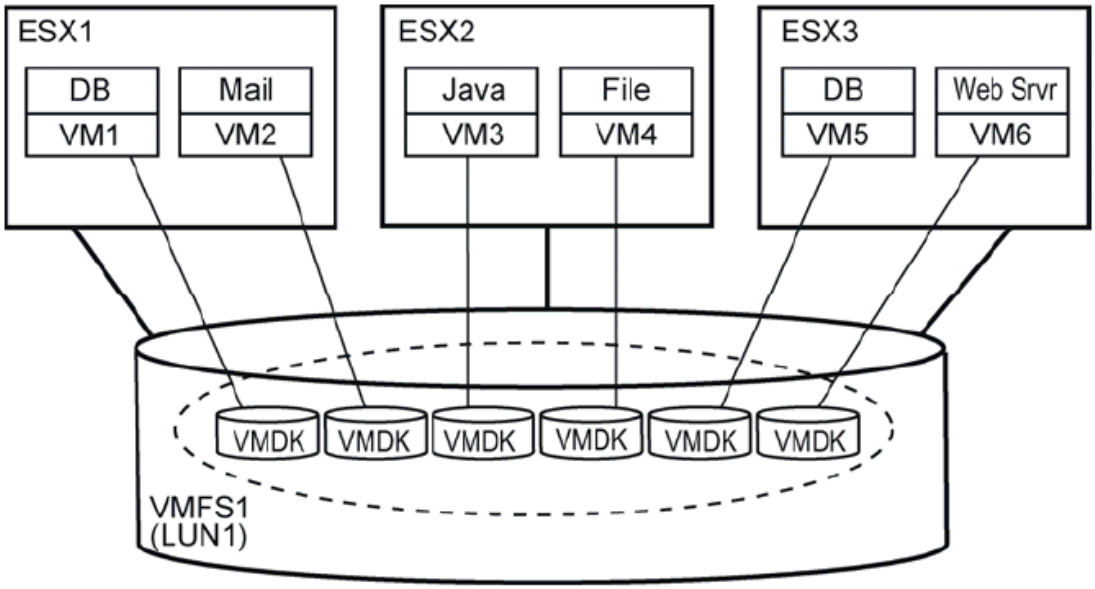

Abbildung 17: VMFS- Anwendung (vgl.: VMware 2007 b, S 5

Jeder der ESX bzw ESXi Server hat 2 VM's laufen welche auf dem VMFS Volume gespeichert sind. Jeder der Server speichert seine VM's in einem Sub Directory auf dem VMFS Filesystem. Wenn eine VM läuft setzt das VMFS einen „lock“ auf die Datei damit kein anderer Server die Datei ändern kann. Dadurch stellt das Filesystem sicher, dass immer nur ein Server die VM öffnen kann.

Bei einer NFS Freigabe werden die selben Funktionen unterstützt wie bei VMFS. Das Management des Dateisystems liegt aber nicht in der Hand des ESXi Servers sondern des Dateiservers. Die Performance von VMFS ist bei den meisten Anwendungen besser. Doch wenn eine Firma bereits NFS verwendet spricht nichts dagegen die vmdk Files auf eine NFS Freigabe zu legen.

Virtuelle Festplatten müssen nicht als vmdk Datei abgelegt werden. Es kann auch eine physikalische Partition mittels Raw Device Mapping (RDM) einer VM durchgereicht werden. Bei RDM gibt es ein File in einem VMFS Dateisystem welches wie ein Proxy für physikalische Raw Devices fungiert. Es speichert Metadaten die benutzt werden um die Zugriffe auf das physikalische Device zu managen.

Für den Großteil der Anwendungen ist VMFS die bessere Lösung. Nur bei einigen Spezialanwendungen wie Quorum Disks wird RDM verwendet.

(vgl.: VMware 2007b, S 4 f)
(vgl.: VMware 2007c, S2 f)

5.3 Lizenzierung

Beim ESXi Server benötigt man für jede installierte VM eine normale Lizenz wie bei einem physikalischen Server. Der Vorteil ist, dass man für das Management des Servers keine Lizenz benötigt, da es die RCLI auch für Linux Systeme gibt. Ob die User dann damit arbeiten wollen bleibt ihnen überlassen. Wenn man den Luxus des grafischen Virtual Infrastruktur Clients will benötigt man aber eine Windows Lizenz, denn diesen Client gibt es nur für Windows.
Der ESXi Server selbst ist frei erhältlich und ist die kleinste Form des ESX Servers. Es gibt einige Editionen des Servers. Je teurer die Editionen sind desto mehr Enterprise Features sind inkludiert und desto umfangreicher sind die Managmenttools.

In der Abbildung 18 sind die Editionen aufgelistet und die jeweiligen Erweiterungen zum ESXi Server.

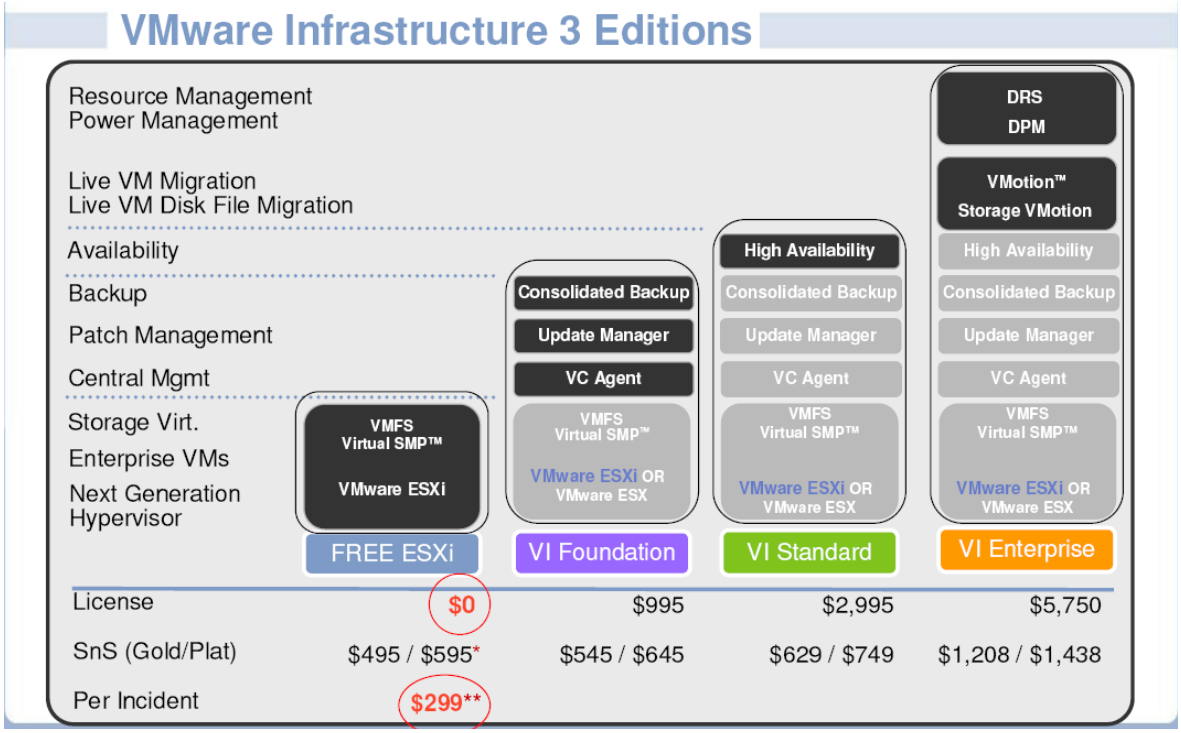

Abbildung 18: ESXi Editions (vgl.: VMware (Präsentation), S 12)

6 Citrix XenServer

Der Citrix XenServer 5.0 ist eine Hypervisor- basierte (VMM vom Type 1) Virtualisierungssoftware von der Firma Citrix. Die Grundlage für diese Software ist der Open Source Hypervisor Xen in der Version 3.2. Die Technologie hinter Xen ist Paravirtualisierung um eine möglichst hohe Geschwindigkeit der angepassten VM's zu erzielen. Wenn der Host über Hardwarevirtualisierung (AMD- V oder Intel VT) verfügt dann können auch nicht angepasste Betriebssysteme wie Microsoft Windows in einer virtuellen Umgebung von Xen laufen. Diese Technologie wird bei Xen „Hardware Virtual Machine“ (HVM) genannt.

Die Virtualisierungssoftware XEN entstand ursprünglich im Jahre 2003 an der University of Cambridge und wurde als Open Source freigegeben. Bis 2007 gab es ein Unternehmen namens Xensource, welches erweiterte Funktionen und Support zu dem Open Source Xen verkaufte. Diese Firma wurde von Citrix aufgekauft und das Produkt wird jetzt als XenServer vertrieben.
Es gibt noch immer die Open Source Virtualisierungslösung Xen und diese wird auch weiterentwickelt. Die Firma Citrix hebt sich mit ihrer Software gegenüber der Open Source Version vor allem durch komfortable Management Tools ab.

Diese Tools sind:

- XenCenter: Eine grafische Oberfläche zur Remote Administration unter Windows
- xconsole: eine Menü basierende Oberfläche für alle administrativen Tätigkeiten direkt auf dem Server
- CLI: mit dem Programm xe kann man direkt in der Command Line des Servers alle Funktionen des XenServers ansprechen

(vgl. Prabhakar,S 6 f)
(vgl.: Baumeister 29.12.2008,1, Ratgeber:XenServer 5 einrichten und konfigurieren, http://www.pcwelt.de/start/software_os/systemtools/praxis/188212/xenserver_5_einrichten_und_konfigurieren/)

6.1 Systemanforderungen und Features

Systemanforderungen:

Komponente	Anforderung
Prozessor	• 64 bit Prozessor • Min.1,5 Ghz • gleiche Prozessoren im ganzen Ressourcepool (Enterprise Edition) • Hardware- Virtualisierung für Windows Gäste (AMD- V oder Intel VT)
Speicher	• Min. 1GB • Max. 128 GB
Festplatten Speicherplatz	• Min. 16GB • Empfohlen 60Gb und mehr
Netwerkkarten	• Min. 1 Netzwerkarte 100Mb/s • Empfohlen 2 oder mehr
Remote Management	• PC mit Windows 2000, XP, Vista, Server 2003, Server 2008 • .NET Framework 2.0 oder höher • Netzwerkadapter

Tabelle 4: Systemanforderungen XenServer (vgl.: citrix 6.2.2009, 1, http://www.citrix.com/English/ps2/products/subfeature.asp?contentID=1681139)

Features:

Komponente	Unterstützung
Prozessoren Host	• 2 Sockel in der Express Edition • 4 Sockel in der Standard Edition • unbegrenzt in der Enterprise und Platinum Edition
Prozessoren VM	• Bis zu 32 Prozessoren (Linux) • Bis zu 8 Prozessoren (Windows)
RAM Host	Bis zu 128 GB RAM
RAM VM	Bis zu 32 GB

Komponente	Unterstützung
Netzwerkkarten VM	• Bis zu 7 Netzwerkkarten pro VM (Windows) • Bis zu 3 Netzwerkadapter pro VM (Linux)
Storage Host	• Local Storage • iSCSI oder FC LUN • NFS • NettApp LUN
Storage VM	• Bis zu 7 virtuelle Disks Linux • Bis zu 6 virtuelle Disks Windows
Sonstige Hardware	• 1 CD Laufwerk
Lokales grafisches User Interfache	Ja aber nicht alle Funktionen verfügbar. Lokale CLI alle Funktionen verfügbar
HA Clustering (Hochverfügbar-keits Cluster)	Nicht vorhanden bei der Express Edition, erst ab der Enterprise Edition
Backup	Ja
Verschlüsselung	Nein
XenMotion (verschieben einer laufenden VM von einem Host zum Anderen mit minimaler Ausfallzeit	Nicht vorhanden bei der Express Edition erst ab der Enterprise Edition möglich.
Möglichkeit zusätzliche Server Rollen hinzuzufügen	Nicht vorhanden
Unterstützte Gast Betriebssysteme	• Windows Server 2008 (32bit und 64bit) in Enlightened Mode • Windows Server 2003 (32 bit und 64 bit) Standard, Enterprise, Datacenter Edition und SBS Editions • Windows Server 2000 mit Service Pack 4 • Windows Vista Enterprise (32bit) • Windows XP SP2 und SP3

Komponente	Unterstützung

	• Suse Linux Enterprise Server 9 with Service Pack 4
	• Suse Linux Enterprise Server 10 with Service Pack 1 oder 2 (32bit und 64bit)
	• Red Hat Enterprise Linux 4.5- 4.7
	• Red Hat Enterprise Linux 5.0-5.2 (32bit und 64 bit)
	• CentOS 4.5, 4.6
	• CentOS 5.0-5.2 (32bit und 64bit)
	• Oracle Enterprise Linux 5.0-5.2 (32bit und 64 bit)
	
	• Build -In Linux Distributionen (werden Mitgeliefert)
	  ◦ Debian Sarge 3.1
	  ◦ Debian Etch 4.0

Tabelle 5: Features XenServer (vgl.: citrix 6.2.2009, 2, http://www.citrix.com/English/ps2/products/subfeature.asp?contentID=1680964 vgl.: citrix, 3, http://www.citrix.com/English/ps2/products/subfeature.asp?contentID=1681139)

6.2 Aufbau

Der Citrix XenServer 5 ist ein Microkernelized VMM vom Type 1 und nutzt Paravirtualisierung und Hardware Assisted Virtualization.
In diesem Kapitel werden der Aufbau und die Komponenten des XenServers genauer erklärt. In der Abbildung 19 sind die wichtigsten Komponenten und ihre Lage im Aufbau des Servers dargestellt.
Bei Xen werden die VM als Domains bezeichnet. Es gibt 3 Arten dieser Domains:

- Domain 0 (Privilegierter Gast)
- Domain U (Paravirtualisierte Gäste)
- HVM (=Hardware Virtual Machine)Guest (Vollvirtualisierte Gäste)

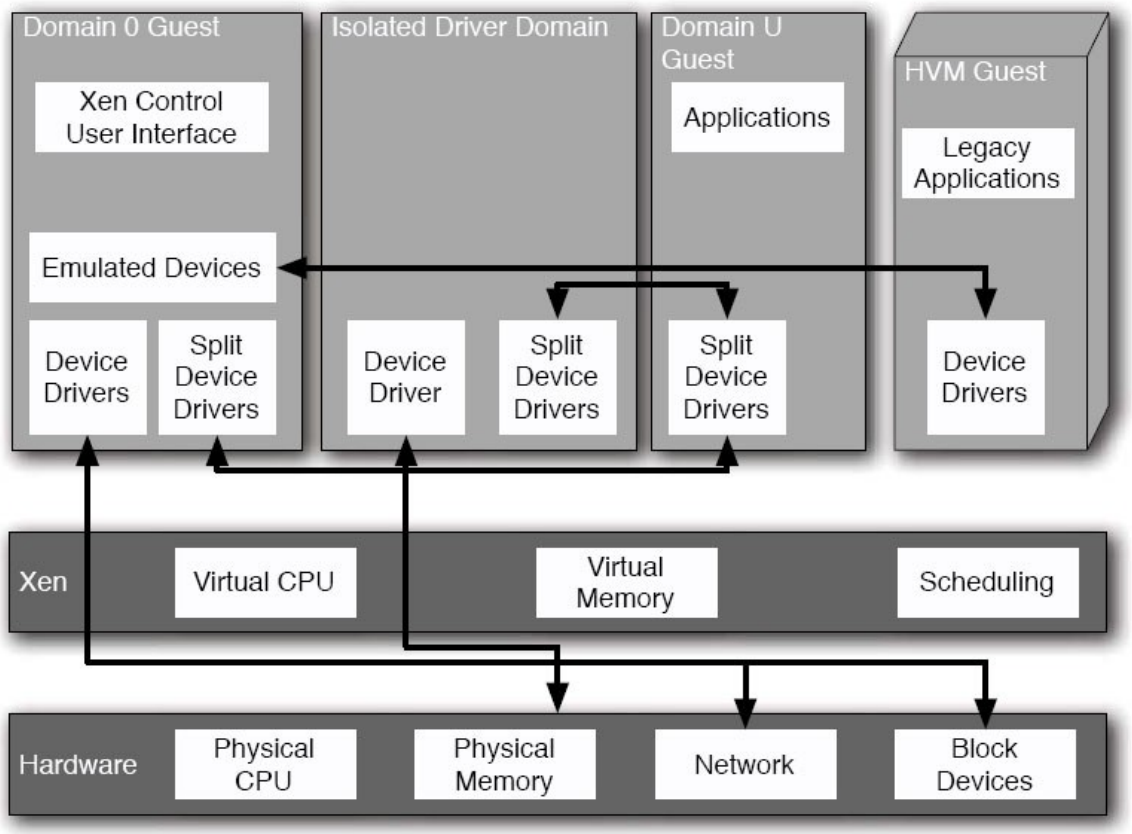

Abbildung 19: Aufbau Xen (vgl.: Chisnal, S. 25)

Der Xenserver besteht wie der Microsoft Hyper-V Server aus einer Hypervisorschicht die direkt auf der Hardware liegt (in der Abbildung …..... Xen genannnt).Das Management der VM's und die Bereitstellung der Treiber bzw. der Hardware übernimmt hier die Domain 0. Die Hauptbestandteile des XenServers 5 sind:

- Domain 0
- Domain U / Isolated Driver Domain
- HVM Gäste
- Netzwerk
- Storage

6.2.1 Domain 0

Beim Booten des Systems wird zuerst die Domain 0 geladen da sie erhöhte Privilegien besitzt. Diese Domain ist sehr wichtig für das komplette Xen System. Es stellt das User Interface für den Hypervisor und die Treiber für alle Gäste zur Verfügung und sorgt für die Storage Anbindung. Als Betriebssystem der Domain 0 läuft beim Citrix XenServer 5 CentOS 5.2.

Die wichtigste Aufgabe der Domain 0 ist das Verwalten der Hardware. Es stellt den VM's die virtuellen Geräte zur Verfügung. Diese Bereitstellung erfolgt über diese 3 Komponenten:

- Split Driver
- Multiplexer
- Real Driver

In der Abbildung 20 wird erklärt welchen Weg ein Paket nimmt wenn es von einer Applikation in einer Domain U übers Netzwerk an ein reales Ziel schickt.

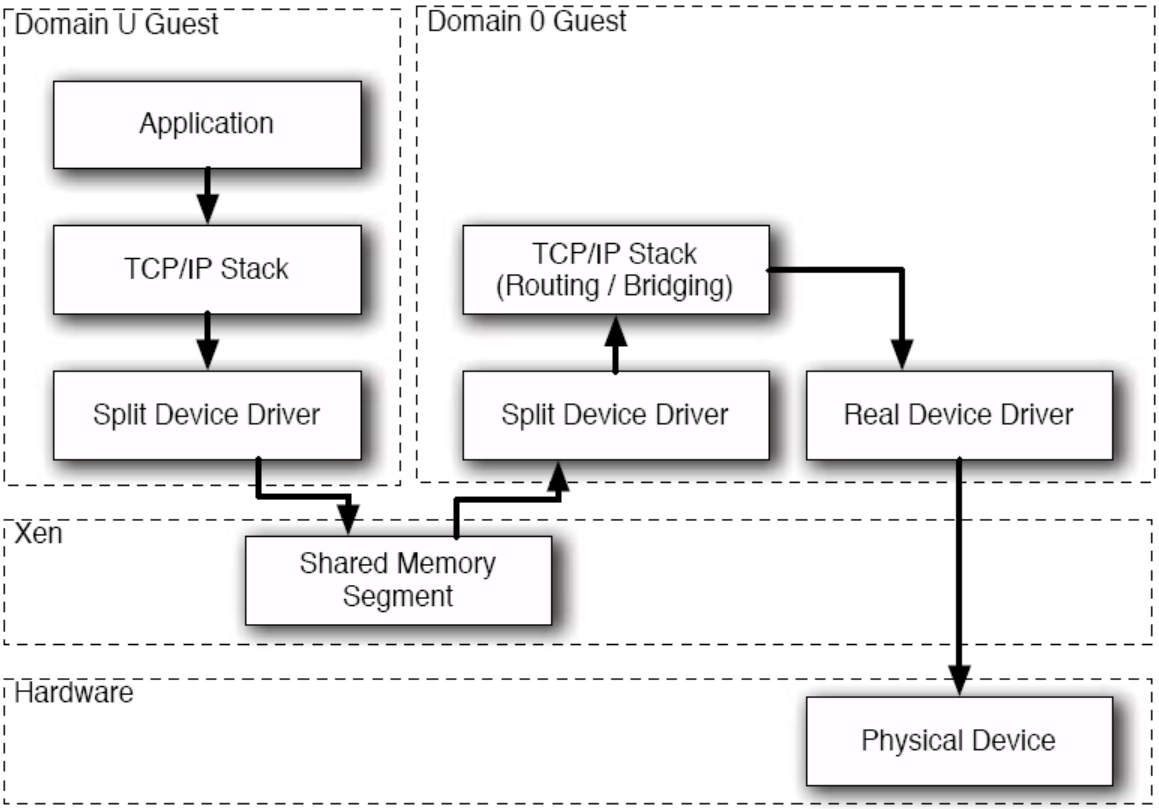

Abbildung 20: Xen Domain 0 Weg eines Netzwerkpakets (vgl.: Chisnall , 2008. S.20

Das Paket wird von der Applikation in der VM an den TCP/IP Stack des installierten Betriebssystems weitergegeben. Danach würde es normalerweise an den realen Treiber für die Netzwerkkarte gehen. Hier liegt aber anstatt dieses normalen Treibers ein Teil des Split Drivers. Dieser legt das Paket in einem Shared Memory ab. Von dort kann es sich der zweite Teil des Split Driver holen und an den TCP/IP Stack der Domain 0 weitergeben. Der TCP/IP Stack der Domain 0 hat vollen Zugriff auf den Treiber der physikalischen Netzwerkkarte (Real Driver) und der leitet das Paket dann an die Netzwerkkarte und somit ins physikalische Netz weiter. Den Part des Multiplexers (Verteiler) übernimmt in diesem Beispiel der TCP/IP Stack der Domain 0. Er kann bei mehrere Netzwerkverbindungen unterscheiden wem welches Paket gehört.

(vgl. Prabhakar,S 7 f)
(vgl.: Chisnall, S 19 f)

6.2.2 Domain U

Die Domain U 's (U= unprivileged) haben weniger Rechte als die Domain 0. Es ist ihnen prinzipiell untersagt direkt auf die Hardware zuzugreifen. In bestimmten Fällen können Ausnahmen eingerichtet werden.
Anstatt dem Zugriff auf die physikalische Hardware, wird ein Split Driver für jedes Gerät implementiert, über diesen kann die Domain U dann über die Domain 0 auf die Hardware zugreifen.

Bei manchen Anwendungen, wenn z.B.: ein Treiber für ein Gerät Bugs enthält, kann die Domain 0 zum Absturz gebracht werden. Um dem entgegen zu wirken kann man einen Treiber in einer eigene Domain isolieren, der Isolated Driver Domain.

(vgl.: Chisnall, S 22 f)

Zum Erzeugen einer Domain U werden beim Citrix XenServer Templates verwendet. Diese Templates sind im Server integriert und beinhalten die benötigten Einstellungen um eine neue VM zu instanzieren. Sie reichen von „generic raw VM's“ (Installation von einem Herstelltermedium oder einer Netzwerkinstallation z.B.: Red Hat Enterprise Linux) bis hin zu komplett vorkonfigurierten VM's (z.B.: Debian Etch).
Mit den Linux Templates werden reine paravirtualisierte VM erzeugt. Im Gegensatz dazu werden aus den Windows Templates HVM VM's.

(vgl.: Citrix Systems, Inc., 2008a, S.2)

Erzeugung einer Windows VM

Um Windows VM's erzeugen zu können muss der Host mit einem Prozessor der Hardware Virtualisierung (Intel Vt oder AMD-V) unterstützt ausgestattet sein.
Die Installation eines Windows Systems wird in zwei Teile aufgespalten:

- Die eigentliche Installation
- Installation der „paravirtualisierten device driver“ (XenTools)

Die XenTools enthalten paravirtualisierte Treiber für Netzwerk und SCSI Controller. Durch sie steigert sich die Performance dieser Geräte erheblich.

Erzeugung einer Linux VM

Bei einer Linux Vm wird nach der Betriebssysteminstallation der Linux Agent anstatt der XenTools installiert.

Dieser Agent enthält im Vergleich zu den XenServer Tools keine paravirtualisierten Treiber, sondern er übermittelt dem Host Informationen über die VM, wie:

- Name der Linux Distribution und Version
- Kernel Version
- IP Adressen der Netzwerkadapter
- Größe des RAMs und freier Speicherplatz im RAM

Bei der Installation eines unterstützten Linux Systems werden keine angepassten Treiber benötigt, da die Anpassung des Kernels durch das Benutzen der Templates erfolgt.

(vgl.: Citrix Systems, Inc., 2008a, S.20)

6.2.3 HVM (Hardware Virtual Machine) Gast

Bei dieser Art von Gästen muss der Host mit einem Prozessor der Hardware Virtualisierung (Intel Vt oder AMD-V) unterstützt ausgestattet sein. Es können dann nicht modifizierte Betriebssysteme (z.B.: Windows) in dieser Domain installiert werden.

Der Unterschied besteht darin, dass ein unmodifiziertes Betriebssystem nichts mit den Split Drivern anfangen kann. Es benötigt emulierte Hardware die es normal ansprechen kann. Die Domain 0 emuliert die benötigten Geräte für diese VM's.

(vgl.: Chisnall, S. 22 ff)

6.2.4 Netzwerk

Der XenServer 5 unterstützt bis zu 6 physikalische oder gebündelte Netzwerkadapter. Jeder VM können bis zu 7 virtuelle Netzwerkadapter zugewiesen werden.
Es wird zwischen 3 Netzwerk Objekten beim XenServer unterschieden:

- PIF: repräsentiert einen physikalischen Netzwerkadapter an einem XenServer Host. Dieses Objekt enthält einen Namen, eine Beschreibung, eine eindeutige Nummer, die Parameter des physikalischen Netzwerkadapters und das angeschlossene Netzwerk.
- VIF: repräsentiert einen virtuellen Netzwerkadapter. Dieses Objekt enthält den Namen, eine Beschreibung, eine eindeutige Nummer und an welches Netzwerk und VM sie gebunden ist.
- Network: repräsentiert einen virtuellen Ethernet Switch auf einem XenServer Host. Es enthält einen Namen, eine Beschreibung, eine eindeutige Nummer und eine Liste aller VIFs und PIFs die an ihm angeschlossen sind.

Durch das Kombinieren dieser drei Objekte lassen sich interne Netzwerke (nur zwischen VM's) und externe Netzwerke erzeugen.

(vgl.: Citrix Systems, Inc. ,2008b, S. 46)

6.2.5 Storage

Der XenServer definiert für jedes Speicherziel einen Container namens „Storage Repository (SR)“. In diesem Container werden die virtuellen Festplatten (VDI- Virtuel Disk Images) gespeichert. Ein VDI ist eine Datei in der der gesamte Inhalt einer virtuellen Festplatte gespeichert ist.
Es wird eine große Anzahl an Speichergeräten unterstützt (z.B.: IDE, SATA, SAS,...)
Durch die Abstraktion der Daten mittels VDI und SR können alle Features der Speichergeräte ausgenutzt werden, wie z.B.: Snapshots. Wenn die Speichergeräte nicht über diese Funktionen verfügen werden sie softwaretechnisch realisiert.

Es gibt 3 unterschiedliche VDI Typen:

- VHD(Microsofts Virtual Hard Disk Format): Dieses Format kann nur bei Speicherung des Images auf einer lokalen Festplatte oder einem NFS Share benutzt werden. Der Vorteil dieses Formates ist, dass nur der Speicherplatz der benötigt auch belegt wird und nicht die Größe der virtuellen Festplatte.
  Ein weiterer Vorteil dieses Systems ist, dass beim Klonen einer VM Daten auf einem VHD Image gemeinsam genutzt und bei der geklonten VM nur die Änderungen gespeichert werden
- LVM (Logical Volume Manager): Hier wird mittels des LVM dem VDI direkt ein „Logical Volume“ aus einer „Volume Group“ zugewiesen
- Supported storage appliances: Bei unterstützten Speichergeräten, wie einer NetApp appliance oder einem Dell EqualLogics filer wird das VDI direkt als LUN (=Speicherbereich auf einem SAN) gespeichert.

(vgl.: Withoff Oliver, S. 9 f)

7 Vergleich der Produkte

Die Gewichtung der Funktionen hängt natürlich immer vom geplanten Einsatzgebiet ab und kann daher nicht pauschal bewertet werden. In der Bewertung dieser Arbeit wird als Anwendung eine Serverlösung mit lokalem Speicher für kleine und mittlere Betriebe angenommen. Der Grund dafür ist, dass sich für diese Anwendung die kostenlosen Varianten der drei Virtualisierungslösungen bestens eignen.

Der Vergleich der Virtualisierungslösungen gliedert sich in 2 Teile

- Der theoretischer Vergleich:
  Gegenüberstellung von wichtigen Funktionen und Features anhand dieser Punkte
  - Allgemeine Merkmale
  - Host
  - VM
  - Management
  - Storage
  - Backup
  - Netzwerk
  - Hochverfügbarkeit
- Der Vergleich der Benchmarkergebnisse

7.1 Theoretischer Vergleich anhand der Funktionen

	VMware ESXi	Microsoft Hyper- V Server 2008	Citrix XenServer 5
Version			
Allgemein	Allgemein	Allgemein	Allgemein
VMM Type	Type 1	Type 1	Type 1
Eingesetzte Virtualisierungsart	Binary Rewriting	Paravirtualisierung und Hard Assisted Virtualisation	Paravirtualisierung und Hard Assisted Virtualisation
Host	Host	Host	Host
Architektur	32 bit und 64 bit	64 bit, AMD-V oder Intel-VT	64 bit, AMD-V oder Intel-VT wird benötigt wenn die Gäste voll Virtualisiert werden
Anzahl der unterstützten Prozessoren	Bis zu 32	Bis zu 4 (bis zu 64 in der Windows Server 2008 Enterprise und Datacenter Version)	2 Sockel in der Express Edition (bis hin zu unbegrenzt Enterprise Edition)
Unterstützter RAM	256GB	32 GB (bis zu 1 TB in Datacenter Version)	128GB
Host Betriebssystem	Eigenständiger Kernel	Windows Server 2008	CentOS
VM	VM	VM	VM
Unterstützte Architektur	32 bit und 64 bit	32 bit und 64 bit	32 bit und 64 bit
Anzahl der virtuellen Prozessoren	4	4	8 Windows 32 Linux
Unterstützter RAM pro VM	64GB	31GB (Bei Enterprise und Datacenter 64GB)	128 GB
Snapshots (Momentaufnahme der VM) Möglichkeit	Ja	Ja	Ja
Unterstützte Betriebssysteme	Große Anzahl von Windows, Linux und Unix	Windows und 2 Linux Betriebssysteme	Große Anzahl von Windows und Linux Betriebssysteme
Angepasste Treiber für die VM	VMware Tools	Integration Components	Xen Tools
Templates	Nein (nur mit Virtual Infrastructure)	Nein (nur mit System Center)	ja

Management	Management	Management	Management
Management Tools	VI Client	Hyper-V Manager	XenCenter,xconsole, CLI
Ressourcen Management	Ja	Indirekt (mittels Ressourcen Manager des Betriebssystems)	Ja
Storage	Storage	Storage	Storage
Unterstützte Medien	SAN, NAS, DAS	SAN, NAS, DAS	SAN, NAS, DAS
Backup	Backup	Backup	Backup
Backup Möglichkeit	Nein (erst mit Virtual Infrastrukture)	Volume Shadow Copy Service	Ja
Netzwerk	Netzwerk	Netzwerk	Netzwerk
Virtuelle Netze (Netzwer nur zwischen VM's)	Ja	Ja	ja
VLAN	Ja	Ja	Nein (erst ab Standard Edition)
Bündelung von mehreren physikalischen Netzwerkadapter	Ja	Nein	Ja
Hochverfügbarkeit	Hochverfügbarkeit	Hochverfügbarkeit	Hochverfügbarkeit
Hochverfügbarkeits-Funktion	Nein (erst mit Virtual Infrastrukture)	Nein (ab Enterprise)	Nein (ab Enterprise Edition)
Live Migration (verschieben einer laufenden VM auf eine anderen Host ohne Ausfallzeit)	Nein (Vmotion mit Virtual Infrastrukture)	Quick Imigration (kurze Ausfallszeit)	Nein (XenMotion ab Standard Edition)

Tabelle 6: Theoretischer Vergleich der Produkte

Beim Vergleich der Features sieht man eine große Übereinstimmung der Produkte und dass sich keine der drei Lösung signifikant absetzten kann. Als nächstes werden einige Punkte hervorgehoben die bei der Entscheidungsfindung von großer Bedeutung sind.

Bei Hardwareunterstützung und Performance sollten die Produkte von Microsoft und Citrix dem ESXi aufgrund ihrer Architektur überlegen sein, was im praktischen Teil mittels der Benchmarks ermittelt wird.

Die Maximalwerte der Hardware wie RAM und Anzahl der unterstützten CPUs, usw. sind für das genannte Anwendungsbeispiel, einer Serverlösung in kleinen und mittleren Betrieben, nicht relevant. In diesen Betrieben werden kaum Server mit mehr als 30GB RAM und mehreren CPUs eingesetzt.

Ein weiterer wichtiger Punkt für diese Unternehmen kann die Anzahl der unterstützten Betriebssysteme sein. Wenn nicht nur Windows und SUSE Linux zum Einsatz kommen geht der Punkt klar an ESXi und XenServer. Wobei man Aufgrund der Architektur beim ESXi Server eine größere Chance hat nicht unterstützte Betriebssysteme zum Laufen zu bringen.

Die Management Interfaces sind vielen Benutzern sehr wichtig und es werden vor allem grafische Lösungen erwartet. Alle Kandidaten liefern Lösungen mit unterschiedliche Schwachstellen. Ein Problem beim Hyper- V ist, dass es den Hyper-V Manager nur für Windows Vista SP1 und Windows Server 2008 gibt. Beim ESXi ist die Management Lösung zumindest unter Windows XP und Windows Vista lauffähig. Beim Management ist XenServer seinen Konkurrenten überlegen, da es nicht nur eine funktionale grafische Oberfläche mitbringt, sondern auch komplett über die Command Line direkt am Server gesteuert werden kann.

7.2 Aufbau der Testumgebungen

Bei den exemplarischen Implementierungen werden die jeweiligen Virtualisierungslösungen nacheinander auf der selben Hardware installiert und mittels Benchmarks getestet. Als Ergebnis der Tests soll eine Bewertung der verschiedenen Lösungen getroffen werden.

Es werden jeweils drei VM's mit unterschiedlichen Betriebssystemen installiert um die Produkte bei einem möglichst realistischen Einsatz zu testen.

Es werden folgende Betriebssysteme in den virtuellen Umgebungen installiert:

- Windows Server Enterprise 2008 (32bit)
- SUSE Linux Enterprise Server 10 (32bit)
- OpenSolaris 2008.11

Die Auswahl der beiden ersten Systeme fiel aufgrund ihrer weiten Verbreitung. Sie werden von allen Virtualisierungslösungen offiziell unterstützt. OpenSolaris wurde ausgewählt da es aus lizenzrechtlichen Gründen nicht erlaubt ist unter Solaris 10 Benchmarks auszuführen und die Ergebnisse zu veröffentlichen. Durch die Wahl dieser Betriebssysteme ist ein weites Spektrum, von Windows über Linux hin zu Unix, abgedeckt.

In diesen Maschinen werden Benchmarks ermittelt um die Performance in der jeweiligen virtuellen Umgebung zu messen. Es wird bei der Ermittlung der Benchmarks vor allem auf die unterstützten Betriebssysteme Wert gelegt.
Da OpenSolaris nicht offiziell unterstützt wird stehen hier vor allem die Installation und die Funktion der virtuellen Hardware im Vordergrund. Wenn die Installation und die virtuelle Hardware funktionieren werden dann auch auf OpenSolaris einige Benchmarks durchgeführt.

Danach werden diese Betriebssysteme direkt auf der Hardware installiert und die selben Benchmarks ermittelt. Diese Benchmarks werden verglichen um die Vor- und Nachteile der Produkte zueinander und zum nativen Betrieb zu ermitteln.

7.2.1 Testhardware

Der Rechner für die Testumgebung wurde von der Fachhochschule St. Pölten bereitgestellt. Bei der Auswahl der Testhardware wurde auf die Erfüllung der Mindestanforderungen der zu testenden Produkte geachtet. Ein Problem mit der Hardware trat bei der Installation des ESXi Servers auf (siehe: Testumgebung des VMware ESXi Servers, S.80), doch dieses Problem konnte gelöst werden und es wurden dadurch keine Tests behindert oder verfälscht.

Die Daten der Testhardware sind:

- Prozessor:
  - Intel Core 2 CPU 6320 @ 1.86GHz
  - 2 Kerne pro Prozessor
  - Unterstützt Intel VT
  - Unterstützt Hardware Data Execution (Intel XD bit)
- RAM:
  - 4 Gb RAM (beim Testen der Virtualisierungslösungen)
  - 3 Gb RAM bei der nativen Installation der 3 Betriebssysteme
  - Type des RAMs: pro Slot ein Baustein mit 1Gb DDR2 (Samsung M3 78T2953EZ3-CD5)
- Mainboard:
  - Intel Corporation DQ965GF
- Netzwerkadapter:
  - Intel(R) PRO/1000 GT-Desktopadapter (Ethernet, 1Gbps) wurde für die Netzwerktest verwendet.
  - Onboard Netzwerkadapter: Intel® 82566DM Gigabit Ethernet Controller
- Physische Speichergeräte:
  - ST380815AS 80GB (SATA300, 3.5", NCQ, 8MB Cache)75GB
  - ST3500410AS 500GB (SATA300, 3.5", NCQ, 16MB Cache)466GB
- DVD Laufwerk

7.2.2 Konfiguration der VM's

Auf allen Virtualisierungsprodukten wurden die VM's mit den gleichen Eckdaten konfiguriert damit ein aussagekräftiges Ergebnis zustande kommt und die Daten zwischen den Produkten verglichen werden können.
Die Eckdaten der VM's sind:

- 2 Pozessoren
- 3000 MB RAM
- 40Gb Festplattenkapazität gespeichert auf der 500GB Festplatte
- 1 Netzwerkkarte die mit der Intel(R) PRO/1000 GT-Desktopadapter verbunden ist

7.2.3 Benchmarks

Benchmarks in der Informatik dienen zum Vergleich der Leistung von EDV-Systemen. Meist wird dabei Software verwendet um die Leistung verschiedener Hardware-Systeme zu messen und zu vergleichen.
(vgl.: wikipedia, 1, http://de.wikipedia.org/wiki/Benchmark)

Bei den Benchmark Programmen werden für jedes Betriebssystem eigene Benchmarks verwendet. Es gibt keine Tools die auf allen Plattformen funktionieren, daher wurden spezielle Benchmarks für jedes Betriebssystem verwendet.
Diese Vorgehensweise ist aber bei den Tests in dieser Arbeit kein Problem da immer nur das selbe Betriebssystem in verschiedenen virtuellen Umgebungen miteinander verglichen wird und nicht die Betriebssystem zueinander.

Windows Benchmark

Für Windows Server 2008 wurde die Systemanalyse und Benchmark Suite Sandra Lite 2009 (15.60) von SiSoftware verwendet. Mit Hilfe dieser Software lassen sich komplette Berichte über das Betriebssystem und die Hardware anlegen. Von den vorhandenen Tests dieser Software wurden folgende verwendet:

- Prozessorleistung Arithmetik:
  Testet die ALU (Arithmetic-Logic Unit)und FPU (Floating Point Unit) Prozessoreinheiten. Zeigt die Leistung des Systems bei Arithmetik- und Fließkommaberechnungen.
  Solche Operationen sind typische Anwendungsfälle bei vielen Programmen.
  - Dhrystone ALU:
    Dieser Test wird benutzt um die Leistungsfähigkeit des Prozessors zu bestimmen. Er beinhaltet typische numerische Operationen die von einer Vielzahl von Applikationen verwendet werden.
    Es wird eine Multi-Threaded, 32/64bit Variante dieses Tests verwendet. Es werden bis zu 64 CPUs unterstützt. Das Ergebnis wird in MIPS (Million Instructions Per Second) angegeben). Je höher der Wert ist, desto schneller ist der Prozessor
  - Whetstone iSSE3:
    Dieser Test wird benutzt um die Leistungsfähigkeit des FPU bzw. CoProzessors zu testen (Ein Teil eines modernen Prozessors). Die FPU bzw. CoProzessor wird vor allem von wissenschaftlichen, technischen Programmen oder von Statistik- Programmen verwendet.
    Es wird eine Multi-Threaded, 32/64bit Variante dieses Tests verwendet. Es werden bis zu 64 CPUs unterstützt. Das Ergebnis wird in MFLOPS (Million FLoating OPerations per Second) angegeben). Je höher der Wert ist, desto performanter ist der Prozessor.

  (vgl: SiSoftware ,6.2.2009, 1, http://www.sisoftware.net/index.html?dir=qa&location=ben_cpu&langx=en&a=)
  (vgl.: SiSoftware, 2008, Kapitel Prozessor Arithmetik)

- Prozessor: Kryptografieleistung:
  Es wird die Verschlüsselungsleistung der Prozessoreinheiten getestet. Die Funktionen die dabei ausgeführt werden sind: Verschlüsseln, Entschlüsseln und Hashing.
  Alle Ergebnisse werden in MB/s angegeben. Das bedeutet wie viele Daten pro Sekunde ver- bzw. entschlüsselt werden können.
  Die verwendeten Algorithmen sind:
  - AES256 wird für die Ver- und Entschlüsselung verwendet
  - SHA256 wird für die Signierung verwendet

  (vgl.: SiSoftware, 6.2.2009, 2, http://www.sisoftware.net/index.html?dir=qa&location=crypto_perf&langx=de&a=)
  (vgl.: SiSoftware, 2008, Kapitel Kryptografieleistung)
- Dateisystem:
  Es werden die gemounteten Dateisysteme getestet. Dabei wird die Geschwindigkeit des Volumes, die von zahlreichen Faktoren, wie Dateisystem, Systemcache des Betriebssystems, Position auf dem Laufwerk usw. abhängt, selbst gemessen. Das Ergebnis ist der Laufwerksindex, es ist die Gesamtleistung basierend auf einem Ergebnismittel der Lese-, Schreib- und Suchtests.
  - Laufwerksindex wird in MB/s gemessen.
  - Durchschnittliche Zugriffszeit wird in ms gemessen.

  (vgl.: SiSoftware, 2008, Kapitel Dateisystem)
- Speicherbandbreite:
  Es wird die Speicherbandbreite des Systems getestet.
  Der Test basiert auf dem bekannten STREAM Speicherbenchmark.
  - Arithmetischer Benchmark in GB/s: Integer Buff'd iSSE2
  - Fliesskomma-Benchmark in GB/s: Fließkomma Buff'd iSSE2

  (vgl.: SiSoftware, 2008, Kapitel Speicherbandbreite)

- Netzwerk-Bandbreite:
  Es wird die Netzwerkbandbreite des Systems gemessen. Der Test verwendet die ICMP (ping/echo) Schnittstelle um die Antwortzeiten und Bandbreite zu messen. Dazu wurde in einem zweiten Rechner die selbe Netzwerkkarte wie im Testrechner eingebaut und mittels eines „Crossover“ Netzwerkkabels verbunden um die Störeinflüsse gering zu halten.Der Testaufbau entspricht dem Aufbau bei den Netzwerktests der beiden anderen Betriebssysteme (siehe Abbildung 21).
  - Bandbreite Daten in MB/s
  - Latenzzeit Daten in us

SUSE und OpenSolaris Benchmarks

Für den SUSE Server und OpenSolaris wurde die Phoronix Test Suite 1.6 verwendet (http://phoronix-test-suite.com/). Dieses Softwarepakt besteht aus über 80 einzelnen Tests und über 30 Test Suites.

Aus den verfügbaren Tests wurden 6 repräsentative Tests für den SUSE Server ausgewählt.
Diese Tests sind:

- Iozone Version 3.315:
  Es misst die Performance des Filesystems. Es wurde einmal pro Maschine mit den Parametern „2GB“ und „Read“ ausgeführt und das zweite mal mit „2GB“ und „Write“. Das Ergebnis dieser Tests ist die Geschwindigkeit beim Lesen bzw. beim Schreiben und wird in MB/s angegeben.
- RAMSpeed
  Es wird die Performance des RAMs gemessen. Dieser Test wurde zwei Mal pro Maschine aufgerufen. Einmal mit den Parametern „Add“, „Integer“ und „10 Times“ und das zweite Mal mit „Copy“ „Int“ und „10 Times“. Das Ergebnis dieser Tests ist die Geschwindigkeit des RAMs und wird in MB/s angegeben.
- Compress-gzip:
  Bei diesem Test wird die Zeit ermittelt, die das System zum Komprimieren einer 2 GB Datei, mittels des Programms gzip, benötigt. Dieser Test fordert vor allem die Performance der CPU und des RAMs.

- SCIMark2:
  SciMark 2.0 ist eine Java Benchmark für wissenschaftliches und numerisches Rechnen. Das Ergebnis wird in MFLOPS (Million Floating Point Operations per Second) ausgegeben. Je höher der Wert ist, desto performanter ist der Prozessor
- encode MP3:
  Bei diesem Test wird die Zeit gemessen die das System benötigt, um eine .wav Datei mittels des LAME (Version 3.98.2) mp3 Decoders in eine mp3 Datei umzuwandeln. Die .wav Datei wird von der Phoronix Test Suite zur Verfügung gestellt.
- SuperPI
  Bei diesem Test wird das Programm SuperPI eingesetzt. Es ermittelt die Zahl PI bis zu einer einstellbaren Anzahl von Stellen. Bei den Tests in dieser Arbeit wurde PI bis auf „Millionen Stellen berechnet“.

Für OpenSolaris wurden diese Tests aus der Phoronix Test Suite ausgewählt:

- Compress- gzip
- Bork File Encrypter:
  Ist ein in Java programmiertes Verschlüsselungsprogramm. Es wird ein 2,1 GB File verschlüsselt und das Ergebnis dieses Tests ist die benötigte Zeit.
- SciMark2

Ein weiterer Test wurde noch in OpenSolaris durchgeführt:

- dd :
  Bei diesem Test werden Daten von einem virtuellen Gerät auf ein anderes geschrieben. Dadurch wird die Leistungsfähigkeit des I/O Systems bzw. IO Stacks ermittelt. Es werden 15 GB Daten mit dem Programm dd kopiert. Das Ergebnis dieses Tests ist die Zeit die benötigt wird. Das Programm wird mit diesen Parametern aufgerufen
  dd if=/dev/zero of=/dev/null count=3000000

Zusätzlich zu diesen Tests wurde bei SUSE und OpenSolaris mittels des Programms „netperf 2.4.4“ die Performance der Netzwerkadapter gemessen. Dazu wurde in einem zweiten Rechner eine Netzwerkkarte vom selben Type wie im Testrechner eingebaut und mittels eines „Crossover“ Netzwerkkabels verbunden um die Störeinflüsse gering zu halten.

Aufbau des Netzwerktestes:

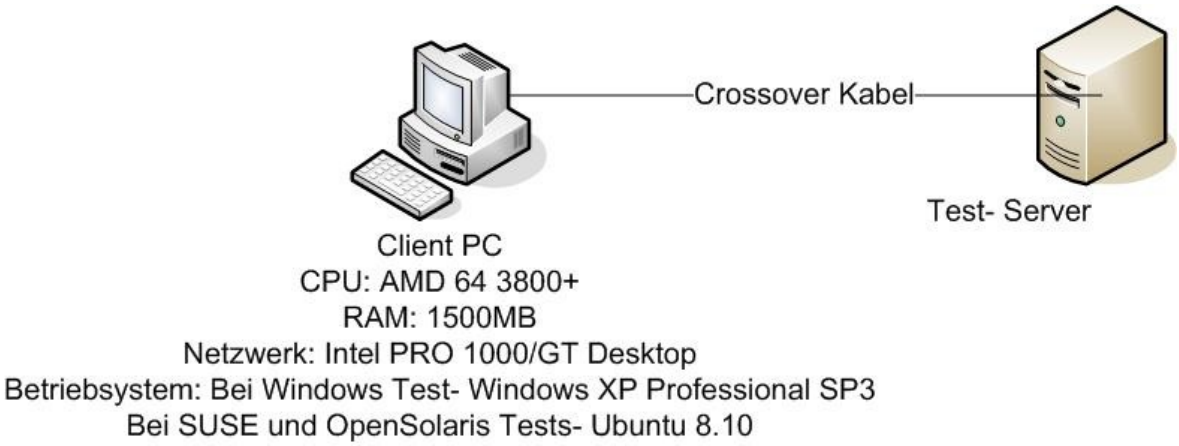

Abbildung 21: Testumgebung Netzwerktests

7.3 Testumgebung des Microsoft Servers 2008 Hyper-V

Es wurde von der Microsoft Site (http://www.microsoft.com/servers/hyper-v-server/default.mspx) die Version 1.0 des MicrosoftHyper-V Server 2008 (kostenlose Version) heruntergeladen und für die Installation auf eine CD gebrannt. Des Weiteren wurden noch die Linux-Integrationskomponenten für Hyper-V heruntergeladen und auf eine DVD gebrannt, da diese für die Unterstützung von Linux VM's benötigt werden.
Für die Administration wurde das Hyper-V Remote Management Tool für Windows Vista heruntergeladen (http://www.microsoft.com/downloads/details.aspx?FamilyId=A46D0047-E383-4688-9449-83373226126A&displaylang=en). Hierbei muss erwähnt werden, dass dieses Tool nicht leicht zu finden ist, da es auf der Site des Hyper-V Server keinen Link dazu gibt.

7.3.1 Installation

Es wurde von der Installations-DVD des Hyper-V gebootet. Der Installationsdialog ist fast identisch einer Windows Server 2008 Standardinstallation. Die Installation ist klar und strukturiert.

Nach Abschluss der Installation erscheinen am Bildschirm des Hyper-V Servers zwei Fenster. Ein Windows Cmd Fenster und ein zweites Fenster mit einem textbasierenden Menü für einige Grundeinstellungen, siehe Abbildung 22 (.die Daten stimmen in der Abbildung nicht mit dem Testrechner überein, da dieses Bild nur als Beispiel dient und aus einem Tutorial übernommen wurde)

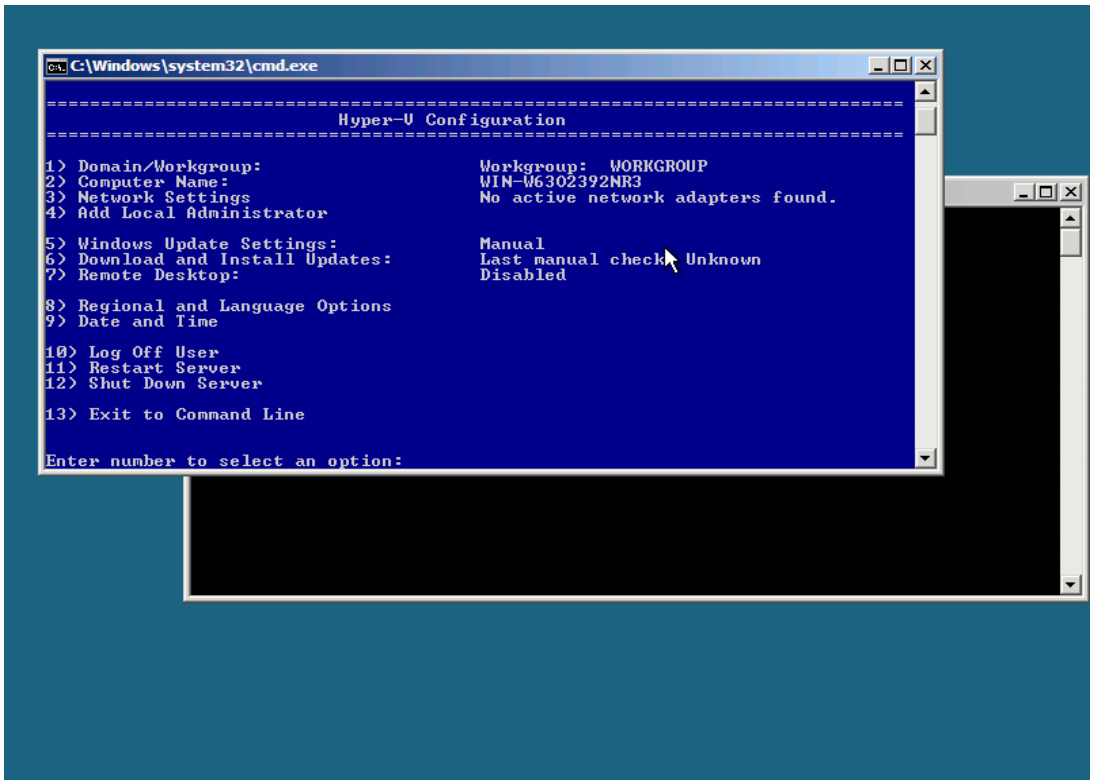

Abbildung 22: Windows Server 2008 Oberfläche direkt am Server (vgl.: http://blogs.msdn.com/blogfiles/virtual_pc_guy/WindowsLiveWriter/IllustratedInstallationofHyperVServer_848A/HyperVServerInstall20_2.png)

Der nächste Schritt ist die Installation des Management Tools auf einem Rechner mit Windows Vista Servicepack 1. Die Installation verlief ohne Probleme, die gab es erst bei der Verbindung zum Server mittels des Hyper-V Managers.

Die standardmäßig aktivierten Firewalls auf dem Windows Hyper-V Server und dem Windows Vista verhinderten die Verbindung. Nach Konfiguration der beiden Firewalls laut dieser Anleitung (http://blogs.technet.com/jhoward/archive/2008/03/28/part-1-hyper-v-remote-management-you-do-not-have-the-requested-permission-to-complete-this-task-contact-the-administrator-of-the-authorization-policy-for-the-computer-computername.aspx) funktionierte das Management Tool.

7.3.2 Erstellen der virtuellen Maschinen

Es wurden die drei Testmaschinen erstellt. Der Ablauf der Erstellung ist bei allen VM's sehr ähnlich, darum wird nur die Erzeugung der VM mit SUSE Linux Enterprise Server 10 genauer erläutert. Bei den anderen Maschinen wird dann nur mehr kurz darauf eingegangen und die Abweichungen erklärt.

Erstellen des SUSE Linux Enterprise 10 Servers

Zum Erstellen einer neuen VM gibt es den Menüpunkt „New – Virtual Machine“. Es wird ein Wizard gestartet der durch das Erstellen der VM leitet, siehe Abbildung 23.

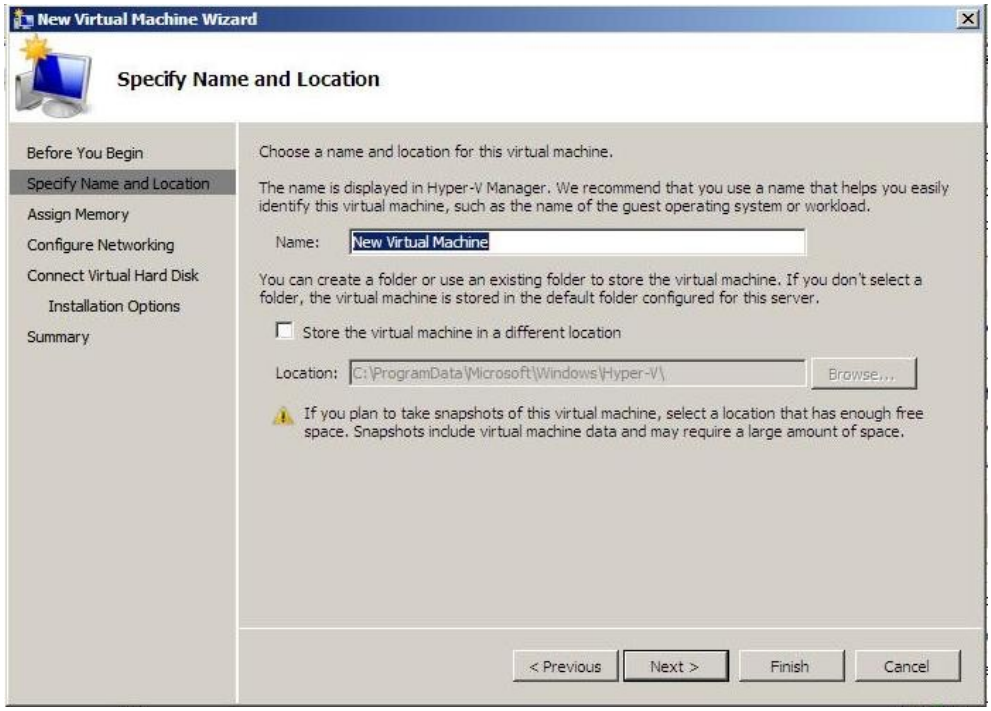

Abbildung 23: Hyper-V New Virtual Machine Dialog

Mit Hilfe dieses Wizard werden die Eigenschaften der VM konfiguriert:

- Name der Maschine → SUSE
- Speicherort der VM
- Hauptspeichergröße → 3000MB
- Zuweisung an ein virtuelles Netz (das Netz muss separat erstellt werden unter dem Menüpunkt Virtual Network Manager)
- Größe und Speicherort der virtuellen Festplatte → 40GB und auf der 500GB Festplatte
- Ort des Installationsmediums (.iso File oder physikalisches CD/DVD Laufwerk) für die Betriebssysteminstallation → physikalisches CD Laufwerk

Die Anzahl der CPUs kann man danach in den Settings der VM einstellen.
Die VM wird von der CD gebootet und wie auf einer realen Maschine installiert.
Nach der Installation müssen die „Integration Components“ für Linux installiert werden um das Betriebssystem anzupassen und alle Funktionen zu ermöglichen (siehe 4.4.2 Hypervisor aware bzw. Enlightened). Diese Komponenten befinden sich momentan noch im Beta Stadium und sind nur nach einer Registrierung über Microsoft Connect (http://connect.microsoft.com) erhältlich.
Sie werden mithilfe eines iso Files als CD in das System eingebunden und nach der Anleitung „Linux-Integrationskomponenten für Hyper-V”, die dem iso File beiliegt, installiert.

Danach ist die Netzwerkkarte in der VM verfügbar und kann konfiguriert werden.

Erstellen des Windows Server 2008

Das Erstellen der VM verläuft analog zur Vorgehensweise beim SUSE Linux Enterprise Server. Der einzige Unterschied ist, dass man nicht die „Integration Components“ für Linux sondern für Windows installiert. Danach ist die Maschine einsatzfähig.

Erstellen des OpenSolaris Servers

Das Erstellen der VM verläuft analog zur Vorgehensweise beim SUSE Linux Enterprise Server. Der einzige Unterschied ist das es keine „Integration Components“ für Solaris bzw. OpenSolaris gibt.
Unter den Settings der VM muss ein „Legacy Networkadapter“ der VM hinzugefügt werden, da der Standard Netzwerkadapter des Hyper- V nur nach einer Installation der „Integration Components“ funktioniert (siehe 4.2.4 Netzwerk). Doch aufgrund eines Bug des Hyper-V konnte trotzdem keine Netzwerkverbindung hergestellt werden, siehe http://bugs.opensolaris.org/view_bug.do?bug_id=6695174 .

7.3.3 Benchmarks ermittleln

Ergebnisse der Windows Benchmarks:

Prozessor Arithmetik:	
Dhrystone ALU	15,48 GIPS
Whetstone iSSE3	11,60 GFLOPS
Prozessor Kryptografie:	
AES 256	109 MB/s
SHA256	167 MB/s
Dateisystem:	
Laufwerksindex	85,24MB/s
Durchschnittliche Zugriffszeit	10ms
Speicherbandbreite:	
Integer Buff´d iSSE2	4,52 GB/s
Buff´d Fließkomma iSSE2	4,53 GB/s
Netzwerkbandbreite	
Bandbreite	36, 72MB/s
Latenzzeit	385 us

Tabelle 7: Hyper-v Benchmarkergebnisse Windows VM

Ergebnisse der SUSE Linux Benchmarks:

Allgemeine Tests	
Compress- gzip	162,25 s
Encode- mp3	61,84 s
SciMark2	51,05 MFLOPS
Super-PI	73,52 s
Dateisystem	
Iozone read	47,74 MB/s
Iozone write	53,43 MB/s
RAM	
RAMspeed- Copy- Integer	2336,8 MB/s
RAMspeed- Add- Integer	2582 MB/s
Netzwerkbandbreite	
Netperf senden	495 Mbit/s
Netperf empfangen	671 Mbit/s

Tabelle 8: Hyper-V Benchmarkergebnisse SUSE Linux VM

Ergebnisse der OpenSolaris Benchmarks:

Allgemeine Tests	
Compress- gzip	Nicht möglich
Bork File Encrypter	Nicht möglich
SciMark2	Nicht moöglich
Dd	59,5331 s
Netzwerkbandbreite	
Netperf senden	Nicht möglich
Netperf empfangen	Nicht möglich

Tabelle 9: Hyper-V Benchmarkergebnisse OpenSolaris VM

Es war kein Test außer dem mittels dd möglich, da der Netzwerkadapter nicht funktionierte und dadurch keine zusätzliche Software installiert werden konnte.

7.4 Testumgebung des VMware ESXi Servers

Als erstes wurde die aktuelle Version des ESXi Servers von der VMware Site heruntergeladen (https://www.VMware.com/tryvmware/?p=esxi). Für diese Teststellung wird die Version VMware ESX Server 3i- Version 3.5.0- Build 123629 verwendet. Dabei ist der VMware Infrastructure Client Version 2.5.0- Build 119801 für das Management des Servers.

Bei der Testhardware gab es einige Probleme bei der Treiberunterstützung des SATA Controllers des Mainboards. Es konnte keine zertifizierte Hardware für den ESXi Server angeschafft werden. Aufgrund dieser Tatsache mussten einige Dateien gepatched werden. Diese Anpassungen sind aber nicht Inhalt dieser Arbeit und werden daher nicht näher beleuchtet. Es gibt im Internet eine Site die sich unter anderem mit diesem Thema beschäftigt, die URL der Site ist http://www.vm-help.com/ . Laut den Anleitungen dieser Site wurden die Dateien geändert um die Hardwareunterstützung zu verbessern. Nach diesen Anpassungen funktionierte der ESXi Server problemlos und unterstützte die komplette Hardware des Testrechners.
Dieses angepasste ISO Image des ESXi wurde für die Installation auf eine CD gebrannt.

7.4.1 Installation

Der Testrechner wurde mit der zuvor gebrannten CD gebootet. Daraufhin kam es zur Auswahl ob man den ESXi- Server installieren möchte, siehe Abbildung 24

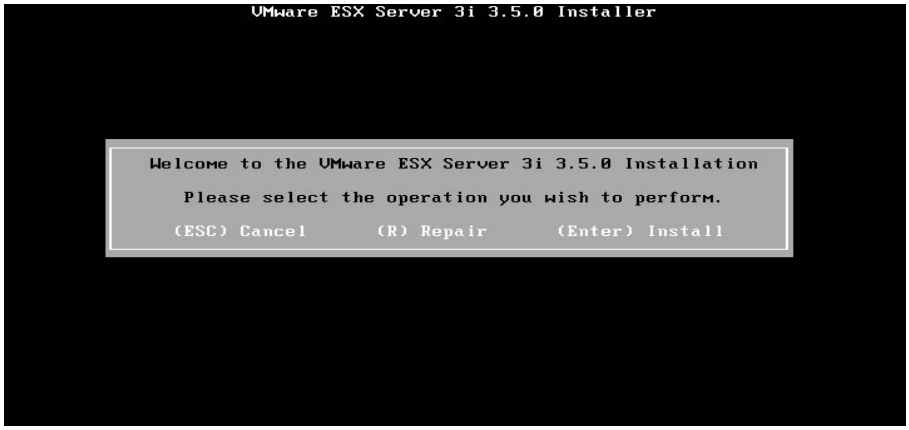

Abbildung 24: ESXi Installationsschirm

Es wurde Enter gedrückt für die Option- Install. In den nächsten Fenstern wurden die Lizenzvereinbarungen und der Installationsort abgefragt. Als Installationsort wurde die interne SATA Festplatte mit 70GB Kapazität gewählt, da auf der zweiten Festplatte dann die VM's gespeichert werden sollten. Nach der erfolgreichen Installation kam man zum Standardschirm des ESXi, das Direct Console User Interface (DLCI). Von diesem Punkt aus kann man alle Management Tätigkeiten erreichen die direkt auf dem Host möglich sind, siehe Abbildung 25 (die Daten über die Hardware, IP, usw. stimmen in der Abbildung nicht mit dem Testrechner überein, da dieses Bild nur als Beispiel dient und aus einem Tutorial übernommen wurde)

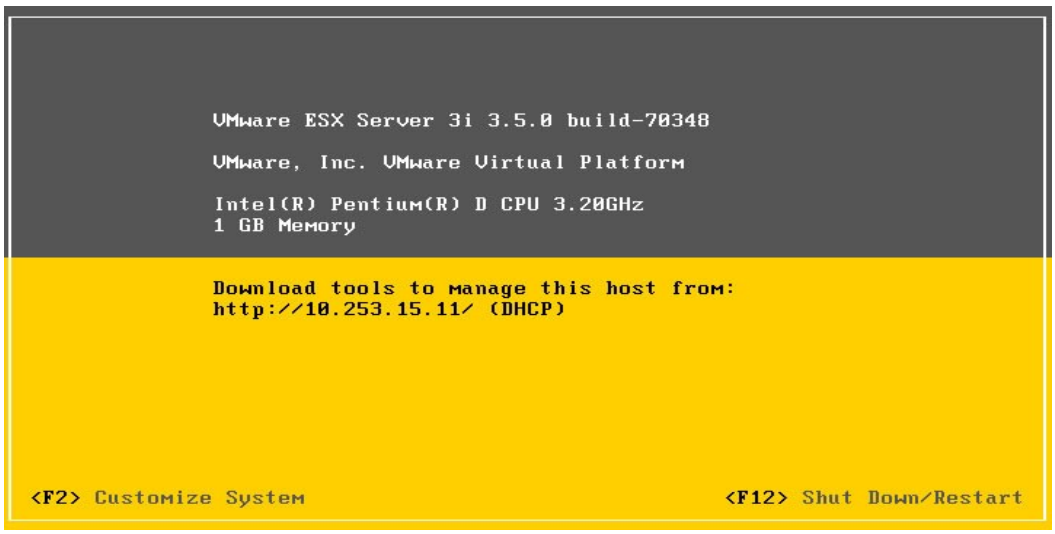

Abbildung 25: Standardschirm ESXi auf dem Host (vgl.: 6.2.2009, http://qemu-buch.de/de/index.php/Bild:VMware-ESX-Server-Install06.png)

In der Mitte des Schirms werden die Daten des Servers und seine aktuelle IP Adresse (wenn eine konfiguriert ist) angezeigt. Wenn er eine IP Adresse hat kann man mit einem Browser diese Adresse ansteuern und sich den Virtual Infrastructur Client (VI- Client) für Windows herunterladen, was hier auch gemacht wurde.
Des wichtigste Menü dieses Schirms ist mit F2 zu erreichen, zu finden links unten „Customize System“. Nach der Installation muss man in dieses Menü gehen um ein Passwort für den User root zu vergeben. Weiters kann man noch das Netzwerk für das Management mit einer statischen IP- Adresse konfigurieren , siehe Abbildung 26.

Vom Standardschirm aus kann man auch den Server mit der Taste F12 Herunterfahren bzw. Neustarten, siehe rechts unten.

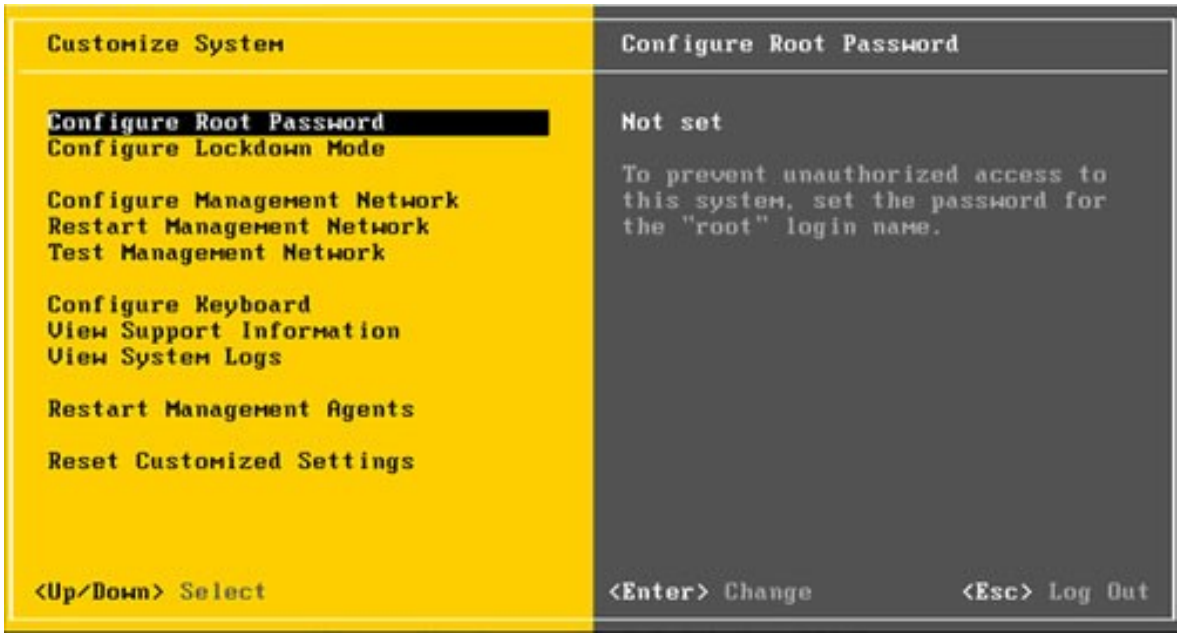

Abbildung 26: ESXi DLCI (vgl.: 6.2.2009, http://qemu-buch.de/de/index.php/Bild:Esxi-02.png)

Der nächste Schritt ist die Installation des VI- Clients auf einem Windows XP Rechner. Nach der Installation kann man sich mit Hilfe dieses Clients auf den Server verbinden (siehe Abbildung 27) und alle Management Aufgaben mithilfe dieser Oberfläche erledigen (siehe Abbildung 28).

Abbildung 27: VI Client Login

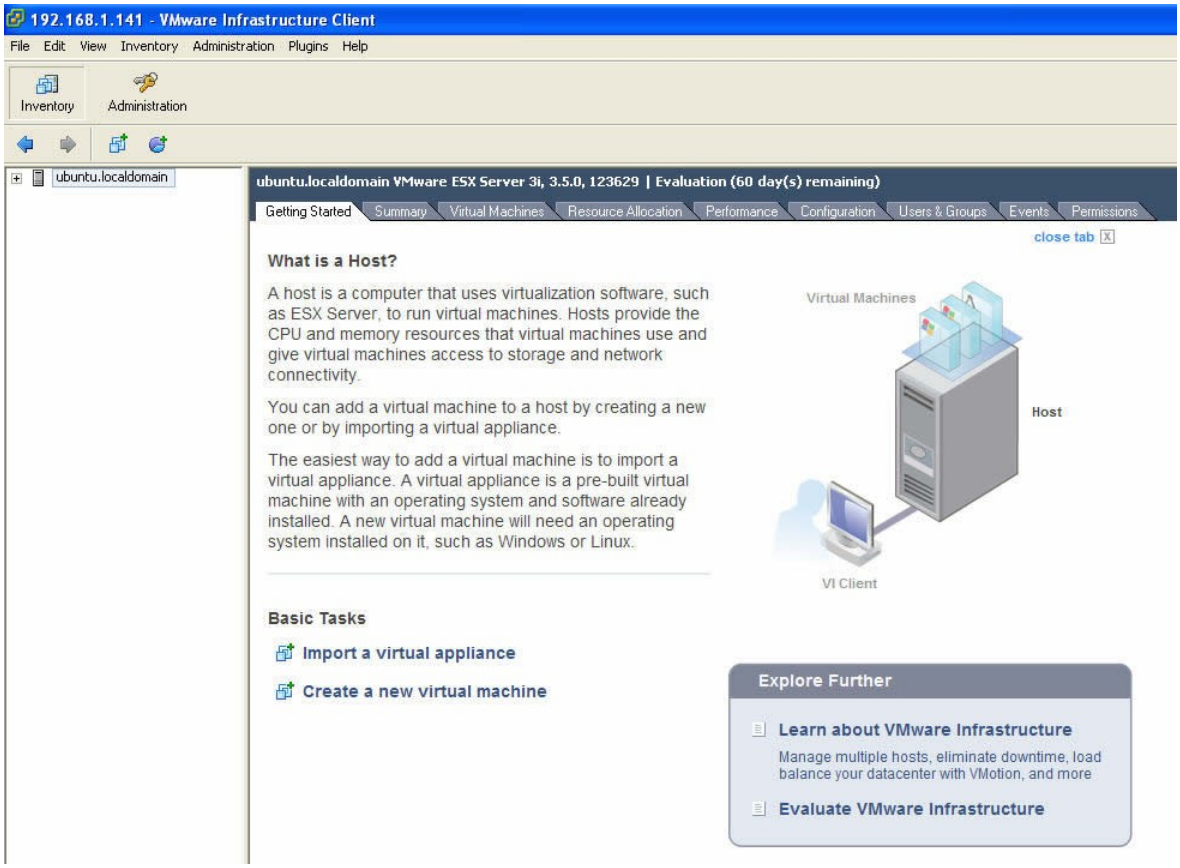

Abbildung 28: ESXi VI- Client Startschirm

Der nächste und letzte Schritt der Installation ist die Eingabe der Lizenznummer Reiter – Configuration – License Features.

Zur Installation kann man sagen, dass sie leicht zu tätigen ist und wenn man auf die zertifizierte Hardware achtet, sollte es auch zu keinen Problemen kommen.

7.4.2 Erstellen der virtuellen Maschinen

Es wurden die drei Testmaschinen erstellt. Der Ablauf der Erstellung ist bei allen VM's sehr ähnlich, darum wird nur die Erzeugung der VM mit SUSE Linux Enterprise Server 10 genauer erläutert. Bei den anderen Maschinen wird dann nur mehr kurz darauf eingegangen und die Abweichungen erklärt.

Erstellen des SUSE Linux Enterprise 10 Servers

Zum Erstellen einer neuen VM klickt man im VI- Client auf die Zeile „Create a new virtual machine“ oder über die Menüleiste unter File – New – Virtual Machine. Daraufhin öffnet sich ein Wizard der durch das Erstellen der VM leitet, siehe Abbildung 29.

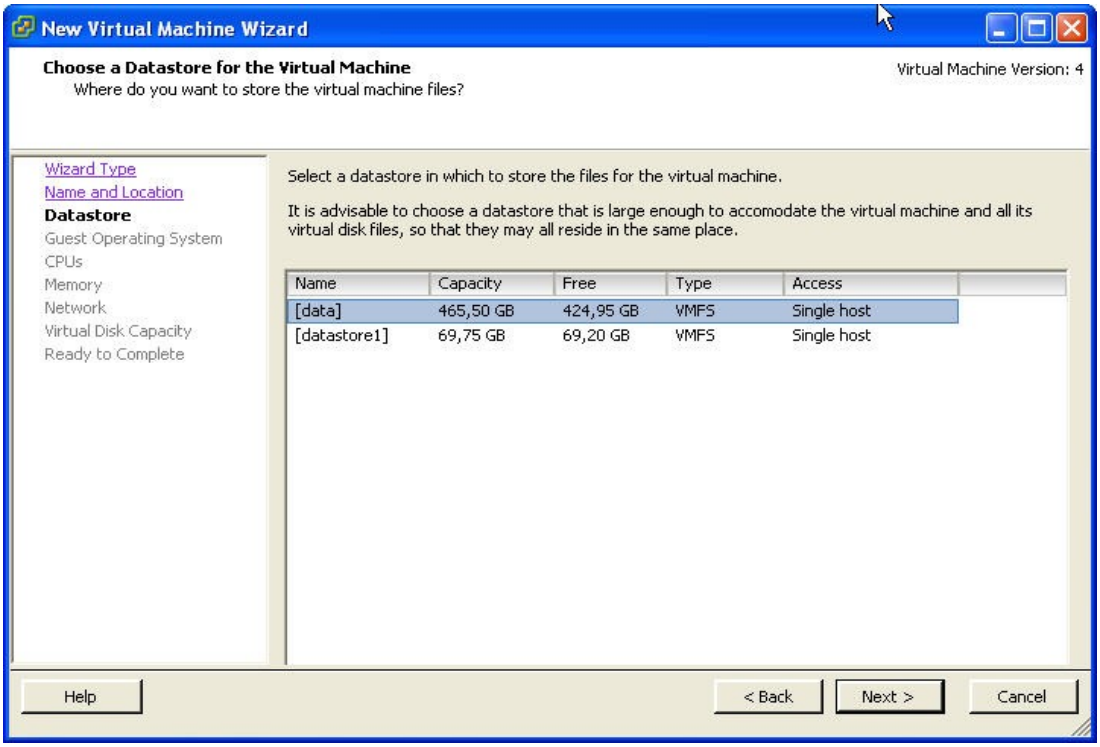

Abbildung 29: ESXi neue VM erstellen

Mit Hilfe dieses Wizard werden die Eigenschaften der VM konfiguriert:

- Welche Art der Konfiguration (Typical oder Custom) → Typical
- Name der Maschine → SUSE Enterprise 10
- Speicherort der VM → data (500 GB Platte auf dem Host)
- Betriebssystem das installiert wird → SUSE Linux Enterprise 10
- Anzahl der CPUs → 2
- Hauptspeichergröße → 3000MB
- Netzwerkadapter (Anzahl ,Hardware, Name) → 1 Netzwerkkarte, flexibel, VM Network
- Größe der virtuellen Festplatte → 40GB

Bei der Custom Konfiguration kann man noch zusätzlich einstellen:

- Storage Adapter Type
- Art der virtuellen Festplatte

Jetzt wo die Maschine erstellt ist, kann man sie über das linke Tree Menü anwählen und starten. Wenn sie läuft öffnet man eine Konsole über die Menüleiste oder mittels Rechtsklick auf die Maschine und „Open Console“.
Die Maschine startet jetzt wie ein normaler Rechner ohne Betriebssystem. Jetzt muss von der SUSE DVD gebootet werden da noch kein Betriebssystem installiert ist, siehe Abbildung 30.

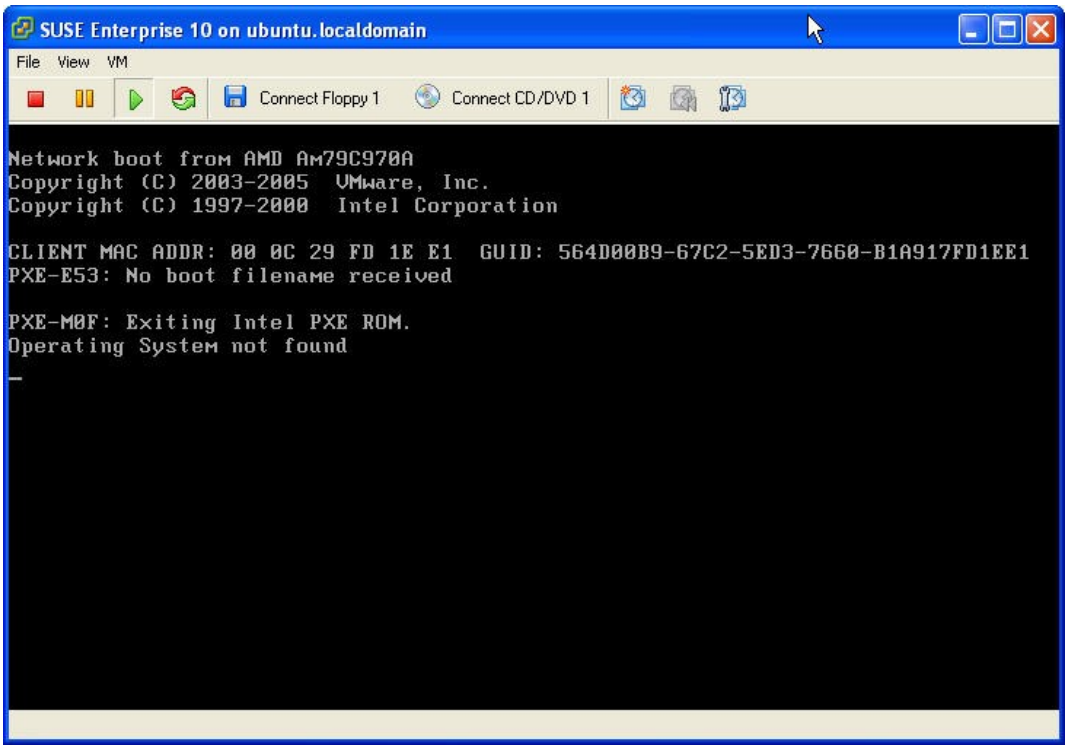

Abbildung 30: ESXi Konsole SUSE ohne Betriebssystem

Um eine DVD bzw. CD einzubinden klickt man auf den Button „Connect CD/DVD 1“, dann kann man ein ISO File in das virtuelle CD/DVD Laufwerk oder ein physikalisches Laufwerk einbinden . Das Image muss vom Remote Rechner erreichbar sein um es einbinden zu können. Es wird das Image der SUSE Installations- DVD eingebunden.

Nach einem Tastendruck bootet die VM von dem eingebundenen DVD Image. Bei der

Auswahl des SUSE Menüs wird Installation gewählt um die Installation zu starten.

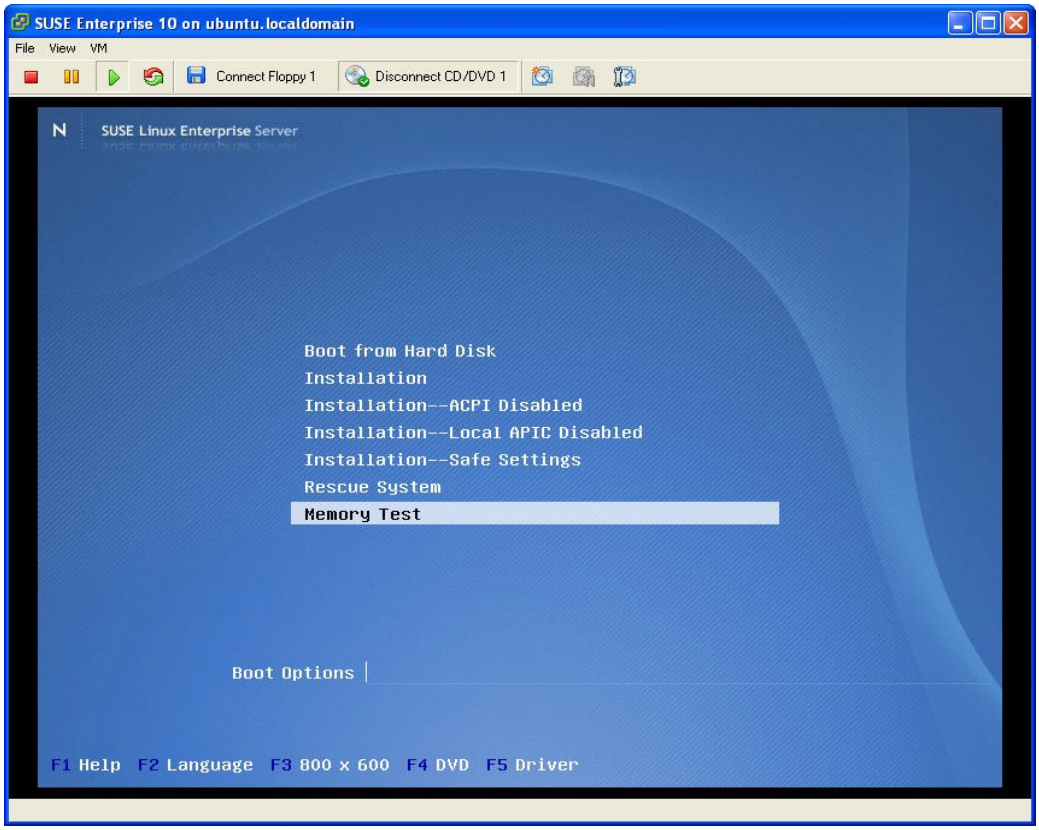

Abbildung 31: ESXi Konsole Startbildschirm SUSE Linux

Die Installation des Systems wird mit Hilfe des Wizard von SUSE, wie auf einem physikalischen Rechner durchlaufen. Die einzige Konfiguration die man im Vergleich zu einer Standardinstallation ändern soll ist der Bootloader von Grub auf LILO, laut dem Manuel vom ESXi Server. Danach wird die Installation normal gestartet.

Die erste Tätigkeit auf dem neuen System ist die Installation der VMware Tools um das volle Potenzial der VM auszuschöpfen. Die Tools werden installiert indem man in der Menüleiste unter VM auf Install/Upgrade VMware Tools klickt. Dadurch wird ein CD-Image, mit den Tools darauf eingebunden.
Bei SUSE Linux muss man bevor man sie installiert Ipv6 ausschalten, da es sonst zu einer Fehlermeldung kommt und man die bessere Performance des Netzwerkadapters nicht nutzen kann.

(vgl.: VMware 2009 S. 185 f)

Erstellen des Windows Server 2008 Enterprise Servers

Die Installation erfolgt analog zur bereits erläuterten Installation des SUSE Servers. Die Unterschiede bestehen darin, dass die Windows Server 2008 DVD eingebunden wird und keine Änderungen in der Standardinstallation notwendig sind. Die Installation läuft ganz normal durch.

Erstellen der OpenSolaris VM

Die Installation erfolgt analog zur bereits erläuterten Installation des SUSE Servers. Der Unterschied besteht darin, dass die OpenSolaris DVD eingebunden wird.

7.4.3 Benchmarks ermitteln

Ergebnisse der Windows Benchmarks:

Prozessor Arithmetik:	
Dhrystone ALU	11,96 GIPS
Whetstone iSSE3	8,97 GFLOPS
Prozessor Kryptografie:	
AES 256	84 MB/s
SHA256	132 MB/s
Dateisystem:	
Laufwerksindex	100,17 MB/s
Durchschnittliche Zugriffszeit	7ms
Speicherbandbreite:	
Integer Buff´d iSSE2	4,22 GB/s
Buff´d Fließkomma iSSE2	4,23 GB/s
Netzwerkbandbreite	
Bandbreite	40,54 MB/s
Latenzzeit	271 us

Tabelle 10: ESXi Benchmarkergebnisse Windows VM

Ergebnisse der SUSE Linux Benchmarks:

Allgemeine Tests	
Compress- gzip	151,96 s
Encode- mp3	61,19 s
SciMark2	69,23 MFLOPS
Super-PI	60 s
Dateisystem	
Iozone read	286 MB/s
Iozone write	72 MB/s
RAM	
RAMspeed- Copy- Integer	2573,37 MB/s
RAMspeed- Add- Integer	3039,74 MB/s
Netzwerkbandbreite	
Netperf senden	642,75 Mbit/s
Netperf empfangen	707,1 Mbit/s

Tabelle 11: ESXi Benchmarkergebnisse SUSE Linux VM

Ergebnisse der OpenSolaris Benchmarks:

Allgemeine Tests	
Compress- gzip	161,07 s
Bork File Encrypter	64,86 s
SciMark2	53,21 MFLOPS
Dd	76,4056 s
Netzwerkbandbreite	
Netperf senden	216 Mbit/s
Netperf empfangen	41 Mbit/s

Tabelle 12: ESXi Benchmarkergebnisse OpenSolaris VM

7.5 Teststellung des Citrix Xen Servers

Es wurde von der Citrix Site die Version 5.0.0 (#10918p) des Citrix XenServer 5 Express Edition (kostenlose Version) heruntergeladen (www.citrix.com) und für die Installation auf eine CD gebrannt. Des Weiteren wurde noch das Linux Pack ISO heruntergeladen und auf eine CD gebrannt, da sie für die Unterstützung von Linux VM's benötigt wird.
Für die Administration wurde die aktuelle Version des XenCenters von der Citrix Site heruntergeladen.

7.5.1 Installation

Der Testrechner wurde mit der zuvor gebrannten CD gebootet. Es wird ein Wizard zur Installation des XenServers gestartet.
Im Laufe dieser Installation werden diverse Einstellungen getroffen:

- Verwendete Tastatur
- Upgrade oder Neuinstallation (Neuinstallation)
- Installationsort des XenServers (/dev/sda = 80Gb Festplatte im Testrechner)
- Speicherort der VM's (/dev/sdb = 500 Gb Festplatte im Testrechner)
- Auswahl des Installationsmediums: Möglich wären local, HTTP, FTP oder NFS (lokal von der Cdrom)
- Abfrage ob die Linuxunterstützung mitinstalliert werden soll (ja)
- Auswahl des Netzwerkadapters für das Management LAN über die MAC Adresse (eth0) und Konfiguration des Adapters
- Zeitzonen Einstellung und NTP Server
- Danach erfolgt die Installation des XenServers und die Installation des Linux Packs

Nach dem Neustart startet der XenServer die xconsole, siehe Abbildung 32.

Abbildung 32: XenServer xconsole (vgl.: 6.2.2009, http://wiki.computerwoche.de/lib/exe/detail.php/virtualisierung/xen/xsconsole-1.png?id=virtualisierung%3Axen%3Axenserver5&cache=cache)

Der nächste Schritt ist die Installation des XenCenters auf einem Windows XP Rechner mittels der .msi Datei von der Citrix Site. Nach dem Start des Managementtools fügt man den XenServer (siehe Abbildung 33) hinzu um ihn mit dem XenCenter zu managen. Für die weiteren Managementaufgaben wird in dieser Arbeit das XenCenter verwendet da es eine sehr einfache und komfortable Art der Verwaltung ist.

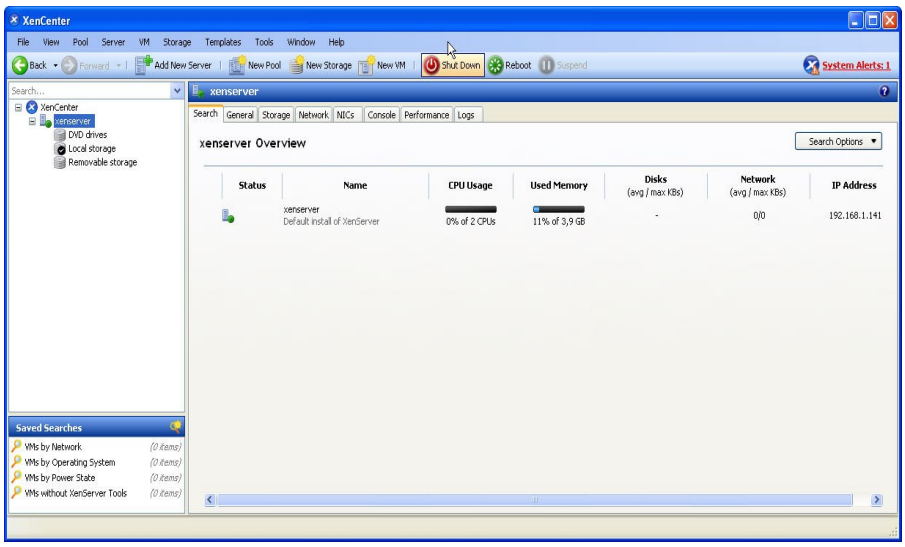

Abbildung 33: XenCenter

7.5.2 Erstellen der virtuellen Maschinen

Es werden die drei Testmaschinen erstellt. Der Ablauf der Erstellung ist bei allen Maschinen ähnlich daher wird nur die Erzeugung des Windows Servers näher erläutert. Bei den anderen Maschinen wird dann nur mehr kurz auf die Abweichungen eingegangen.

Erstellen der Windows Server 2008 VM

Um Windows in einer Xen VM überhaupt installieren zu können muss die CPU des physikalische Servers Hardwarevirtualisierung unterstützen (Intel VT oder AMD-V).
Die Installation besteht aus zwei Teilen:

- Installation des Windows Systems
- Installation der paravirtualisierten Treiber die Citrix Tools for Virtual Machines genannt werden.

Die eigentliche Installation der VM erfolgt durch das Klonen eines passenden Templates, das von Citrix mitgeliefert wird, mittels des XenCenters oder über die CLI.

Der erste Schritt ist die Bereitstellung der CD bzw. DVD Images des Betriebssystems. Das kann über eine NFS oder SMB/CIFS Freigabe erfolgen. Man klickt auf „New Storage“ und dann kann dann mittels eines Wizards die Freigabe auf der die ISOs liegen einbinden. (siehe Abbildung 34)

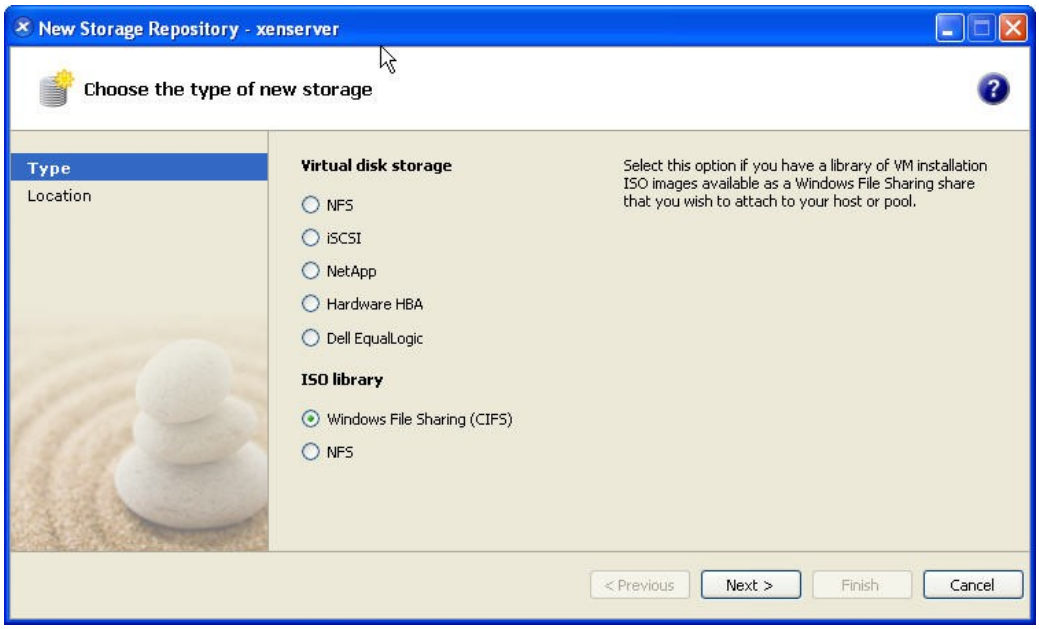

Abbildung 34: XenServer ISOs einbinden

Der nächste Schritt ist dann die neue VM zu erstellen. Dazu klickt man auf den Button „New Vm“. Es öffnet sich ein Wizard der durch die Erstellung der VM leitet, siehe Abbildung 35.

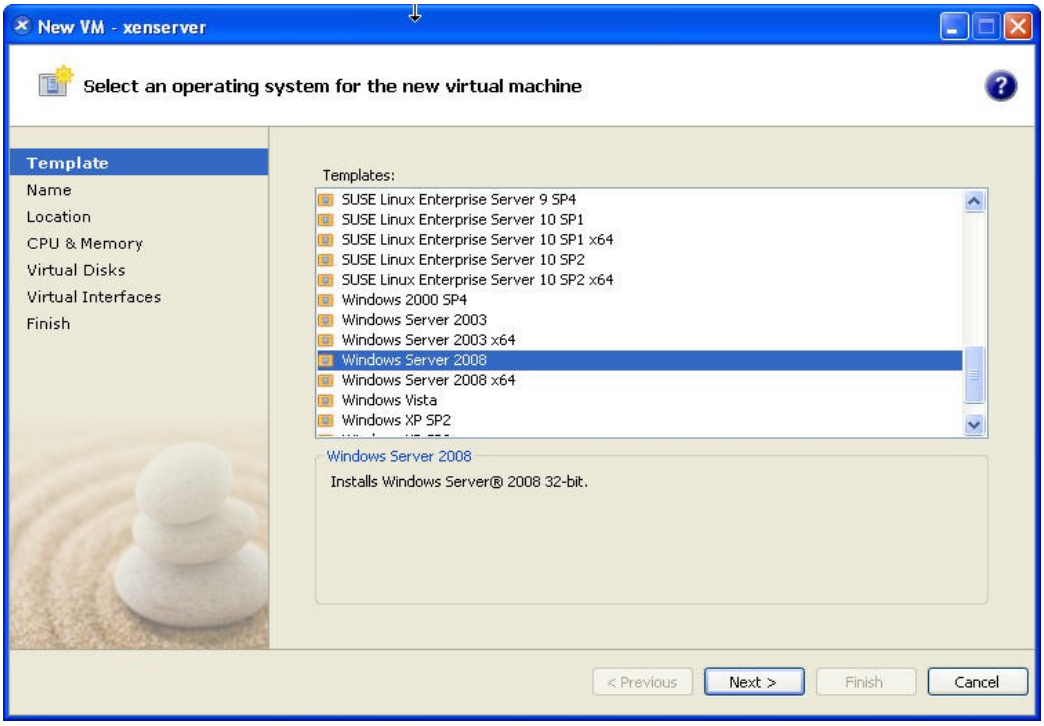

Abbildung 35: XenServer erstellen einer VM

Es wird das Template, für das Betriebssystem, das installiert werden soll, ausgewählt. Weiters werden noch weitere Konfigurationen mit diesem Wizard erledigt:

- Name der VM →Windows Server 2008
- ISO (Image des Installationsmediums) oder Zuweisung des physikalisch CD/DVD Laufwerks des Servers → ISO File der Windows Server 2008 DVD
- Anzahl der CPUs →2
- Größe des RAMs →3000MB
- Größe der virtuellen Festplatte und Speicherplatz →40Gb und Local Storage
- Konfiguration der Netzwerkadapter (Anzahl und an welches virtuelles Netzwerk sie angeschlossen sind → 1 Netzwerkkarten, Network 0

Danach wird die VM gestartet und man kann mittels des Reiters „Console“ im XenCenter auf den Windows Server 2008. Die VM wird vom ISO File wie von einer normalen CD/DVD gebootet. Man kann mit der Installation des Betriebssystems beginnen und sie wie auf einem physikalischen Rechner durchführen.

Wenn das System installiert ist werden die XenServer Tools installiert um die paravirtualisierten Treiber des XenServers zu nutzen und dadurch die Performance zu steigern und weitere Funktionen zugänglich zu machen. Um die Tools zu installieren klickt man auf die Menüleiste „VM -Install XenServer Tools“. Dadurch wird das „xs-tools.iso“ auf der VM eingebunden. Man führt auf der CD das File xensetup.exe aus und dann werden die Tools installiert. Nach zweimaligem Neustart der VM ist die Installation erledigt.

(vgl.: Citrix Systems, Inc. 2008a, S13 f)

Erstellen des SUSE Linux Enterprise 10 Servers

Die Installation erfolgt fast gleich wie die des Windows Server 2008 auf dem XenServer. Es wird nur bei der Erstellung der neuen VM die SUSE Distribution ausgewählt und das richtige Image zugewiesen.
Unterschiede gibt es erst nach der eigentlichen Installation. Das Problem ist, dass man mittels des Reiters „Console“ des XenCenters nach der Standardinstallation nur auf die Konsole des SUSE Server kommt und es keine grafische Oberfläche gibt. Um dieses Problem zu beheben muss zuerst der „Linux guest agent“ installiert werden.

Die unterstützten Linux Distributionen benötigten keine speziellen Treiber da sie bereits für Paravirtualisierung ausgelegt sind.
Dieser Agent wird ebenfalls über die Menüleiste „VM – Install XenServer Tools“ installiert. Dabei muss man aber im Linux die CD manuell mounten und dann ein „install“ Skript starten. Nach einem Neustart der VM ist der Agent fertig installiert.
Der nächste Schritt zur grafischen Oberfläche ist die Konfiguration des VNC Servers (XenCenter verwendet für den Remote Zugriff auf die Server das VNC Protokoll) auf dem SUSE Server. Der VNC Server wird mittels „yast“ aktiviert und danach muss noch die Konfiguration des „xinetd Daemons“ angepasst werden. Diese Anpassungen findet man in dem Dokument „XenServer Virtual Machine Installation Guide“. Wenn alle Anpassungen gemacht wurden kann man mittels des XenCenters auf die grafische Oberfläche zugreifen.

Erstellen der OpenSolaris VM

Es war zu Beginn nicht möglich OpenSolaris in einer VM des XenServers zu installieren, denn es gab Probleme mit dem Treiber des Storage Controller. Es wurden einige Versuche mit Änderungen in den Bootparametern (Disable DMA) unternommen. Danach lies es sich zwar installieren aber lief so langsam, dass keine brauchbare Bedienung möglich war. Daher wurde der Versuch mit OpenSolaris abgebrochen und als nicht Durchführbar gekennzeichnet.

7.5.3 Benchmarks ermitteln

Ergebnisse der Windows Benchmarks:

Prozessor Arithmetik:	
Dhrystone ALU	15,63 GIPS
Whetstone iSSE3	11,63 GFLOPS
Prozessor Kryptografie:	
AES 256	111 MB/s
SHA256	168 MB/s
Dateisystem:	
Laufwerksindex	97,04 MB/s
Durchschnittliche Zugriffszeit	8 ms
Speicherbandbreite:	
Integer Buff´d iSSE2	4,73 GB/s
Buff´d Fließkomma iSSE2	4,74 GB/s
Netzwerkbandbreite	
Bandbreite	41,36 MB/s
Latenzzeit	196 us

Tabelle 13: XenServer Benchmarkergebnisse Windows VM

Ergebnisse der SUSE Linux Benchmarks:

Allgemeine Tests	
Compress- gzip	145,75 s
Encode- mp3	57,76 s
SciMark2	64,08 MFLOPS
Super-PI	50,8 s
Dateisystem	
Iozone read	397,58 MB/s
Iozone write	126,43 MB/s
RAM	
RAMspeed- Copy- Integer	2679,85 MB/s
RAMspeed- Add- Integer	3206,77 MB/s
Netzwerkbandbreite	
Netperf senden	656,74 Mbit/s
Netperf empfangen	732,71 Mbit/s

Tabelle 14: XenServer Benchmarkergebnisse SUSE Linux VM

7.6 Teststellung der nativen Systeme

Die Testhardware wurde an die Installation der nativen Systeme angepasst indem 1GB RAM entfernt wurde. Dadurch sind die Eckdaten der VM's und der physikalischen Maschine für die Ermittlung der Benchmarks gleichwertig und es kommt zu keiner Verzerrung der Ergebnisse.

Durch die Ergebnisse dieser Test lässt sich der Overhead, der bei der Virtualisierung entsteht, ermitteln und darstellen. Durch den Vergleich der Ergebnisse der nativen Maschine mit den Ergebnissen aus den virtuellen Umgebungen kann die Effektivität der Produkte gezeigt werden.

Bei dieser Teststellung wurde das jeweilige Betriebssystem auf die 80GB Festplatte installiert. Dabei wurden die Einstellungen auf den Standardwerten belassen.

Nach der erfolgreichen Installation wurden die Benchmarks ermittelt.

7.6.1 Auswertung der Benchmarks

Ergebnisse der Windowsbenchmarks:

Prozessor Arithmetik:	
Dhrystone ALU	15,94 GIPS
Whetstone iSSE3	12,04 GFLOPS
Prozessor Kryptografie:	
AES 256	113 MB/s
SHA256	173 MB/s
Dateisystem:	
Laufwerksindex	61,97 MB/s
Durchschnittliche Zugriffszeit	7ms
Speicherbandbreite:	
Integer Buff´d iSSE2	4,02 GB/s
Buff´d Fließkomma iSSE2	4,51 GB/s
Netzwerkbandbreite	
Bandbreite	47,96 MB/s
Latenzzeit	161 us

Tabelle 15: Native Windows Benchmarks

Ergebnisse der SUSE Linux Benchmarks:

Allgemeine Tests	
Compress- gzip	144,21 s
Encode- mp3	57,95 s
SciMark2	52,17 MFLOPS
Super-PI	49,38 s
Dateisystem	
Iozone read	739,35 MB/s
Iozone write	99,64 MB/s
RAM	
RAMspeed- Copy- Integer	1588,66 MB/s
RAMspeed- Add- Integer	2265,34 MB/s
Netzwerkbandbreite	
Netperf senden	669,11 Mbit/s
Netperf empfangen	743,53 Mbit/s

Tabelle 16: Native SUSE Linux Benchmarks

Ergebnisse der OpenSolaris Benchmarks:

Allgemeine Tests	
Compress- gzip	162,91 s
Bork File Encrypter	121,3 s
SciMark2	37,53 MFLOPS
Dd	58,3602 s
Netzwerkbandbreite	
Netperf senden	29,99 Mbit/s
Netperf empfangen	690 Mbit/s

Tabelle 17: Native OpenSolaris Benchmarks

7.7 Vergleich der Benchmarkergebnisse der Virtualisierungslösungen

In diesem Punkt werden die Ergebnisse der Tests von den Betriebssystemen pro Virtualierungsprodukt gegenübergestellt. Damit ist ersichtlich welche Lösung weniger Virtualisierungs- Overhead erzeugt. Es wird nur auf den Windows Server und den SUSE Server eingegangen, da diese beiden offiziell unterstützt sind und der OpenSolaris Server bei zwei von drei Produkten eingeschränkt oder gar nicht funktionierte.

Ergebnisse der Windows Benchmarks im Vergleich:

Prozessor Arithmetik:	Microsoft Hyper-V Server	VMware ESXi Server	Citrix XenServer 5	Windows Server 2008 native
Dhrystone ALU	15,48 GIPS	11,96 GIPS	15,63 GIPS	15,94 GIPS
Whetstone iSSE3	11,60 GFLOPS	8,97 GFLOPS	11,63 GFLOPS	12,04 GFLOPS
Prozessor Kryptografie:				
AES 256	109 MB/s	84 MB/s	111 MB/s	113 MB/s
SHA256	167 MB/s	132 MB/s	168 MB/s	173 MB/s
Dateisystem:				
Laufwerksindex	85,24MB/s	100,17 MB/s	97,04 MB/s	61,97 MB/s
Durchschnittliche Zugriffszeit	10ms	7ms	8 ms	7ms
Speicherbandbreite:				
Integer Buff´d iSSE2	4,52 GB/s	4,22 GB/s	4,73 GB/s	4,02 GB/s
Buff´d Fließkomma iSSE2	4,53 GB/s	4,23 GB/s	4,74 GB/s	4,51 GB/s
Netzwerkbandbreite				
Bandbreite	36, 72MB/s	40,54 MB/s	41,36 MB/s	47,96 MB/s
Latenzzeit	385 us	271 us	196 us	161 us

Tabelle 18: Vergleich der Windows Benchmarks

Ergebnisse der SUSE Linux Benchmarks im Vergleich:

Allgemeine Tests	Microsoft Hyper- V Server	VMware ESXi Server	Citrix XenServer 5	SUSE Linux Enterprise Server
Compress- gzip	162,25 s	151,96 s	145,75 s	144,21 s
Encode- mp3	61,84 s	61,19 s	57,76 s	57,95 s
SciMark2	51,05 MFLOPS	69,23 MFLOPS	64,08 MFLOPS	52,17 MFLOPS
Super-PI	73,52 s	60 s	50,8 s	49,38 s
Dateisystem				
Iozone read	47,74 MB/s	286 MB/s	397,58 MB/s	739,35 MB/s
Iozone write	53,43 MB/s	72 MB/s	126,43 MB/s	99,64 MB/s
RAM				
RAMspeed- Copy- Integer	2336,8 MB/s	2573,37 MB/s	2679,85 MB/s	1588,66 MB/s
RAMspeed- Add- Integer	2582 MB/s	3039,74 MB/s	3206,77 MB/s	2265,34 MB/s
Netzwerkbandbreite				
Netperf senden	495 Mbit/s	642,75 Mbit/s	656,74 Mbit/s	669,11 Mbit/s
Netperf empfangen	671 Mbit/s	707,1 Mbit/s	732,71 Mbit/s	743,53 Mbit/s

Tabelle 19: Vergleich der SUSE Linux Benchmarks

Bei den RAM Tests der nativen Installation war das Ergebnis, dass die virtuellen Umgebungen schneller sind. Dieses Ergebnis kam daher, dass ein RAM-Baustein aus dem Testrechner zur Reduktion des RAMs auf 3 GB ausgebaut wurde. Dadurch waren die RAM Slots unsymmetrisch bestückt und es kam zu den schlechteren Ergebnissen.

Bei den Dateisystem Tests sind die nativen Werte bei den Benchmarks schlechter da der Test nicht an die virtuelle Umgebung angepasst ist. Die Werte werden dadurch verfälscht, dass der darunter liegende Hypervisor einige Daten im RAM hält und nicht auf die Festplatte schreibt.

Daher kann man bei den beiden Tests keine sichere Aussage zum Virtualisierungs – Overhead geben. Aber die Vergleiche zwischen den virtuellen Umgebungen wurden dadurch nicht beeinflusst.

Aus der Auswertung der Benchmark Ergebnisse kann man erkennen, dass Paravirtualisierung die bessere Gesamtperformance bietet. In den meisten Fällen liegt der XenServer vorne.
Der Hyper-V Server kann vor allem bei Windows Gästen punkten und liegt bei diesen nur knapp hinter dem XenServer. Die Linux Inegration Components sind beim Hyper-V noch im Beta Stadium, was man auch an den Ergegbnissen mit den Linux Gästen sehen kann. Der ESXi Server liegt aber nicht weit hinter den Ergebnissen der beiden Konkurrenten zurück. Bei der Virtualisierung des SUSE Server kann er sich bei allen Punkten vom Hyper-V Server absetzen.

8 Bewertung

Die Bewertung der Produkte beruht auf den Ergebnissen des theoretischen Vergleichs, der exemplarischen Implementierungen und den ausgeführten Benchmarks.

Weiters ist das Ergebnis nicht für alle Einsatzgebiete und Anwendungszwecke gültig, sondern bezieht sich auf die Annahme einer „ Ein Serverlösung“ für kleine und mittlere Betriebe. Bei diesen lassen sich die kostenlosen Varianten der Virtualisierungslösungen einsetzen und die „ Enterprise Features“ wie Hochverfügbarkeit oder „ Live Imigration werden nicht benötigt.

Beim theoretischen Vergleich der Features gab es keinen eindeutigen Sieger, ein großer Teil der Features ist gleichwertig und nur bei ein paar Punkten konnte sich die eine oder andere Lösung Vorteile verschaffen.
Wenn man vor allem auf viele unterstützte Betriebssysteme wert legt und auf umfangreiche Management Tools dann ist der Citrix XenServer 5 der Sieger in dieser Kategorie. Aber wenn man sich in einer Windowsumgebung bewegt spricht natürlich auch einiges für den Windows Hyper-V Server da er sich in eine Windowsumgebung sehr gut integrieren lässt.

Bei den exemplarischen Implementierungen kam es zu keinen positiven wie negativen Überraschungen, alle Produkte funktionierten wie erwartet und wenn man sich an die Vorgaben der Hersteller hält sollte es auch zu keinen Problemen kommen.

Die Benchmarks unterstützten das Ergebnis des theoretischen Vergleichs. Die Performance der paravirtualisierten Systeme war in den meisten Fällen besser als die des ESXi Servers. Diese guten Ergebnisse kamen aber nur zustande wenn es ausgereifte Anpassungen der virtualisierten Systeme gibt, wenn nicht verschlechtern sich die Ergebnisse und der Vorteil der Paravirtualisierung ist dahin. Bei der Performance konnte der XenServer überzeugen. Der Hyper- V Server konnte mit guter Performance bei Windows VM's aufzeigen, aber bei der VM mit SUSE Linux sank die Performance unter die des ESXi Servers. Der ESXi Server brachte in allen Belangen ein akzeptables Ergebnis und war manchmal besser und manchmal schlechter als die Konkurrenz.

Das Ergebnis dieser Bewertung ist, dass der Citrix XenServer 5.0 die beste Wahl in diesem Fall ist da er die beste Performance liefert, eine große Anzahl von Betriebssystemen unterstützt und eine Vielzahl an Management Tools hat.

9 Anhang

9.1 Anhang A: Literaturverzeichnis

Bücher:

Savill, John (2008): The complete guide to Windows server 2008. Addison-Wesley

Prabhakar Chaganti (2007): Xen Virtualisation. Packt Publishing Ltd.

David Chisnall (2007):The Definitive Guide to the Xen Hypervisor. Prentice Hall

Warnke, Robert, Ritzau, Thomas (2008): QEMO Virtuelle Computer für viele Betriebssysteme. Books on Demand GmbH

Shields, Greg (2007): Der schnelle Weg zur Wahl der richtigen Virtualisierungslösung. Realtimepublishers

Zimmer, Dennis (2007): VMware ESX- Automatisierung,Befehle, Scripting. Galileo Press

Zeitschriften:

Hantelmann, Fred (2007): Marktübersicht: Server-Virtualisierung,Ins Glas geschaut In: iX6/2007

Hantelmann, Fred (2008): Microsofts Hyper-V Server 2008 zum Ausprobieren, Muckefuck aus Redmond In: iX12/2008

Segor, Christian (2008): Microsofts neue Server- Konsolidierung: Windows Server Hyper-V Mit direktem Zugriff. In iX1/2008

Whitepapers:

VMware (2007): Understanding Full Virtualization, Paravirtualzation, and Hardware Assist. http://www.vmware.com/files/pdf/VMware_paravirtualization.pdf

VMware (2007a): VMware Virtual Networking Concepts, http://www.vmware.com/files/pdf/virtual_networking_concepts.pdf

VMware (2007b): VMware Virtual Machine File System: Technical Overview and Best Practices, http://www.vmware.com/pdf/vmfs-best-practices-wp.pdf

VMware (2007c): Performance Characteristics of VMFS and RDM, http://www.vmware.com/files/pdf/vmfs_rdm_perf.pdf

VMware (2008): Configurations Maximum. http://www.vmware.com/pdf/vi3_35/esx_3/r35u2/vi3_35_25_u2_config_max.pdf

VMware (2009): Guest Operatin System Installation Guide. http://www.vmware.com/pdf/GuestOS_guide.pdf

Charu Chaubal (2007): The Architecture of VMware ESXi, http://www.vmware.com/files/pdf/vmware_esxi_architecture_wp.pdf

Charu Chaubal (2007a): Managing VMware ESXi, http://www.vmware.com/files/pdf/vmware_esxi_management_wp.pdf

IBM Systems (2005): Virtualization Version 2 Release 1. http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/eicay/eicay.pdf

Microsoft Corporation (2008): Windows Server 2008 Hyper- V Technical Overview, http://download.microsoft.com/download/4/2/b/42bea8d6-9c77-4db8-b405-6bffce59b157/Hyper-V%20Technical%20Overview.docx

Microsoft Corporation (2008a): Windows Server 2008 Hyper- V Planning and Deploying Guide, http://download.microsoft.com/download/8/1/5/81556693-1f05-494a-8d45-cdeeb6d735e0/HyperV_Deploy.doc

Microsoft Corporation (2008b): Windows Server 2008 Hyper-V, http://download.microsoft.com/download/c/b/2/cb23f604-a8f7-4888-8784-ddf185b92c18/DE_HyperVDatenblattV1_customerready.pdf

Withoff Oliver (2008): XenServer Storage Overview, http://support.citrix.com/article/CTX119088

Citrix Systems, Inc. (2008a): XenServer Virtual Machine Installation Guide 5.0.0, http://support.citrix.com/servlet/KbServlet/download/18053-102-19050/guest.pdf

Citrix Systems, Inc. (2008b) XenServer Administrator's Guide 5.0.0, http://support.citrix.com/servlet/KbServlet/download/18051-102-19048/reference.pdf

Anleitungen bzw. Hilfe von Programmen:

SiSoftware (2008):SiSoftware Sandra Hilfe, Bestandteil der Software SiSoftware Sandra

Präsentationen:

Vmware: VMware ESXi 3.5 update 2,
http://www.vmware.com/files/pdf/ESX_Server_3i_presentation.pdf

9.2 Anhang B: Quellenangaben aus dem Internet

Zimmer, Dennis (30.01.2008), wiki.computerwoche.de

Radonic, Andrej *(8.03.2008), wiki.computerwoche.de*

Author unbekannt (13.1.2009), www.itwissen.info

Author unbekannt (30.11.2007), www.micosoft.com

Rudolph, Benjamin (27.3.2008). www.linux-mag.com

Gabe, Knuth (11.3.2008), www.brainmadden.com

Author unbekannt (22.1.2009), www.vmware.com

Author unbekannt (4.12.2008), kb.vmware.com

Author unbekannt (6.2.2009), www.citrix.com

Baumeister, Johann (29.12.2008) www.pcwelt.de

Author unbekannt (6.2.2009), www, http://www.sisoftware.net

Author unbekannt (6.2.2009), www.de.wikipedia.org

9.3 Anhang C: Abbildungsverzeichnis:

Abbildungsverzeichnis

Abbildung 1: Schema der Ringarchitektur (vgl.: Vmware 2007, S 3).....6
Abbildung 2: Binary Rewriting (vgl.: VMware 2007, S. 4).....8
Abbildung 3: System call- Native versus Paravirtualiserten Umgebung (vgl.:Chisnall 2007, S 12).....11
Abbildung 4: Hardware unterstützte Virtualisierung beim x86 (vgl.:VMware 2007, S6).....12
Abbildung 5: Darstellung der Schichten bei Verwendung einer Emulationssoftware.....14
Abbildung 6: Darstellung der Schichten bei Verwendung von Virtualisierung auf Betriebssystemebene (vgl: Shields 2007, S 6).....16
Abbildung 7: VMM Type 1.....19
Abbildung 8: Monolithic VMM versus Microkernelized VMM.....19
Abbildung 9: VMM Type 2.....21
Abbildung 10: Hybrid VMM.....22
Abbildung 11: Aufbau Hyper-V (vgl.: Microsoft Corporation 2008b, S. 2).....29
Abbildung 12: Hyper-V VMBus (vgl.: Savill, John 2008 S1288).....31
Abbildung 13: Integration Services (vgl.: Savill, John 2008 S. 1339).....33
Abbildung 14: Aufbau ESXi (vgl.: VMware 2007 S 2).....42
Abbildung 15: Aufbau Hypervisor ESXi (vgl.: Charu Chaubal 2007, S 3).....43
Abbildung 16: Netzwerkstruktur ESXi (vgl.: VMware 2007a, S 3 – angepasst).....48
Abbildung 17: VMFS- Anwendung (vgl.: VMware 2007 b, S 5.....50
Abbildung 18: ESXi Editions (vgl.: VMware (Präsentation), S 12).....52
Abbildung 19: Aufbau Xen (vgl.: Chisnal, S. 25).....57
Abbildung 20: Xen Domain 0 Weg eines Netzwerkpakets (vgl.: Chisnall , 2008. S.20 59
Abbildung 21: Testumgebung Netzwerktests.....75
Abbildung 22: Windows Server 2008 Oberfläche direkt am Server (vgl.: http://blogs.msdn.com/blogfiles/virtual_pc_guy/WindowsLiveWriter/IllustratedInstallationofHyperVServer_848A/HyperVServerInstall20_2.png).....76
Abbildung 23: Hyper-V New Virtual Machine Dialog.....77
Abbildung 24: ESXi Installationsschirm.....81
Abbildung 25: Standardschirm ESXi auf dem Host (vgl.: 6.2.2009, http://qemu-buch.de/de/index.php/Bild:VMware-ESX-Server-Install06.png).....82
Abbildung 26: ESXi DLCI (vgl.: 6.2.2009, http://qemu-buch.de/de/index.php/Bild:Esxi-02.png).....83
Abbildung 27: VI Client Login.....83
Abbildung 28: ESXi VI- Client Startschirm.....84
Abbildung 29: ESXi neue VM erstellen.....85
Abbildung 30: ESXi Konsole SUSE ohne Betriebssystem.....86
Abbildung 31: ESXi Konsole Startbildschirm SUSE Linux.....87
Abbildung 32: XenServer xconsole (vgl.: 6.2.2009, http://wiki.computerwoche.de/lib/exe/detail.php/virtualisierung/xen/xsconsole-1.png?id=virtualisierung%3Axen%3Axenserver5&cache=cache).....91
Abbildung 33: XenCenter.....91
Abbildung 34: XenServer ISOs einbinden.....93
Abbildung 35: XenServer erstellen einer VM.....93

9.4 Anhang D: Verzeichnis der Tabellen

Tabellenverzeichnis

Tabelle 1: Systemanforderungen Hyper-V (vgl.: microsoft 6.2.2009, 2, System Requirements, http://www.microsoft.com/servers/hyper-v-server/system-requirements.mspx)....24
Tabelle 2: Features Hyper-V (vgl.: microsoft 6.2.2009, 3,Microsoft Hyper-V Server 2008 http://www.microsoft.com/servers/hyper-v-server/default.mspx vgl.: Microsoft Corporation 2008a, S. 3 f)....28
Tabelle 3: Features ESXi (vgl.: VMware 2008, S 2 vgl: VMware 2009, S31f vg.: VMware 2007a, S 11 vgl.: VMware 22.1.2009, 1, VMware ESXi Features, http://www.vmware.com/products/esxi/features.html vgl.: kb.vmware.com 4.12.2008, 1, Vmware ESX and ESXi Comparison, http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1006543)....41
Tabelle 4: Systemanforderungen XenServer (vgl.: citrix 6.2.2009, 1, http://www.citrix.com/English/ps2/products/subfeature.asp?contentID=1681139)....54
Tabelle 5: Features XenServer (vgl.: citrix 6.2.2009, 2, http://www.citrix.com/English/ps2/products/subfeature.asp?contentID=1680964 vgl.: citrix, 3, http://www.citrix.com/English/ps2/products/subfeature.asp?contentID=1681139)....56
Tabelle 6: Theoretischer Vergleich der Produkte....66
Tabelle 7: Hyper-v Benchmarkergebnisse Windows VM 79
Tabelle 8: Hyper-V Benchmarkergebnisse SUSE Linux VM....80
Tabelle 9: Hyper-V Benchmarkergebnisse OpenSolaris VM....80
Tabelle 10: ESXi Benchmarkergebnisse Windows VM....88
Tabelle 11: ESXi Benchmarkergebnisse SUSE Linux VM....89
Tabelle 12: ESXi Benchmarkergebnisse OpenSolaris VM....89
Tabelle 13: XenServer Benchmarkergebnisse Windows VM....96
Tabelle 14: XenServer Benchmarkergebnisse SUSE Linux VM....96
Tabelle 15: Native Windows Benchmarks....97
Tabelle 16: Native SUSE Linux Benchmarks....98
Tabelle 17: Native OpenSolaris Benchmarks....98
Tabelle 18: Vergleich der Windows Benchmarks....99
Tabelle 19: Vergleich der SUSE Linux Benchmarks....100