INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Diplomarbeit

Dienstevirtualisierung mit Hilfe von VMware am Beispiel der Astrium GmbH

Markus Krieser

Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Nils gentschen Felde Feng Liu Tobias Lindinger
Abgabetermin:	30. September 2007

INSTITUT FÜR INFORMATIK
DER LUDWIG–MAXIMILIANS–UNIVERSITÄT MÜNCHEN

Diplomarbeit

Dienstevirtualisierung mit Hilfe von VMware am Beispiel der Astrium GmbH

Markus Krieser

Aufgabensteller:	Prof. Dr. Heinz-Gerd Hegering
Betreuer:	Nils gentschen Felde Feng Liu Tobias Lindinger
Abgabetermin:	30. September 2007

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

München, den

. . . .

(Unterschrift des Kandidaten)

Die IT Landschaft besteht heutzutage in den meisten Rechenzentren aus einer Vielzahl von Servern. Diese sind mit einer Rechenleistung ausgestattet, die von den meisten Anwendungen kaum genutzt wird. Dennoch ist es aus verschiedenen Gründen sinnvoll, jeder Applikation einen eigenen Server zur Verfügung zu stellen. Beispielsweise laufen die Anwendungen auf unterschiedlichen Betriebssystemen, was einen Parallelbetrieb schwer oder gar unmöglich macht. Solch eine Infrastruktur ist somit von einer optimalen Auslastung weit entfernt und besteht unter anderem aus einer komplexen Verkabelung und erhöhtem Administrationsaufwand.
Die in den letzten Jahren wieder aufkommende Idee der Partionierung von Ressourcen, ermöglicht eine optimierte Auslastung der leistungsstarken Server. Diese Technik nennt sich Virtualisierung und erlaubt es nicht nur bestimmte Ressourcen (wie Hauptspeicher oder CPU), sondern einen kompletten Rechner nachzubilden. Die Vorteile dieser Partionierung liegen auf der Hand. So entfällt die Anschaffung mehrerer Rechner, denn es werden nur noch wenige leistungsstarke Maschinen benötigt. Auch die meist einfachere Verwaltung der Server oder ein besseres Backupsystem, bei dem der komplette Server gesichert wird, haben diese Technik in den letzten Jahren so erfolgreich gemacht. Dies belegen die stetig wachsenden Umsatzzahlen. Der Marktführer VMware hat beispielsweise im Jahr 2006 einen Umsatz von 709 Millionen US-Dollar erzielt. Doch auch andere Hersteller bieten eine Vielzahl von Produkten an, begonnen mit einer kostenlosen Einstiegsmöglichkeit bis hin zum Komplettpaket im Datacenter Bereich.
Im Rahmen der Diplomarbeit werden zuerst der Begriff der Virtualisierung, sodann ihre Entwicklung und aktuellen Möglichkeiten vorgestellt. Hierbei werden allgemeine technische Voraussetzungen und neuste Technologien berücksichtigt. Es erfolgt eine kurze Übersicht, welche Produkte sich aktuell auf dem Markt befinden (Stand: September 2007) und wie ihre Einsatzmöglichkeiten aussehen. Mit diesen Grundlagen wird ein allgemeines Verständnis der eingesetzten Techniken und Produkte geschaffen. Dabei wird sich herausstellen, dass die zuvor genannten Probleme damit größtenteils gelöst werden können. Das Ziel der Arbeit ist daher die Entwicklung eines Konzeptes zur Virtualisierung einer heterogenen IT Infrastruktur. Dabei werden gewisse Anforderungen und Ziele an das Konzept gestellt, die es zu berücksichtigen gilt. Insbesondere erfolgt eine theoretische Einordnung der Virtualisierung in die ITIL. Damit ist eine Grundlage gegeben, um eine Infrastruktur, die bestimmte Voraussetzungen erfüllt, zu virtualisieren. Zur Überprüfung des Konzepts, erfolgt eine Umsetzung am Beispiel der Firma Astrium GmbH. Die dabei eingesetzte Virtualisierungsumgebung ist das *VMware Infrastructure 3* Paket, das eine Vielzahl von Möglichkeiten bietet. Anhand der Astrium GmbH wird gezeigt, dass eine Umsetzung mittels des Konzeptes leicht durchzuführen ist. Dadurch wird ein zuerst geleisteter Investitionsaufwand in die Virtualisierungstechnologie bald großen Nutzen bringen. Als Abschluss erfolgt eine Bewertung in Bezug auf die zuvor gestellten Anforderungen. Zusätzlich wird es einige Leistungstests, so genannte Benchmarks, am vorliegenden System geben, die eine Einschätzung ermöglichen, wie effizient die Virtualisierung arbeitet. Informationen über die Leistung einer Virtualisierungsumgebung sind meist in der Literatur nicht näher spezifiziert. Die hier durchgeführten Tests geben einen ersten Eindruck, in wie weit Leistungsangaben und Realität übereinstimmen. Alle gewonnenen Informationen fließen am Ende in eine Zusammenfassung ein. Zusätzlich gibt es einen Ausblick auf weitere Forschungsgebiete, die sich während der Arbeit hervorgetan haben.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einführung

STM konnte dank VMware Infrastructure die Kosten um 30 % senken. Virtualisierung ist die Zukunft für eine optimierte IT-Infrastruktur.

(Mike Stefanakis - Concepteur Principale / System-Administrator, Societe de transport de Montreal [vm0 06])

Moderne Rechenzentren stehen heutzutage einer Vielzahl von Aufgaben und Problemen gegenüber, die in den letzten Jahren vermehrt zugenommen haben. Durch fallende Kosten für die Anschaffung von Servern entstehen schnell wachsende Rechnerstrukturen. Dies hat aber auch zur Folge, dass der Aufwand an Betreuung und Überwachung der Server rapide steigt, je größer und in der Konsequenz komplexer ein Rechenzentrum wird. So entstehen Kosten, die um ein Vielfaches höher sind, da wesentlich mehr sogenannte „Manpower” benötigt wird, um die Infrastruktur zu pflegen und zu betreuen. Zusätzlich benötigen Server Strom, entsprechende Verkabelung, Klimatisierung und Platz. Aus diesen Gründen sind in den letzten Jahren virtuelle Maschinen immer populärer geworden. In diesem Zusammenhang ist vor allem das Schlagwort „Virtualisierung” stark verbreitet worden, das aber viele Bereiche umfasst. Meist bezieht sich der Begriff auf die Hostvirtualisierung, die es mit einer Software erlaubt, auf einer einzigen Hardware mehrere Rechner nachzubilden, um darin jeweils unabhängige Betriebssysteme laufen zu lassen. Die Vorteile dieser Technik liegen auf der Hand: Es müssen nicht neue Rechner gekauft, aufgebaut und eingerichtet werden, sondern es kann auf eine virtuelle Maschine zurückgegriffen werden. Der Einsatz kann in den unterschiedlichsten IT Abteilungen von Nutzen sein und ermöglicht beispielsweise das Erstellen von Testumgebungen mit unterschiedlichen Betriebssystemen, eine bessere Ressourcenverteilung anhand der vorliegenden Bedürfnisse sowie Kosteneinsparung durch eine geringere Serveranzahl. Ist ein Einsatz der virtuellen Maschine nicht mehr von Nöten, kann diese gelöscht werden und die Ressourcen stehen wieder zur Verfügung. Die daraus resultierenden Vorteile, wie Zeit- und Geldersparnis, spielen bei der Umsetzung eine wichtige, wenn nicht die wichtigste Rolle. Mit der Virtualisierung hält aber auch eine neue Technologie in das Rechenzentrum Einzug, die eigene Anforderungen mit sich bringt. Gerade bei der Virtualisierung von vorhandenen Maschinen müssen mehrere Punkte beachtet werden, da ansonsten die Vorteile schnell verschwinden können. Deshalb ist ein strukturiertes und geplantes Vorgehen anhand eines Konzeptes notwendig, um die verschiedenen Einsatzmöglichkeiten voll ausnutzen zu können.
Daher wird im ersten Schritt dieser Arbeit eine heutzutage gebräuchliche IT Infrastruktur vorgestellt und gezeigt, mit welchen Aufgaben und Problemen ein Administrator dabei zu kämpfen hat. Ein Teil dieser Aufgaben kann mit Hilfe von Virtualisierung gelöst werden. Im Kapitel 3 werden die Grundlagen der Virtualisierung geklärt. Es geht dabei sowohl um die theoretischen Konzepte, die hinter der Virtualisierung stehen, als auch die Produkte, die diese einsetzen. So müssen mehrere Punkte beachtet und besprochen werden, die durch diese neue Technik entstehen. Das hier ermittelte Wissen dient als Basis für die Anforderungsanalyse in Kapitel 4. Dabei entsteht ein Katalog von priorisierten Anforderungen, die an die Virtualisierung und auch an das Konzept gestellt werden. Den theoretischen Rahmen für das Konzept in Kapitel 5 bietet die *IT Infrastructure Library*, kurz *ITIL*. Hier werden Abläufe und Vorgehensweisen in strukturierten Prozessen abgebildet, die sich auch auf eine Virtualisierung anwenden lassen. Mit dem vorgestellten Konzept lassen sich dann bestimmte Infrastrukturen virtualisieren, wenn sie die Vorbedingungen erfüllen. Beispielhaft für die Umsetzung des Konzeptes in Kapitel 6 wird die Virtualisierung bestimmter Bereiche bei der Firma Astrium GmbH gezeigt. Hier sind die Vorbedingungen erfüllt und ermöglichen dadurch eine Durchführung. Sodann erfolgt eine Bewertung und Analyse in Kapitel 7 für diesen speziellen Fall. Der zuvor erstelle Anforderungskatalog muss sich an der praktischen Umsetzung messen, in wieweit die neue Infrastruktur diesen erfüllt. Zusätzlich wird das Leistungsverhalten der virtuellen Maschinen betrachtet. So erfolgen mehrere Benchmarktests in unterschiedlichen Konstellationen, wobei vor allem der Vergleich zwischen einem physikalischem Server und einer virtuellen Maschine interessant ist. Diese Werte fließen in eine abschließende Bewertung ein. Mit einer Zusammenfassung und einem Ausblick auf weitere interessante Fragestellungen endet die Arbeit.

2 Das Szenario und die daraus resultierenden Aufgaben

Hinter dem Begriff der „Virtualisierung" befinden sich eine Vielzahl von Anwendungsmöglichkeiten und Einsatzgebiete, was und wie virtualisiert werden kann. So darf durch die Popularität des Begriffes nicht der Eindruck entstehen, dass sich Virtualisierung immer und überall eignet. Zuerst muss die Ausgangslage sondiert und dokumentiert werden, an der dann mögliche Konzepte und Realisierungen vorgenommen werden können. Anhand dieser Dokumentation können Schwachstellen und Optimierungen festgestellt werden, die im nächsten Schritt bewertet werden müssen. Geklärt werden muss, ob es sich um geringfügige Probleme handelt, die auch durch einfachere Methoden beseitigt werden können oder ob tiefgreifende Problemfelder vorliegen, die einer größeren Intervention bedürfen. Daraufhin folgt der Beschluss, wie eine Verbesserung zu erreichen ist und ob eine Virtualisierung (z.B. Server-Virtualisierung oder Applikations-Virtualisierung) einzusetzen ist.
Diese analytischen Punkte im Vorfeld werden als gegeben vorausgesetzt, in einem möglichen Szenario motiviert (siehe Abschnitt 2.1) und daraus wird eine Entscheidung zugunsten einer Virtualisierungslösung erwogen. Weiterhin bezieht sich die Aufgabenstellung auf den Bereich der Server-Virtualisierung. Das vorgestellte Szenario wird so allgemein wie möglich gehalten, wobei es sich an eine generische IT Infrastruktur orientiert. Dieses Szenario birgt gewisse Problematiken und Schwierigkeiten, die durch eine Virtualisierung teilweise behoben und verbessert werden können.
Welche Aufgaben daraus entstehen, wird dann im folgenden Abschnitt behandelt. So sollten nicht alle Server virtualisiert werden, da gewisse Voraussetzungen und Sicherheiten hier eine wichtige Rolle spielen. Welche Server wie zu virtualisieren sind, ist nur eine der Aufgaben, die dort kurz vorgestellt werden. Wie die Aufgaben im nächsten Schritt zu lösen sind, wird mit Hilfe der ermittelten Anforderungen aus Kapitel 4 in einem Konzept (siehe Kapitel 5) vorgestellt.

2.1 Mögliches Szenario: Heterogene IT Infrastruktur

In heutigen Unternehmen und Rechenzentren herrscht überwiegend eine heterogene IT Infrastruktur, die es zu verwalten gilt. Aktuelle Studienergebnisse beschreiben die Lage in diesen Rechenzentren als „zeit-/kostenintensiv" und „schlecht ausgenutzt" (vgl. [XEN 06]). So kommen nach Schätzungen auf jeden für Server-Hardware ausgegebenen Euro etwa zehn Euro für dessen Support und Wartung. Die Verfügbarkeit der Server ist in der Regel schlecht, verursacht zu ca. 40% von Bedienungs- und Konfigurationsfehlern. Die Auslastung der Server beträgt dabei nur geschätzte 8 bis 30 Prozent. Die Server arbeiten daher nicht effizient genug. Außerdem muss so viel Zeit und Geld in den Betrieb von Servern investiert werden, dass nur 20% des verfügbaren IT-Budgets neuen Projekten und damit der Innovation gewidmet werden können (alle Studienergebnisse siehe [XEN 06]). Diese Punkte zeigen, dass die Infrastruktur weit unter ihren Möglichkeiten arbeitet. Die Komplexität der Struktur erschwert das Management für den Administrator erheblich. Liegt eine Infrastruktur, wie in Abbildung 2.1 zu sehen ist, vor, muss sich der Administrator nicht nur mit verschiedenen Betriebssystemen, sondern auch mit unterschiedlichen Rechnern auseinandersetzen. Des Weiteren existieren unterschiedliche Netzanbindungen der Server, je nach Bedarf und Leistung. Liegt nun der Anwendungsfall vor, dass ein Administrator den Funktionsstatus aller Server ermitteln möchte, dann kann dies beispielsweise über das SNMP (Simple Network Management Protocol) geschehen. Mit Hilfe von SNMP können zuvor eingerichtete Geräte über eine zentrale Konsole überwacht werden. Diese Einrichtung muss zuerst für jedes Gerät vorgenommen werden und ist bei jedem Betriebssystem anders konfiguriert. Ist die Einrichtung erfolgt, müssen auf Grund verschiedener Netze nicht nur eine zentrale Konsole, sondern mehrere eingesetzt werden. Dadurch erhält der Administrator auf verschiedenen Konsolen nur Teile der Informationen. Außerdem ist nicht

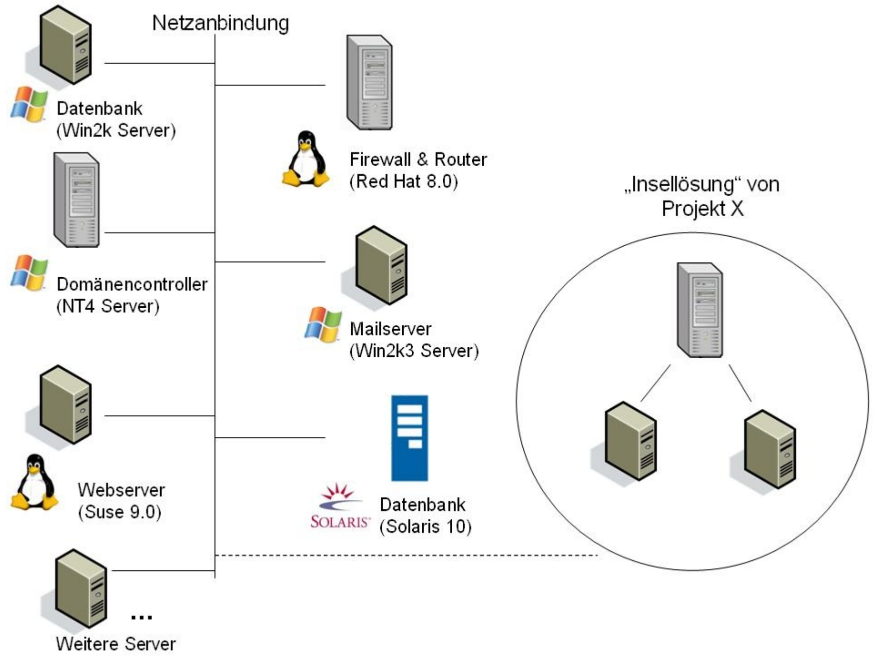

Abbildung 2.1: Mögliche heterogene IT Infrastruktur in einem beliebigen Unternehmen (Quelle: In Anlehnung an [XEN 06])

gewährleistet, dass alle Maschinen berücksichtigt wurden. So können Infrastrukturen entstanden sein, von denen der Administrator keine Kenntnis hat, die aber dennoch als Fehlerquelle im Netz auftauchen können (siehe „Insellösung” in Abbildung 2.1).
Dieser kleine Anwendungsfall zeigt, welche Schwierigkeiten in solch einer Umgebung vorkommen können. Die dabei vorgestellte Struktur in Abbildung 2.1 kommt in der Praxis durchaus so vor. Die unterschiedlich verwendeten Serversymbole stellen dabei eine heterogene Hardware dar. Mögliche Betriebssysteme und Applikationen sind entsprechend gekennzeichnet. Aus dem Anwendungsfall und der vorliegenden Infrastruktur ergeben sich daher mehrere Probleme:

- Betreuung unterschiedlicher Hardware ist komplex und zeitaufwändig
- Anstieg der benötigten „Manpower”, die die komplexe Infrastruktur verwaltet. Dadurch entstehen höhere Kosten durch das Personal.
- Einrichtung verschiedener Managementkonsolen für die verschiedenen Server
- Durch dedizierte Hardware für jede Applikation steigt der Kosten- und Verwaltungaufwand rapide
- Schlechte Ausnutzung der Hardware von den Applikationen
- Unnötiger Strom- und Ressourcenverbrauch durch Leerlaufzeiten der Server
- Hohe Wartungskosten und mehrere Wartungsverträge für die unterschiedlichen Server
- Hohe Komplexität durch Netzkomponenten (Switches, Router, etc.) und Verkabelungskomponenten
- Langsame Reaktion bei Bereitstellung neuer Server, da erst eine Einbindung (Aufbau, Verkabelung, Installation von Managementkomponenten, etc.) in die IT Struktur erfolgen muss
- Flexible Reaktion bei Engpässen durch Zuschalten weiterer Server ist nicht möglich
- Keine genaue QoS Vergabe für bestimmte Server; meist „best-effort” Ansatz für alle Applikationen
- Hohe Verfügbarkeit ist entweder nicht gewährleistet oder wird nur sehr kostenintensiv bewerkstelligt

- Während Wartungsarbeiten ist die laufende Applikation nicht zu erreichen

Dies sind die am Häufigsten vorkommenden Probleme und Schwierigkeiten, mit denen Administratoren umgehen müssen. Welche Aufgaben sich daraus entwickeln und wie eine Virtualisierung dabei helfen kann, wird im nächsten Punkt ermittelt.

2.2 Entwickelte Aufgaben aus dem Szenario

Eine Vielzahl von Problemen haben sich aus dem Szenario ergeben und stellen daher Aufgaben, die nun zu lösen sind. Die Vorteile einer optimalen Hardwareauslastung durch die Virtualisierung führen schnell zu der Meinung, dass am Besten alle vorhandenen Server virtualisiert werden sollten. Dies ist aber nicht für jede Anwendung ratsam. Auch dürfen Sicherheitsaspekte nicht außer Acht gelassen werden. Wenn zum Beispiel in einem kleineren Unternehmen alle physikalischen Server in virtuelle Maschinen umgewandelt werden und dann auf einem einzelnen physikalischen Server laufen, so handelt es sich um einen klassischen „Single Point of Failure” (siehe [Zimm 06]). Bei Ausfall dieses Servers, würde dies einen Totalausfall des Systems nach sich ziehen, was auf jeden Fall vermieden werden muss. Im Folgenden werden daher die Aufgaben aufgelistet, die es zu lösen gilt (nach [XEN 06]):

1. Serverkonsolidierung:
   - Reduzierung der Hardware, indem mehrere voneinander getrennte Systeme (Virtuelle Maschinen; kurz: VMs) auf einer physikalischen Maschine laufen. So kann die zugrunde liegende Hardware besser genutzt werden und es wird zukünftig weniger Hardware benötigt.
   - Reduzierung der TCO[1], indem weniger Betriebskosten (Strom, Kühlung, Ersatzteile, Raummiete, Wartung, etc.) notwendig sind. Zusätzlich gibt es im Rechenzentrum, durch Wegfall von Netzwerk- und Verkabelungskomponenten weniger Komplexität.
2. Flexibilität im Betrieb:
   - Schnellere Reaktion auf kurzfristige Engpässe bei steigender Serverauslastung. Mit Hilfe von VMs kann schneller auf Probleme reagiert werden, indem zur Lastverteilung zusätzliche Maschinen geklont und verwendet werden.
   - Die Anpassung an Applikationen soll jederzeit möglich sein, um eine möglichst optimale Auslastung der Hardware zu gewährleisten. Zusätzlich können mit QoS Parametern die Anwendungen priorisiert werden.
3. Steigende Verfügbarkeit:
   - Backup und Restore können auf Grund der Beschaffenheit von VMs[2] leichter vollzogen werden. Sicherung verschiedener Versionen soll ermöglicht werden.
   - Einsatz von „Failover”-Mechanismen bei Kapazitätsengpässen, im Wartungsfall oder bei sicherheitskritischen Vorfällen.
   - Bessere Softwarewartung, indem Patches und Applikationen nicht auf einem dedizierten System getestet werden müssen, sondern indem die VM geklont und der Test darauf ausgeführt wird.

Diese gestellten Aufgaben können, wie erwähnt, durch eine Virtualisierungsumgebung gelöst werden. Es darf aber nicht übersehen werden, dass durch die Virtualisierung auch eine höhere Komplexitätsstufe hinzukommt (vgl. [Zimm 06]). Die komplette Planung, Einführung und der Betrieb solch einer Umgebung erfordern Wissen und Kompetenz, die sich entweder die Administratoren selbst aneignen oder durch externe Hilfe erlangen müssen (vgl. [XEN 06]). Dadurch kann am Anfang mit noch keiner Kosteneinsparung gerechnet werden,

[1] TCO steht für Total Cost of Ownership und ist ein weit verbreitetes und populäres betriebswirtschaftliches Verfahren zur Berechnung von Investitionen. Zusätzlich werden auch die ständig anfallenden Betriebskosten der gesamten Lebensdauer miteinbezogen [XEN 06].

[2] In der Regel besteht eine virtuelle Maschine aus einer einzelnen Datei (eine Art „Container” für die eigentlichen Daten) und kann so leicht kopiert, geklont oder verschoben werden. Genaueres zu virtuellen Maschinen befindet sich in Kapitel 3.

jedenfalls nicht solange Abläufe und Vorgehensweisen korrekt eingespielt sind. Langfristig ist aber eine Einsparung durchaus zu erwarten und führt des Weiteren meist zu einer verbesserten Servicequalität.

Nachdem ein in der Praxis vorkommendes Szenario mit seinen Problemen und Aufgaben vorgestellt wurde, werden im nächsten Kapitel die Grundlagen für das Thema gelegt, um den bisher unklaren Begriff der Virtualisierung zu definieren und einzuordnen.

3 Grundlagen

Mit diesem Kapitel werden die Grundlagen gelegt, die für den weiteren Verlauf notwendig sind. Das Wort „Virtualisierung" ist schon mehrfach gefallen, doch ist eine Definition oder genaue Erklärung bisher noch ausgeblieben. Dies liegt daran, dass hinter dem Begriff unterschiedlichste Bedeutungen und Verfahren stecken, die aber für das vorangestellte Szenario nicht alle relevant sind. In Abschnitt 3.1 gibt es zu Beginn einen kurzen historischen Überblick, da dieser Begriff schon seit langem in der Informatik verwendet wird. Im Anschluss daran wird dann genauer auf die hier wichtige Virtualisierung, nämlich die Hostvirtualisierung, eingegangen. Dabei gibt es verschiedene Arten bzw. Möglichkeiten, die mit ihren technischen Eigenschaften im Detail vorgestellt werden. Die gezeigten Techniken werden bei einer Vielzahl von Produkten eingesetzt. Diese werden kurz vorgestellt und eingeordnet, wobei die Produkte von VMware in einem eigenen Abschnitt behandelt werden. Am Ende des ersten Abschnitts erfolgt ein Ausblick über neue Technologien und artverwandte Themen. So haben AMD und Intel eine neue Prozessorgeneration entwickelt, die hardware-unterstützende Eigenschaften für die Virtualisierung anbietet.
Im Abschnitt 3.2 wird die Firma VMware mit ihren Produkten vorgestellt. Mit Hilfe der *VMware Infrastructure 3* Umgebung erfolgt die praktische Umsetzung des Konzeptes. Diese Umgebung liefert einige Programme mit, die einen Einsatz im Data Center Umfeld ermöglichen. Dabei spielt vor allem der ESX Server eine wichtige Rolle. Mit seinen speziellen Eigenschaften ist er eine wichtige Komponente, die genau vorgestellt werden muss. Aber auch die Programme, die für eine komfortable Hostvirtualisierung wichtig sind, werden mit ihren wichtigsten Merkmalen aufgezeigt.
Im letzten Abschnitt 3.3 wird auf den bisher vernachlässigten Punkt des Managements von physikalischen und virtuellen Maschinen eingegangen. Durch die Virtualisierung ergibt sich eine zusätzliche Ebene, denn nicht nur die physikalischen Maschinen müssen in die bisherige IT Struktur aufgenommen und verwaltet werden, sondern auch die darauf laufenden virtuellen Maschinen. So spielen hier vor allem Begriffe wie Serververwaltung, Lastverteilung und Sicherheit eine Rolle. Welche Probleme dabei auftreten können und wie diese gelöst werden, wird in diesem Abschnitt geklärt.

3.1 Hostvirtualisierung

Der Begriff „Virtualisierung" ist in den letzten Jahren immer häufiger in verschiedensten Bereichen verwendet worden. Im Folgenden wird immer auf die Hostvirtualisierung eingegangen, außer es wird explizit auf eine andere Virtualisierungsart hingewiesen. Die Begriffe „Hostvirtualisierung" und „Virtualisierung" werden im weiteren Verlauf äquivalent verwendet. Dazu eine kleine Anmerkung: Der Titel der Arbeit ist mit dem Begriff der „Dienstevirtualisierung" etwas irreführend. Dieser war zu Beginn der Arbeit noch zutreffend, hat sich aber währenddessen zur Host- oder Servervirtualisierung gewandelt. Daher wird in der restlichen Arbeit von diesem neuen Begriff ausgegangen.
Eine konkrete Definition erweist sich als schwierig, denn je nach der eingesetzten Methode (Software- oder Hardware-basierend) von Virtualisierung und Hersteller, gibt es unterschiedlichste Definitionen. Eine mögliche allgemeine Definition könnte lauten: „Virtualisierung bezeichnet Methoden, die es erlauben, Ressourcen eines Computers aufzuteilen [Wiki 06]". Eine Weiterführung dieser Definition ist nicht nur die Aufteilung der Ressourcen, sondern die Möglichkeit, „mehrere voneinander unabhängige Systeme der gleichen Prozessorarchitektur auf einem leistungsfähigen Host-System zu betreiben. [XEN 07]". Eine mögliche Definition wäre dann: *„Virtualisierung bezeichnet den Vorgang, mehrere Betriebssysteminstanzen unabhängig von einander parallel auf einer physischen Umgebung laufen zu lassen."*. Streng genommen, gilt dies aber nur für Virtualisierungslösungen, die unterhalb des eigentlichen Betriebssystems arbeiten. Des Weiteren darf die Virtualisierung auch nicht mit einer Emulation verwechselt werden, bei der „eine bestimmte Architektur, die von der Architektur des Host-Systems abweichen darf, komplett in Software" [XEN 06] abgebildet wird. Bei der Virtualisierungssoftware „teilen sich vollständig virtualisierte Systeme nur den Zugriff auf die *vorhandenen*

Komponenten, beispielsweise die CPU [XEN 07]". Dies erreicht in der Regel eine erhöhte Performanz, da es meistens möglich ist, den Zugriff von der virtualisierten Hardware direkt an die physikalische Hardware durchzureichen. Dadurch erfolgt keine umständliche Übersetzung aller Befehle auf die eigentliche zugrunde liegende Hardware (vgl. [XEN 07]). Insgesamt zeigt sich, dass eine allgemeingültige Definition in diesem Bereich schwer möglich ist. Für den späteren Anwendungsfall kann aber die zuvor genannte Definition angewandt werden.
Das Potential von Virtualisierung ist in vielen Bereichen vorhanden, wodurch der Markt von diversen Konkurrenten heiß umkämpft ist. Laut einer Umfrage unter weltweit führenden CIOs, setzen diese den Punkt „Virtualisierung" auf ihre Top-10-Liste[1]. Dazu muss aber im ersten Schritt geklärt werden, welche Möglichkeiten und Lösungen es für die jeweilige Firma gibt. Um Ordnung in die verschiedenen Ansätze zu bekommen, werden die unterschiedlichen Virtualisierungstechniken und Produkte in den folgenden Abschnitten beschrieben.
Zuerst wird kurz die Geschichte und Entwicklung der Virtualisierung vorgestellt. Danach erfolgt eine genaue Darstellung der Möglichkeiten von Virtualisierung. Die wichtigsten Hersteller und deren Produkte werden im darauffolgenden Punkt behandelt. Zuletzt werden aktuelle Trends und Techniken, die auf diesem schnell wachsenden Markt vorherrschen, aufgezeigt.

3.1.1 Geschichte und Entwicklung

Der eigentliche Beginn der Geschichte der Virtualisierung wird im Jahre 1959 mit der Abhandlung „Time Sharing in Large Fast Computers" von Christopher Strachey gesehen. Dieser befasst sich mit der optimalen Ausnutzung eines 1-CPU-Systems: Die Programme werden nacheinander abgehandelt, bis sie abgeschlossen sind. Erfolgt von einem Programm ein Zugriff auf ein Peripheriegerät, so ist in dieser Zeit keine CPU Nutzung vorhanden. Nach Strachey erfolgt nun ein Kontextwechsel und das darauffolgende Programm kann die CPU nutzen, bis es zu einem erneuten Peripherie Zugriff kommt (vgl. [Klee 07]). Dadurch entsteht eine optimale Auslastung der CPU ohne Leerlaufzeit. Für den User erscheint transparent, welche logische CPU tatsächlich die physikalische CPU nutzt. Dieses Konzept ist heutzutage als Multiprogrammierung bekannt.
Ein nächster wichtiger Schritt erfolgte in der Mitte der 60er Jahre mit der Einführung der System 360 Software (OS/360) durch IBM für die Mainframe Architektur im Jahre 1964 (vgl.[Klee 07]). Dessen Weiterentwicklung, das System 370, welches im Sommer 1970 vorgestellt wurde, erlaubte erstmalig die Umwandlung virtueller in reale oder physikalische Speicheradressen mittels der sog. Data Address Translation. Dabei handelt es sich un ein Verfahren, bei dem jede durch einen Prozess angeforderte virtuelle Adresse durch die Memory Management Unit (MMU) zuerst in eine physikalische Adresse umgewandelt wird, bevor sie auf den Adressbus geschrieben wird (vgl.[Klee 07]). Die MMU besitzt hierzu einen speziellen Cache-Speicher, der die jeweils letzten Übersetzungen in Form einer Tabelle ablegt. Den Mechanismus der Übersetzung von logischen Adressen in physikalische Adressen wird auch als Paging bezeichnet. Da dies für die Applikation transparent abläuft, wird von sog. Speichervirtualisierung gesprochen (vgl. [Klee 07]). Ursachen für die Entwicklung dieser Technologie war der sehr teure Hauptspeicher zu jener Zeit und musste daher optimal genutzt werden (vgl. [Pull 06]). Auch wenn der Hauptspeicher inzwischen relativ günstig ist, wird dieses Verfahren auch heutzutage von den meisten Betriebssystemen aktiv genutzt (vgl. [Pull 06]).

Nachdem es schon 1959 von Strachey Überlegungen zu Timesharing-Systemen gab, brachte IBM 1972 ein Mainframe mit dem System VM/370 auf den Markt, das unter Aufsicht eines „Control Program" - heute als „Virtual Machine Monitor" oder „Hypervisor" bezeichnet - virtuelle Maschinen (VMs) mit verschiedenen Betriebssystemen gleichzeitig ausführen konnte. Die Funktionsweise der damaligen virtuellen Maschine war Folgende: „IBM's virtual machines were identical „copies" of the underlying hardware. A component called the virtual machine monitor (VMM) ran directly on „real" hardware. Multiple virtual machines could then be created via the VMM, and each instance could run its own operating system. [Sing 06]". Daraus geht hervor, dass eine virtuelle Maschine üblicherweise eine Kopie einer realen Maschine ist. Die von Kenneth Bowles im Jahre 1977 entwickelte Pseudo-Maschine - kurz p-Maschine genannt - änderte dieses. Sie existierte jedoch nur auf dem Papier. Um Programme ausführen zu können, musste ein Emulator entwickelt werden - ein Programm, das eine p-Maschine auf einem anderen Computer in allen Funktionen nachbildet. Die für die p-Maschine entwickelten Programme wurden portabel, indem solche Emulatoren für verschiedene Plattformen

[1] Gartner CIO Umfrage 2006: Befragung von 1400 IT-Chefs, in rund 30 Ländern, welche die 10 wichtigsten anzupackenden Punkte in ihrem Bereich im Jahre 2006 sind (Quelle: [Moor 07]).

zur Verfügung gestellt wurden. Ähnlich verhält es sich mit der 1991 entwickelten, heute wesentlich verbreiteteren Java Virtual Machine (JVM). Die JVM arbeitet direkt mit Java- Bytecode, muss selbst aber auf einem realen Rechner emuliert werden. Mit Java konnten die Vorteile der Maschinencode-Welt mit denen der interpretierten Sprachen verbunden werden: Eine mittlerweile sehr effiziente und schnelle Emulation mit Hilfe von just-in-time-Compilern sowie eine sehr gute Portabilität. Doch die JVM ging noch einen Schritt weiter als die p-Maschine: 1997 stellte Rockwell-Collins Inc. den JEM1-Mikroprozessor vor. Dieser konnte Java- Bytecode ohne Emulation direkt verarbeiten und stellte so die zur JVM passende „Java Real Machine" dar (vgl. [jav 07]). Doch schon lange vor der JVM untersuchten G.J. Popek and R.P. Goldberg im Jahre 1974, welche Voraussetzungen für eine erfolgreiche Virtualisierung einer Prozessorarchitektur notwendig sind. Deren Ergebnisse wurden in dem Artikel „Formal requirements for virtualizable third generation architectures" festgehalten und in der Fachzeitschrift der ACM (Association for Computing Machinery) veröffentlicht (vgl. [PoGo 74]). Nach Popek und Goldberg ist eine CPU/ISA (Instruction Set Architecture) virtualisierbar, wenn alle privilegierten Instruktionen eine Exception erzeugen, wenn sie in einem unprivilegierten Prozessormodus ausgeführt werden (vgl. [PoGo 74]). Alle sensiblen Instruktionen sind privilegiert. Dies ist aber nicht bei allen Befehlen der IA32 (Befehlssatz von Intel und AMD Prozessoren) der Fall. So gibt es Befehle die modus-sensitiv, aber nicht privilegiert sind (vgl. [Hoex 06]). Aus diesen Gründen ist nach den Popek/Goldberg Bedingungen die x86 Architektur (IA32) nicht virtualisierbar (vgl. [Hoex 06]). Deren Relevanz ist bis heute noch aktuell, denn durch diese Probleme müssen gewisse Umgehungsmöglichkeiten erforscht und entwickelt werden (siehe nächster Abschnitt). Außerdem entwickeln Intel und AMD heutzutage Prozessoren, die den Popek/Goldberg Bedingungen genügen und die Virtualisierung effizienter gestalten (genaueres siehe Abschnitt 3.1.4).

In den 80er Jahren verdrängt die Client/Server Architektur nach und nach die Mainframes. Deshalb ist nicht mehr eine zentrale Komponente vorhanden, die möglichst effizient genutzt wird, sondern es können Aufgaben und Dienste auf verschiedene Rechner verteilt werden. Dadurch gerät die Virtualisierung ganzer Systeme in den Hintergrund. Trotzdem gibt es weiterhin zahlreiche Neuerungen in diesem Bereich. So entwickelte 1993 Sun eine Software namens *WABI* (Windows Applications Binary Interface), mit deren Hilfe Programme, die für das Betriebssystem Windows geschrieben wurden, unter Solaris 2.0 und 2.2 laufen konnten. Dabei musste nicht das ursprüngliche Programm umgeschrieben werden, sondern WABI bildet die meisten API (Application Programming Interface) Befehle von Windows in die entsprechenden Solarisfunktionen um (vgl. [Malf 05]). Unterstützt wurde sowohl die x86 Architektur, wie auch die *SPARC* Architektur von Sun. Bei der Ausführung auf einem *SPARC* Prozessor wurde zusätzlich ein x86 Emulator verwendet. In der Linuxgemeinde entstand im selben Jahr ein ähnliches Projekt namens *WINE* (WINE Is Not an Emulator), das Windows 3.1 Programme unter Linux ausführbar macht. Wie der Name bereits sagt, handelt es sich nicht um einen Emulator und setzt daher eine x86 Architektur voraus. Die Entwicklung von *WINE* hält bis heute an, so dass mittlerweile alle Windows Versionen bis Windows XP geladen werden können, inklusive Unterstützung der Grafikschnittstelle DirectX für entsprechende Spiele (siehe weitere Infos unter [Win 07a]).

Ende der 90er Jahre sind zwei wichtige Neuerungen in der Welt der Virtualisierung bemerkenswert: 1999 stellt die neu gegründete Firma VMware Inc. ihr Programm *VMware Workstation* vor, mit dem sich erstmals ein kompletter x86 Computer auf einem anderen x86 System in annehmbarer Geschwindigkeit virtualisieren lässt. Dies war bis dato nicht möglich und eine Virtualisierung von x86 Systemen galt seit den von Popek/-Goldberg aufgestellten Bedingungen als schwierig bis nicht möglich. VMware spezialisierte sich auf x86 Virtualisierungen und bietet heutzutage mehrere kostenlose und kostenpflichtige Programme in diesem Bereich an.
Die zweite Entwicklung kommt von dem Programmierer Jeff Dike, der im selben Jahr den Linux Kernel so modifizierte, dass ein kompletter Kernel als Anwendungsprozess innerhalb operierender Linux-Systeme ausführbar ist, ohne deren Konfiguration und damit Stabilität zu beeinflussen (vgl. [uml 07]). Dies nannte Dike *User Mode Linux* (*UML*; nicht zu verwechseln mit der *Unified Modelling Language*, die genauso abgekürzt wird). Die Einsatzmöglichkeiten sind so vielfältig, dass UML seit der Linux Kernelversion 2.6 offiziell zum Standard gehört. So können beispielsweise verschiedene Distributionen und Versionen von Linux in einem jeweiligen virtuellen Kernel laufen, um Software für unterschiedliche Systeme zu testen.

Die bisher dargebotenen Entwicklungen sind nur ein Teil der Möglichkeiten, die es in diesem Bereich gibt. Dies aber zeigt, dass sich hinter dem Begriff „Virtualisierung" seit über 40 Jahren eine Vielzahl von eingesetz-

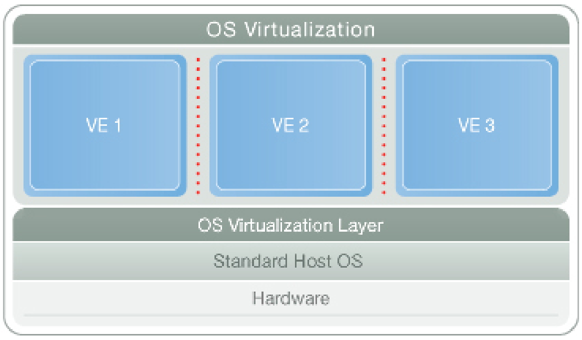

Abbildung 3.1: Virtualisierung auf Betriebssystem-Ebene (Quelle: [SWso 07])

ten Techniken verbirgt und kein neues Schlagwort der jüngsten Zeit ist. In den letzten Jahren wurde der Begriff wieder populärer, da durch steigenden Administrationsaufwand (und die dadurch steigenden Kosten) die vorhandenen heterogenen IT Infrastrukturen eine Konsolidierung verlangen. Mit Hilfe von Virtualisierung kann eine Vereinheitlichung und Vereinfachung erfolgen. Welche Art der Virtualisierung verwendet werden soll, hängt sowohl vom Einsatzwunsch als auch vom eingesetzten Produkt ab. Die Möglichkeiten und wichtigsten Produkte, werden in den folgenden Abschnitten vorgestellt.

3.1.2 Möglichkeiten der Hostvirtualisierung

Wie im vorherigen Punkt schon mehrfach angesprochen, ist die Virtualisierung der x86 Architektur schwierig, da diese nicht dafür ausgelegt ist (vgl. [XEN 07]). Daher müssen Techniken entwickelt werden, die einem virtualisierten System vorgeben, es habe die volle Kontrolle über die existierenden Hardware-Komponenten. Auch effiziente Ressourcennutzung eines Gastes auf dem Host spielt eine Rolle.

Gelöst werden die Probleme zur Zeit durch die folgenden drei softwarebasierenden Ansätze (nach [XEN 07]):

- Virtualisierung auf Betriebssytem-Ebene
- Hardware-Virtualisierung
- Paravirtualisierung

Zusätzlich gibt es weitere Entwicklungen, wie die Unterstützung von Virtualisierung im Prozessor (siehe Abschnitt 3.1.4). Im Folgenden wird nun auf die drei Ansätze genauer eingegangen.

Virtualisierung auf Betriebssystem-Ebene

Dieser Ansatz, auch OS-Level- oder Shared-OS-Virtualisierung genannt, virtualisiert Server auf der Betriebssystem- (Kernel-)Ebene. Diese Virtualisierungsmethode bildet isolierte Partitionen (siehe Abbildung 3.1) oder virtuelle Umgebungen (Virtual Environments = VEs) auf einer einzelnen physikalischen Server- und Betriebssysteminstanz ab (vgl. [SWso 07]). So existiert eine komplette Laufzeitumgebung innerhalb eines geschlossenen Containers, auch *jails*[2] genannt (vgl. [XEN 07]). Jede VE arbeitet und verhält sich wie ein eigenständiger Server. Diese können unabhängig voneinander neu gestartet werden und haben Root-Zugriff, Benutzer, IP-Adressen, Speicher, Prozesse, Dateien, Programme, Systembibliotheken und Konfigurationsdateien [XEN 07]. Das Host-System startet keine zusätzlichen Betriebssystem-Kernel für die einzelnen Instanzen, sondern trennt die unterschiedlichen Prozessräume der virtuellen Instanzen strikt voneinander [XEN 07]. Die Aufteilung der Ressourcen erfolgt durch den Betriebssystem-Kernel, der eine eigene integrierte Ebene für diese Aufgabe hat (in Abbildung 3.1: *OS Virtualization Layer*). Da für diese Technik der Quellcode des Betriebssystem bekannt sein muss, gibt es bisher nur Umsetzungen für einige Open Source Projekte. Einzige Ausnahme ist das Programm *Virtuozzo*, dass es auch für einige Windows Server Versionen gibt.

[2] bei dem Betriebssystem FreeBSD werden diese so genannt.

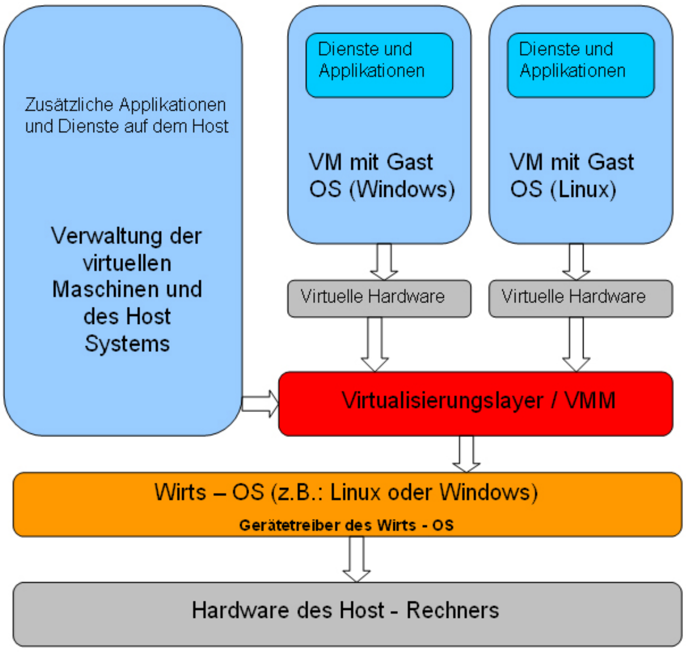

Abbildung 3.2: Aufbau der einzelnen Komponenten bei der Hardware-Virtualisierung (Quelle: [XEN 06])

Durch diese Technik können unterschiedliche Betriebssysteme nicht als VE laufen, da es nur eine Instanz des zugrunde liegenden Kernels gibt. Daher ist der Kernel des Gast- und Hostsystems gleich, wobei es beispielsweise bei *OpenVZ* möglich ist, verschiedene Linux-Distributionen (aber mit identischem Kernel!) in verschiedenen VEs einzusetzen (vgl. [ope 07]). Des Weiteren ist es nicht möglich aus dem Container heraus Treiber zu laden, da dies nur der Kernel des Hosts kann. In Bezug auf die Leistungseinbußen ist das Verhalten bei diesem Verfahren sehr gut. Da in allen Containern dasselbe Betriebssystem, sogar derselbe Kernel läuft, arbeiten Gast- und Wirtsystem gut zusammen und es entstehen sehr geringe Leistungseinbußen. Laut Kir Kolyshkin, dem Entwicklungsleiter von *OpenVZ*, liegt der Overhead „je nach Anwendung (...) bei 1% [Baad 06]". Dadurch lassen sich die VEs gut skalieren, da durch die geringe Auslastung eine gute Anpassung an den zugrundeliegenden Server möglich ist. Der Einsatz dieser Technik zeichnet sich durch gute Skalierbarkeit, einfache Handhabung und kostengünstige Produkte für eine schnell aufgebaute Virtualisierungsumgebung aus. Auf Grund der Open Source Projekte herrscht eine ständige Weiterentwicklung und neueste Technologien werden rasch integriert. Bekannte Vertreter sind die freien Programme von *OpenSolaris Zones*, *FreeBSD Jails*, *OpenVZ*, *Linux VServer* und das kommerzielle Programm *Virtuozzo* (das für Linuxkerne aber auf Basis von *OpenVZ* funktioniert) (vgl. [Wiki 06]).

Hardware-Virtualisierung

Der Begriff „Hardware-Virtualisierung", oft auch „Full Virtualization" genannt, ist mehrfach besetzt und wird unterschiedlich definiert. So wird einerseits gesagt, dass Hardware-Virtualisierung auf Prozessoren mit Hardware-Virtualisierungstechnologien wie Intel VT-x (vgl. [int 05]) oder AMD-V (vgl. [amd 07]) basieren, andere trennen zwischen „Full Virtualization" und „Hardware-basierte Virtualisierung" (vgl. [XEN 07]). Der Begriff „hardware-basierend" ist leicht irreführend, denn er suggeriert, dass bereits eine Virtualisierung im Prozessor vorgenommen wird. Dies ist aber bisher nicht der Fall, sondern der Prozessor bietet unterstützende Funktionen zur Virtualisierung an (genaueres in Abschnitt 3.1.4). Daher wird ab sofort der Begriff der hardware-unterstützten Virtualisierung verwendet und im Folgenden der zweite Ansatz verwendet.
Um eine Hardware-Virtualisierung handelt es sich, wenn die Gastsysteme unverändert in der virtualisierten Umgebung lauffähig sind und der Kernel des Gastsystems nicht an die virtuelle Umgebung angepasst werden muss [XEN 07]. Die Tatsache, dass eine Virtualisierung stattfindet, wird vor dem Gast vollständig verborgen (vgl. [XEN 06]). Daher ist der Gast vom Wirtbetriebssystem unabhängig und wird zum Beispiel nicht durch den selben Kernel beschränkt, wie dies bei der Virtualisierung auf Betriebssystem-Ebene der Fall ist.

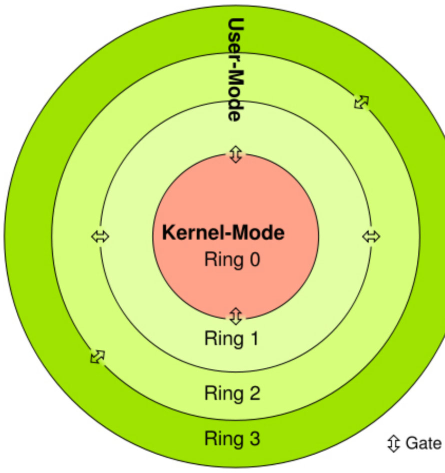

Abbildung 3.3: Schematischer Aufbau der Ringe bei einem x86 System (Quelle: [Wiki 06])

Ein Gast wird in den meisten Fällen nicht mehr als Container (siehe Abschnitt 3.1.2) bezeichnet, sondern als virtuelle Maschine (kurz: VM) (vgl. [AHN 07]). Diese VM stellt die komplette Hardware-Umgebung für das virtualisierte System dar [XEN 07]. So erscheint eine virtuelle Maschine wie ein unabhängiger Rechner, der alle Komponenten, z.B. Festplatten, RAM, Netzwerkkarte und CPU, besitzt. Dennoch darf eine VM nicht direkt mit den physikalischen Komponenten kommunizieren, da dies die Isolation der einzelnen VMs verletzen würde. Die Virtualisierungssoftware muss daher den Zugriff der VMs steuern und zum Beispiel eine physische Netzwerkkarte im virtualisierten System als eigene Komponente simulieren. Die VM steuert diese simulierte Komponente über einen eigenen Treiber an und weiß nicht, wie die weitere Behandlung durch die Software erfolgt. Diese Softwareschicht, die sich zwischen das Gastbetriebssystem und der realen Hardware schiebt, wird *Virtualisierungslayer* oder *Virtual Maschine Monitor* (kurz: VMM) genannt (siehe Abbildung 3.2). Die Aufgaben des VMM sind unter anderem, die Hardware für die virtuellen Maschinen zu emulieren, den VMs entsprechende CPU Zeit zuzuteilen oder den kontrollierten Zugriff auf bestimmte physikalische Geräte des Hostsystems zu ermöglichen (vgl.[AHN 07]). Bei den meisten Produkten läuft diese Schicht auf dem Wirtsbetriebssystem und greift daher nicht direkt auf die zugrundeliegende Hardware. Diese Zwischenschicht verursacht dementsprechend Leistungseinbußen von 20 bis 25 Prozent (laut [XEN 07]), da diese Schicht alle virtuellen Maschinen koordinieren muss. Die einzelnen Zugriffe, zum Beispiel auf die Netzwerkkarte, müssen vom VMM behandelt und an das Hostsystem übergeben werden. Dieses wiederum muss die Zugriffe entsprechend behandeln und an die physische Hardware weitergeben. So eine Übergabe kostet Performanz, wenn jede Schicht die Ereignisse gesondert behandeln muss. Dies deuten die Pfeile in Abbildung 3.2 bei einem Zugriff auf bestimmte Hardwarekomponenten an.

Um die Problematik der Zugriffe einer VM auf die physikalische Hardware zu verdeutlichen, wird dies im Folgenden genauer beleuchtet. Wie bereits erwähnt, kann eine VM nicht direkt auf die Hardwareressourcen zugreifen. Wenn dies allen Gästen erlaubt wäre, könnte eine Abschottung nicht mehr gewährleistet werden (vgl. [AHN 07]). Auch das Betriebssystem muss die Kontrolle über alle laufenden Anwendungen (inklusive der Virtualisierungssoftware mit deren VMs) haben und den Zugriff koordinieren. Ansonsten könnte die Anwendung am Betriebssystem vorbei den Zugriff auf eine Ressource ermöglichen und möglicherweise das komplette System abstürzen lassen. Aus diesem Grund muss es für das Betriebssystem eine andere Priorität als für eine Anwendung geben. Bei x86 Systemen unterscheiden 80286-kompatible Prozessoren vier Privilegierungsstufen: Ring 0, 1, 2 und 3 (siehe Abbildung 3.3). Laufende Prozesse im Ring 0 haben die höchste Priorität und die volle Kontrolle über das System. Anwendungen aus höheren Ringen können auf darunter liegende Ringe und auf die Hardware dagegen nicht direkt zugreifen, sondern mittels 'gates' auf Schnittstellen (*APIs*), die wiederum von Anwendungen im Ring 0 kontrolliert werden [AHN 07]. Die meisten Betriebssysteme (Ausnahme: OS/2) nutzen nur zwei der vier Ringe: Im Ring 0 (dem sogenannten Kernelmodus) werden der Kernel und alle Hardwaretreiber ausgeführt, während die Anwendungssoftware im unprivilegierten Ring 3 (sogenannter Benutzer- /Usermodus) arbeitet (siehe Abbildung 3.3). Ruft ein Prozess in einem weniger priviligierten Ring eine privilegierte Operation auf, erzeugt der Prozessor eine *Exception*. Diese kann in einem

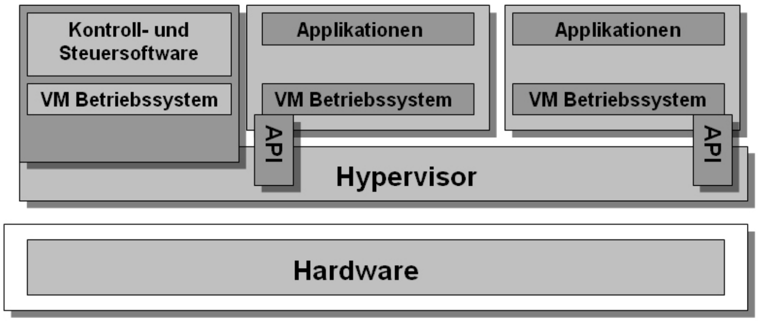

Abbildung 3.4: Modell einer paravirtualisierten Umgebung (Quelle: [XEN 06])

privilegierteren Ring abgefangen und behandelt werden. Wird so eine Exception nicht abgefangen und behandelt, erzeugt sie einen *General Protection Fault* und der verursachende Prozess stürzt ab [XEN 07].
Damit die Virtualisierungssoftware alle VMs kontrollieren kann, müssen diese im Benutzermodus von Ring 3 laufen, als wären die Gastbetriebssysteme normale Applikationen [AHN 07]. Da aber für eine VM die darunter liegenden Schichten transparent sind, versucht ein Gastsystem, wie es das als Koordinator des Kernel-Modus gewohnt ist, die Kontrolle über die Hardware zu erlangen. Der Virtualisierungslayer (Abbildung 3.2) fängt *privilegierte Operationen* der Gastbetriebssysteme ab, die versuchen, die Hardware direkt anzusprechen. Diese Operationen werden dann mit anderen ungefährlichen Befehlssequenzen nachgebildet, ohne dass der Gast davon etwas mitbekommt (vgl. [AHN 07]). Ein Problem ist hierbei, dass sich nicht alle gefährlichen Befehle abfangen lassen, da die x86 Architektur nicht für Virtualisierung vorgesehen war und dadurch nicht alle Befehle privilegiert sind (siehe Popek/Goldberg [PoGo 74]). So funktioniert dies allerdings nicht immer, da einerseits nicht alle Schutzverletzungen *Exceptions* auslösen und andererseits einige Befehle sich in den verschiedenen Ringen unterschiedlich verhalten [Ahle 07]. Aus diesem Grund muss der VMM den ausgeführten Code ständig überwachen, analysieren und Befehle, die nicht wie erwartet funktionieren, durch Workarounds ersetzen (vgl. [Ahle 07]). Teilweise wird im ersten Durchlauf jede Befehlsfolge im Gast vom VMM im Einzelschritt-Modus (auch Debug-Modus genannt) abgearbeitet, damit jede Anweisung einzeln betrachtet werden kann [AHN 07]. Dadurch können zukünftige Befehle schneller behandelt werden. Dennoch führt diese Arbeit der Virtualisierungsschicht zu Einbußen bei der Performanz. So waren bei der Einführung dieser Virtualisierungstechnik Effizienzeinbrüche von 20 bis 25 Prozent (laut [XEN 07]) bei den Produkten von VMware und Microsoft ermittelt worden, welche aber durch die Erfahrung in neueren Versionen verringert wurden. Dennoch ist die Performanz schlechter als bei der vorangegangenen Technik. Aber es können unterschiedliche Betriebssysteme verwendet werden, ohne dass sie modifiziert werden müssen. Meist aber bieten die Hersteller eine Modifizierung an, um ein besseres Leistungsverhalten zu erzielen.
Dies hat gezeigt, welche Probleme und Schwierigkeiten sich hinter dieser Technik verbergen und warum die Virtualisierung einer x86 Architektur lange Zeit als nicht möglich galt. Erst durch die Produkte von VMware und Connectix (mittlerweile von Microsoft gekauft und deren Produkt *Virtual PC* weiterentwickelt [Fors 07]) wurde diese Technologie Ende der 90er Jahre bekannt. Aktuelle Vertreter sind die Produkte von VMware (z.B. *VMware Server*, *VMware Workstation*), *Microsoft Virtual PC/Server* oder *VirtualBox*. Eine besondere Stellung der Hardwarevirtualisierung nimmt der *VMware ESX Server* ein, der zwar zu dieser Technologie zählt, aber ein eigenes Hostbetriebssystem mitbringt (genaueres siehe Abschnitt 3.2.2).

Paravirtualisierung

Bei der Paravirtualisierung handelt es sich um einen Kompromiss zwischen der Virtualisierung auf Betriebssystemebene und der Hardwarevirtualisierung [XEN 06]. Bei dieser neuesten Technologie greifen die voneinander eigenständigen virtuellen Maschinen mit ihrem jeweiligen Betriebssystem über eine bereitgestellte API direkt auf die gemeinsame Hardware zu. Die Koordination und Steuerung dieser Zugriffe übernimmt der *Virtual Machine Monitor*, hier *Hypervisor* genannt (siehe Abbildung 3.4). Diese spezielle Schnittstelle (API), die die verwendete Virtualisierungslösung vorgibt, muss für das Gastsystem implementiert werden (vgl. [XEN 07]). Dadurch ist keine Transparenz notwendig, denn durch die Implementierung ist dem Gastbe-

triebssystem bekannt, dass es mit dem Hypervisor über eine abstrahierte Hardwareschnittstelle kommuniziert (vgl. [XEN 06]). Aus diesem Grund muss keine Überwachung erfolgen, um alle *Exceptions* zu behandeln oder mögliche sensitive Zugriffe abzufangen, die vom Gastbetriebssystem kommen (vergleiche hierzu vorherige Technik). Das Wirtssystem kann nur noch aus dem Hypervisor bestehen (es gibt auch Produkte, die auf ein Betriebssystem aufsetzen), bei dem es sich um einem spezialisierten, optimierten Kernel handelt, sowie einem privilegiertem Betriebssystem für Management-Zwecke (siehe erste VM in Abbildung 3.4). Bis auf Ausnahmen werden ausschließlich die Treiber dieses privilegierten Systems verwendet, so dass eine Virtualisierung auf jeder Hardware möglich ist, auf der auch das Wirtsbetriebssystem läuft - unabhängig davon, welche Hardwarekomponenten das Gastsystem unterstützen [XEN 06]. Diese Technik, die sich hinter Paravirtualisierung verbirgt, kann auch als „erweiterter x86-Befehlssatz” [XEN 07] bezeichnet werden, den sowohl das Gastsystem, als auch der Hypervisor, implementiert. Deshalb ist die Virtualisierungssoftware Teil des eigentlichen Kernels und läuft nicht im Benutzer-Modus, wie bei der Hardwarevirtualisierung. Durch diese hardwarenahe Konzipierung entsteht nur ein geringer Overhead und sie macht damit diese Technik sehr leistungsstark. Die Virtualisierung ist „mit minimalen Leistungseinbußen möglich” [Herm 07] und die Verlustleistung zwischen einem paravirtualisierten und einem nicht virtualisierten System „beläuft sich in der Regel auf einige wenige Prozentpunkte” [XEN 07].
Bekanntester Vertreter dieser Technologie ist *XEN*, dessen Vorläufer das System *Denali* war (vgl. [XEN 07]). Eine genauere Behandlung von XEN erfolgt in Abschnitt 3.1.3. Ein weiteres Beispiel für Paravirtualisierung ist *User Mode Linux* im *SKAS* Modus. Genaueres dazu findet sich im Abschnitt 3.1.3.

3.1.3 Ein kurzer Marktüberblick

Im Folgenden werden nun einige Produkte vorgestellt, die die oben genannten Techniken einsetzen. Nicht immer ist eine klare Zuordnung möglich, da manche Produkte mehrere Virtualisierungstechniken verwenden. Jeder Hersteller hat sich auf unterschiedliche Gebiete spezialisiert, die im nächsten Abschnitt kurz genannt werden. VMware wird im darauffolgenden Abschnitt 3.2 separat behandelt, da es für die Realisierung des Konzeptes eingesetzt wird und eine gesonderte Stellung erhält.

Microsoft

Microsoft ist erst spät in den Virtualisierungsmarkt eingestiegen (vgl. [pcw 07]) und hat dadurch einen großen Nachteil sich auf dem Markt zu behaupten. Durch den Kauf der Firma *Connectix* im Jahre 2003 hat Microsoft eine Firma übernommen, die im Virtualisierungsbereich schon einige Erfolge erzielt hat und deren Produkt in das Portfolio von Microsoft aufgenommen und weiterentwickelt wurde. Daraus resultieren folgende Produkte von Microsoft:

- *Microsoft Virtual PC* - aktuell: Version 2007 für Windows und Version 7.02 für Mac OS
- *Microsoft Virtual Server* - aktuell: Version 2005 R2 Service Pack 1

Microsofts *Virtual PC* wurde ursprünglich für Mac OS PowerPC Systeme von der Firma *Connectix* entwickelt, um eine x86 Architektur zu emulieren. Dies war Bestandteil der Office Reihe für Mac OS (vgl. [Fors 07]). Im Jahre 2003 kaufte Microsoft *Connectix* und portierte ein Jahr später die Software für Windows [Fors 07]. Seit Mitte 2006 bietet Microsoft die Software kostenlos an. Die Mac-Version ist weiterhin kostenpflichtig.
Bei *Virtual PC* handelt es sich um einen Vertreter der Hardwarevirtualisierung [XEN 07] im Desktopbereich. Für den Macintosh ermöglicht *Virtual PC* inzwischen, Windows Programme unter Mac OS lauffähig zu machen [Fors 07]. Es handelt sich aber um einen Emulator, auf dessen Unterschiede bereits zu Beginn in Abschnitt 3.1 eingegangen wurde. *Virtual PC* gibt es, neben der Mac OS Version, nur für die gängigen Windows Betriebssysteme. Es unterstützt daher keinen Linux-Host [AHN 07]. Es virtualisiert einen Standard-PC mit dem Host Prozessor, bis zu drei Festplatten, ein CD-/DVD-Laufwerk, Arbeitsspeicher variabler Größe (abhängig von der Kapazität des Hosts), eine 100-MBit Netzwerkkarte, eine Audio-Karte und eine 8MB-Grafikkarte [Wiki 06]. Die Daten werden für jede virtuelle Maschine in einer Konfigurationsdatei gespeichert, die mit einem beliebigen Texteditor geöffnet und bearbeitet werden kann. *Virtual PC* zeichnet sich durch wenige, aber ausreichende Features aus [AHN 07]. Die gleichzeitige Anzahl an Gästen wird nur durch die Ressourcen des Hosts limitiert. Als Betriebssystem in einer virtuellen Maschine wird neben fast allen Windows

und Linux Varianten auch das Betriebssystem OS/2 unterstützt[3]. In Version 2007 kann auch die hardwareunterstützte Virtualisierung (siehe Abschnitt 3.1.4) verwendet werden. Zu den Nachteilen gehört eine fehlende Unterstützung bei den Gästen von USB und SCSI. Außerdem ist die Verwaltung von Wiederanlaufpunkten, sog. Snapshots, zwar möglich, aber umständlich zu handhaben. Wie bereits erwähnt, ist eine Installation von *Virtual PC* unter Linux nicht möglich (vgl. [AHN 07]).

Auf Basis der Technologie von *Virtual PC* entstand das Produkt *Virtual Server* und wurde im Jahr 2005 veröffentlicht [Fors 07]. Auch hier kann seit 2006 das Produkt kostenlos heruntergeladen und eingesetzt werden. *Virtual Server* arbeitet ähnlich wie *Virtual PC*, hat aber einige entscheidende Unterschiede und Erweiterungen. So läuft der Virtual Server nur auf Windows Serverbetriebssystemen. Für den nicht-produktiven Einsatz gibt es auch die Möglichkeit, Windows XP zu nutzen [Sier 06]. Mit Hilfe des Webserver *IIS* (Internet Information Services) von Microsoft können die Konfigurationsdateien der VMs verwaltet und bearbeitet werden. Zusätzlich bietet die Weboberfläche einige zusätzliche Einstellungen an (vgl. [Fors 07]). Die Bedienung des Gastsystems erfolgt, ähnlich einer Remote Desktop Protokoll-Verbindung (RDP-Verbindung), über den sogenannten Remotesteuerungsclient (RSC). Eine weitere Option ist die Host-Cluster-Funktion, bei der die Einbindung aller VMs eines Hosts in die Microsoft Cluster Dienste ermöglicht wird. Dadurch werden bei einem Host-Ausfall die Gäste auf einem anderen Knoten des Clusters neu gestartet (*Failover*) (vgl. [AHN 07]). Des Weiteren bietet *Virtual Server* die Funktion an, dass mittels „Suspend" die Gastmaschinen auf andere Cluster-Knoten verschoben werden können, falls Wartungsarbeiten am aktuellen Host notwendig sind.
Auch hier ist eine Installation auf einem Linux-Host nicht möglich (vgl. [Fors 07]). Die Performanz erreicht akzeptable Werte und bietet für Firmen mehrere Einsatzmöglichkeiten (vgl. [AHN 07]). Zu den Nachteilen gehören die unzureichenden Funktionen, die dadurch einen Einsatz im Datacenter Bereich verhindern. So unterstützt der *Virtual Server* beispielsweise keine 64-Bit Gastsysteme und reicht immer nur eine virtuelle CPU durch (vgl. [AHN 07]). Auch ist die Bedienung zur Verwaltung der virtuellen Maschinen teilweise kompliziert und nicht komfortabel (vgl. [Fors 07]).

Microsofts Virtualisierungsprogramme *Virtual PC / Server* eignen sich für kleinere Umgebungen und Tests durchaus, haben aber nie den gewünschten Marktanteil bekommen. Dies erklärt auch der Schritt, ihre kostenpflichtigen Programme seit 2006 kostenlos zu Verfügung zu stellen. VMware bietet ein Teil seiner Produktpalette schon länger kostenlos an, außerdem gibt es für größere Firmen kostenpflichtige Produkte, die wesentlich mehr können als die von Microsoft. Die nächsten Linux-Versionen von Suse und Red Hat bringen die freie Virtualisierungslösung Xen mit [Sier 06], das umfangreicher und leistungsstärker ist (siehe nächster Abschnitt). Daher entwickelt Microsoft eigene Virtualisierungstechniken (unter dem Namen „v.Next" [Zimm 06]) und wird diese in ihrem neuen Server-Betriebssystem (Codename Longhorn) unterbringen (vgl. [Sier 06]). Außerdem arbeitet Microsoft eng mit der Firma Citrix zusammen, die seit kurzem XenSource übernommen haben (vgl. [xen 07b]). Ob daraus sich neue Entwicklungen bei der Hostvirtualisierung ergeben, kann aber nur vermutet werden. Neben der Hostvirtualisierung ist Microsoft in den Bereich der Applikationsvirtualisierung durch den Kauf der Firma Softricity eingestiegen (vgl. [Fors 07]). Dabei handelt es sich um eine weitere Virtualisierungstechnologie, die auf eine komplett andere Zielgruppe abzielt. Aus diesem Grund, wird darauf nicht weiter eingegangen, es dient aber als Hinweis, dass Microsoft sich in anderen Bereichen mit Virtualisierung beschäftigt (mehr Informationen zu diesem Thema befinden sich unter [LUE 07]).

XEN

Der Vorläufer von XEN war das System *Denali*. Bei *Denali* handelt es sich um ein sehr performantes System, das aber die Anpassung sämtlicher Applikationen voraussetzt. Dies stellt eine kaum überwindbare Hürde für einen breiten Einsatz dar (vgl. [Rado 06]). Auf dieser Basis wurde XEN von der Systems Research Gruppe an der University of Cambridge als Teil eines anderen Projektes (XenoServers) entwickelt (vgl. [XEN 06]). Im Jahre 2003 erschien dann XEN 1.0 als eigenständiges Produkt und ist mittlerweile in der Version 3.1 erhältlich. Bei XEN handelt es sich um einen Open Source *Virtual Maschine Monitor*, hier Hypervisor genannt, für x86 (32 und 64 Bit-) Systeme, PowerPC und andere (vgl. [XEN 06]). Der VMM von XEN legt sich als zusätzliche Schicht über die Hardware und eine spezielle Schnittstelle ermöglicht die Zugriffe auf die Hardware. XEN

[3] Eine Liste aller unterstützten Versionen ist beispielsweise unter `http://vpc.visualwin.com/` zu finden.

kennt zwei Operationsmodi: die Paravirtualisierung (das Gastsystem muss angepasst werden) oder die Vollvirtualisierung (welche eine bestimmte Hardware voraussetzt) (vgl. [XEN 06]). Bei der Paravirtualisierung läuft der Hypervisor im Ring 0, das Gastbetriebssystem läuft im weniger priviligierten Ring 1 und die Userspace Prozesse laufen weiterhin in Ring 3 (vgl. [XEN 07]). Da ein Gastsystem von dem Hypervisor weiß, delegiert dieses alle privilegierten Operationen, die im Ring 1 zu einer Exception führen, an den Hypervisor von XEN (vgl. [XEN 07]). Die Systeme werden *Domains* genannt, die alle gleichberechtigt in ihren Funktionen sind. Ausnahme ist eine privilegierte Domain (*Domain 0* oder *dom0* genannt), die für die Steuerung des Hypervisors und der anderen Maschinen zuständig ist. Diese kann einzelne Domains starten, stoppen, pausieren, zerstören oder neue Domains erstellen (vgl. [XEN 06]). Zusätzlich können einige Managementfunktionen zur Konfiguration der Gäste vorgenommen werden.
Insgesamt kann durch XEN eine leistungsfähige Virtualisierungsumgebung aufgebaut werden, deren Entwicklung mittlerweile durch die Firma XenSource vorangetrieben wird (vgl. [xen 07b]). XenSource bietet mit *XenEnterprise* eine umfangreiche Infrastruktur, die in Konkurrenz zu VMwares Umgebung steht (vgl. [xen 07b]). Dieses Potential hat die Firma Citrix erkannt und seit August diesen Jahres XenSource übernommen (vgl. [xen 07b]). Wie bereits erwähnt, zählt zu den Nachteilen der Paravirtualisierung die Anpassung des Gastsystems. Dies ist bei Open Source Systemen in der Regel kein Problem, aber Windows kann so nicht verwendet werden. Daher gibt es noch die Möglichkeit der hardwareunterstützten Virtualisierung, die auf die Verwendung spezieller Prozessoren angewiesen ist (genaueres siehe in Abschnitt 3.1.4). Ein Mischbetrieb mit Paravirtualisierung ist aber auch möglich (vgl. [XEN 06]).
XEN ist ein leistungsstarkes und schnelles Virtualisierungsprodukt, das dank Open Source immer weiterentwickelt wird. Es gibt inzwischen mehrere Projekte zur Verbesserung und Optimierung wie z.B. die Enterprise Lösung von Xensource (vgl. [xen 07b]) oder einen webbasierten Managementserver von Enomaly (vgl. [Enom 07]). Die Vielzahl an unterstützten Systemen und die Eigenschaften (siehe Abbildung 3.19 auf Seite 36) zeigen, welche Stärken in dieser Lösung liegen, zusätzlich ist XEN auch noch frei verfügbar. Die Nachteile liegen einerseits im erhöhten Administrationsaufwand eines XEN Systems (vgl. [XEN 07]), andererseits gibt es bisher keine offizielle grafische Managementkonsole (Ausnahme: Bei *XenSource Enterprise* ist eine vorhanden und es gibt eine Open Source Entwicklung: *ConVirt / XenMan*; vgl. [xen 07a]). Des Weiteren existiert bisher kein offizielles Programm um physikalische Maschinen zu virtualisieren (sog. P2V -physical to virtual - Programme) (vgl. [XEN 06]), lediglich einige Dritthersteller, wie *Platespin Powerconvert* bieten XenSource als Zielsystem an (vgl. [pow 07]).

Weitere Produkte

Neben den bereits vorgestellten Produkten und die im späteren Verlauf extra behandelten VMware Produkte (siehe Abschnitt 3.2), gibt es eine Vielzahl weiterer Programme, die unter dem Namen Virtualisierung Werbung für sich machen. Der Markt ist in den letzten Jahren stark gewachsen, obwohl das Prinzip der Virtualisierung schon lange existiert (siehe Abschnitt 3.1.1). Auch wird der Begriff der „Virtualisierung” und der „Emulation” oft gleichbedeutend verwendet und weshalb einige Emulatoren auch zur Virtualisierung gezählt werden. Daher sei noch einmal darauf hingewiesen, dass ein Emulator (wie z.B. *Bochs* oder *Qemu*) eine komplette Architektur, die von der Architektur des Hostsystems abweichen darf, (beispielsweise laufen alte Spielekonsolen, wie Nintendos SNES oder Gameboy auf einer x86 Architektur) in Software abbildet [XEN 07]. Dies bedeutet, dass es sich beispielsweise bei der zu emulierenden CPU um eine Datenstruktur handelt, die von der Emulations-Software verändert wird. Zur Ein- und Ausgabe benutzt der Emulator das Wirtssystem. Alle Assembler-Befehle werden von der Software geladen, dekodiert und die Wirkung wird auf die Datenstruktur ausgeführt. So muss jeder Befehl zwischen Gast und Wirt entsprechend umgewandelt werden. Bei einer Virtualisierungssoftware werden die vorhandenen Komponenten aufgeteilt und die CPU des Wirtsystems lässt die meisten Prozessorbefehle direkt ausführen [Beie 06]. Eine Ausführung von Prozessorbefehlen des Gastes auf dem Wirt kann aber nur geschehen, wenn beide dieselbe Architektur unterstützen. Nur dann müssen die Befehle nicht für ein anderes System emuliert werden. Dies ist der große Unterschied zwischen Emulation und Virtualisierung.
Im Folgenden werden weitere Vertreter von Virtualisierungsprodukten vorgestellt. Dabei handelt es sich nicht um eine komplette Liste, sondern um einige ausgewählte Produkte:

- Bei *SWsoft Virtuozzo* handelt es sich um ein Produkt bei dem eine Virtualisierung auf Betriebssystem-Ebene erfolgt. Dies gibt es sowohl für Linux (seit 2001) als auch für Windows (seit 2005) (vgl. [SWso 07]).

Es bietet eine Verwaltungs-GUI, Arbeitslastverteilung durch Live-Migration, Tools zum schnellen Einrichten und Klonen von VMs und vieles mehr. SWsoft hat bei der Linux Variante, aus dem Open Source Programm *OpenVZ* ein benutzerfreundliches Paket entwickelt, um eine einfache und schnelle Handhabung zur Verfügung zu stellen (weitere Informationen unter [SWso 07]).

- Das kostenpflichtige *Virtual Iron 3.0* setzt als Basis auf XEN (⇒ auf die Paravirtualisierung) und erweitert dies mit eigenen Produkten wie dem *Virtualization Manager* (vgl. [Stie 06]). Mit diesem lassen sich die virtuellen Server überwachen, es können diese im laufenden Betrieb migriert werden oder es stehen Workload-Balancing Mechanismen zur Verfügung. Als Gastsysteme werden sowohl einige Linux- sowie Windowsdistributionen unterstützt (Weitere Infos befinden sich unter [Stie 06]).

- Mit *VirtualBox* der Firma innotek existiert ein kostenloser Virtualisierer, der sowohl für Windows, Linux (Kernel 2.4 oder 2.6) als auch Mac OS X zur Verfügung steht. Diese Hostsysteme können auch als Gäste verwendet werden, zusätzlich werden auch OS/2, Linux (Kernel 2.2), NetWare und diverse BSD Derivate unterstützt (vgl. [Died 07]). Die aktuelle Version 1.4.0 ist in zwei Versionen vorhanden: Eine Open Source Variante (genannt *VirtualBox OSE*) unter der GNU GPL (General Public License) und ein kostenfreies Komplettpaket für den privaten Gebrauch mit erweiterten Funktionen. Das deutsche Unternehmen *innotek* entwickelte bereits mit Connectix den *Virtual PC* und arbeitete danach am Linux Support von *Virtual PC* und *Virtual Server* (vgl. [Died 07]). *VirtualBox* war bisher nur an besonderen Stellen eingesetzt worden, ist aber seit Anfang 2007 für den Endanwender erhältlich. Es zählt, laut Homepage, zu den 'Full Virtualization' Produkten und versucht so viel Code wie möglich nativ auszuführen (vgl. [inn 07]). Daher läuft in den meisten Fällen der Ring 3 Code des Gastsystems nativ auf dem Hostsystem. Versucht nun der Gast Ring 0 Code auszuführen, führt der Gast diesen im Ring 1 aus und kann dies über den Hypervisor steuern und entsprechend weiterleiten. *VirtualBox* bietet einige Zusatzfunktionen, wie die Unterstützung von VMWare Festplattendateien (seit Version 1.4), USB Geräten, Zugriff per RDP auf die VMs, iSCSI Unterstützung und es gibt Gast-Erweiterungen („Guest Additions"), ähnlich den VMware Tools (siehe Abschnitt 3.2) mit zusätzlichen Erweiterungen zwischen Gast und Host (vgl. [inn 07]). Das Leistungsverhalten ist ähnlich zu den kostenfreien Produkten von VMware und durchaus eine Konkurrenz zu VMware oder Microsoft (vgl. [Died 07]). Nach und nach sollen die erweiterten Merkmale auch in die Open Source Variante integriert werden, für jeden verfügbar und erweiterbar sein.

- *User Mode Linux* wurde bereits in Abschnitt 3.1.1 kurz vorgestellt und ist in seiner ursprünglichen Form eher der Virtualisierung auf Betriebssystem-Ebene zuzuordnen. *UML* hat in seiner ursprünglichen Form ein Sicherheitsproblem, da keine korrekte Trennung des Adressraumes vorgenommen wird. Zusätzlich ist der Adressraum entweder beschreibbar (writable), wodurch ein Prozess ausbrechen kann, oder es setzt die *UML* Daten auf nur lesbar (readonly), was aber zu einem enormen Performanzeinbruch führt (vgl. [ska 07]). Dieses Problem wird durch einen Patch, mit dem Namen *SKAS* (Separate Kernel Address Space) behoben. Wie der Name schon sagt, ermöglicht dieser, für einen Prozess mehrere separate Adressräume zu erzeugen. Daher gibt es nur noch einen einzelnen Prozess, der sich um die virtuellen Prozesse in den virtuellen Umgebungen im UML kümmert. Zusätzlich wurde die *ptrace*-Schnittstelle um neue Funktionen erweitert, die es ab sofort erlauben, sich selbst zu unterbrechen (vgl. [ska 07]). Der Prozess, der sich um die virtuellen Prozesse kümmert, kann sich mit dem *ptrace* Kommando selbst unterbrechen, z.B. auf Grund eines Schedules, seinen Adressraum zu ändern und einem anderen Prozess die Möglichkeit der Ausführung zu geben. Diese Aufgaben entsprechen laut vorheriger Definition die eines Hypervisors. Aus diesen Gründen kann *UML* mit *SKAS* Patch zur Technik der Paravirtualisierung hinzugezählt werden.

Die Entwicklung und Forschung neuer Technologien ist vor allem im IT Bereich ein ständig fortlaufender Prozess. So entsteht eine stetige Verbesserung von aktuellen Problemen und es kommen ständig neue Ansätze, wie eine Lösung aussehen könnte, dazu. Nachdem nun eine kurze Marktübersicht gegeben wurde, werden in den nächsten beiden Abschnitten zwei Entwicklungen vorgestellt, die einerseits eine verbesserte Leistung durch hardwareunterstützte Virtualisierung gewährleisten, andererseits eine Technologie, die teilweise als Konkurrenz aber auch als sinnvolle Ergänzung zur Virtualisierung gesehen wird (vgl. [Rode 07]).

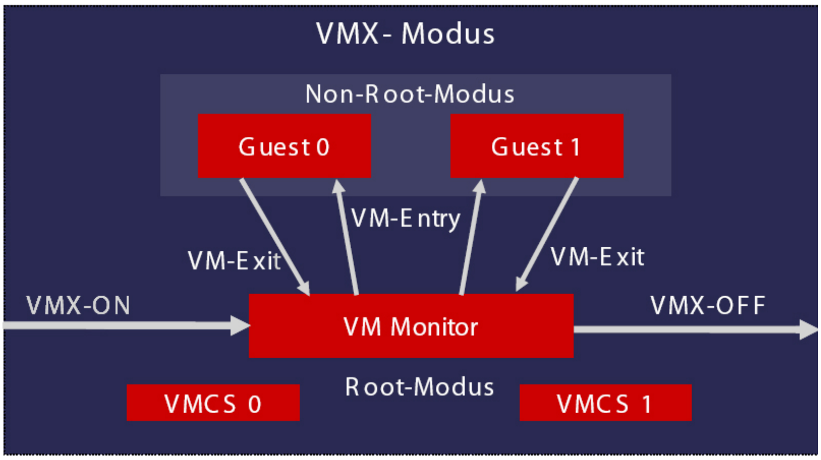

Abbildung 3.5: Vereinfachter Kontextwechsel zwischen *VMX root* und *VMX Nonroot* bei Intels VT-x (Quelle: [Kers 05])

3.1.4 Virtualisierungsunterstützung in Prozessoren

Bei den bisher vorgestellten Softwarelösungen zur Virtualisierung liegt immer ein Performanzverlust vor. Bei einem Einsatz eines VMM / Hypervisor kontrolliert dieser ständig den Zugriff der virtuellen Maschinen auf die Hardware. Der VMM muss alle Zugriffe abfangen und entsprechend weiterleiten. Diese Kontextwechsel „kosten” Performanz und können bei steigender VM-Anzahl zu Leistungseinbußen führen. Zusätzlich ist beispielsweise bei XEN eine Anpassung des Betriebssystems notwendig, damit diese Systeme im Ring 1 laufen (siehe Abschnitt 3.1.3:„Paravirtualisierung”). Dies ist aber bei proprietären Betriebssystemen nicht möglich und sie können daher nicht unterstützt werden. Mit Hilfe von bestimmten Funktionen des VMM in einem Prozessor können diese Probleme gelöst werden. Seit 2006 gibt es sowohl von Intel als auch von AMD eine neue Prozessorgeneration mit Virtualisierungsunterstützung. Bei Intels VT-x wird der Befehlssatz VMX (Virtual Machine Extensions) und bei AMD-V SVM (Secure Virtual Machine) genannt (vgl. [XEN 06]).

Bei Intel erhalten IA32-CPUs mit Vanderpool-Technologie VT-x den sogenannten VMX-Befehlssatz (vgl. [Vils 05b]). Dabei gibt es nun zwei Modi: *VMX Root* und *VMX Nonroot*. Diese bestehen jeweils aus den 4 bereits bekannten Ringen (siehe Abbildung 3.3 in Abschnitt 3.1.2). Der Modus *VMX Root* entspricht dabei weitestgehend (bis auf wenige zusätzliche Virtualisierungs-Instruktionen) dem normalen Modus ohne spezielle Erweiterung. Im Modus *VMX Nonroot* dagegen sind Instruktionen im Vergleich zum normalen Modus eingeschränkt, um dem VMM die Kontrolle über die virtuellen Maschinen zu ermöglichen. Die Einschränkungen beziehen sich auf die Ausführung kritischer Befehle (z. B. Zugriffe auf gemeinsam genutzte Ressourcen), die an den VMM übergeben werden und auf die dieser dann entsprechend reagiert. Der VMM läuft im *VMX Root* Modus und besitzt daher die volle Kontrolle über die CPU und die restlichen Komponenten des Servers (vgl. [Vils 05b]). Die VMs, beziehungsweise die Gast-Software, arbeitet im *VMX Nonroot* Modus (siehe Abbildung 3.5). Der VMM initialisiert und startet (über den Befehl „VM-Entry”) jede virtuelle Maschine. Daraufhin wechselt der Prozessor in den *VMX Nonroot* Modus und führt den Code der virtuellen Maschine aus. Treten systemkritische Situationen wie eine Exception auf, entzieht der Prozessor automatisch der VM die Kontrolle und übergibt diese an den VMM (mittels des Befehls „VM-Exit”), der dann entsprechend handelt (siehe Abbildung 3.5). Soll eine gestoppte virtuelle Maschine weiter rechnen dürfen, so wird die Kontrolle an die VM zurückgegeben. Bei diesem Ablauf führt der Prozessor die meiste Zeit den Code der virtuellen Maschine direkt aus und muss nur in wenigen Fällen zum VMM wechseln, um kritische Situationen zu beheben (vgl. [Vils 05b]). Die Gastsoftware erkennt während der aktiven Zeit nicht, dass sie im *VMX Nonroot* Modus arbeitet, da für sie die ganz normale Ringstruktur vorherrscht. Deshalb ist eine Anpassung der Betriebssysteme nicht notwendig. Die Kontrolle über die Informationen und den Zustand der VMs übernimmt eine neue Datenstruktur mit der Bezeichnung VMCS (Virtual-Machine Control Structur), die sich im physikalischen Adressraum befindet (vgl. [int 05]). Da mehrere VMs gleichzeitig laufen können, existiert pro VM eine VMCS (siehe Abbildung 3.5). Die Initiierung und Festlegung der Werte übernimmt der VMM und kann damit

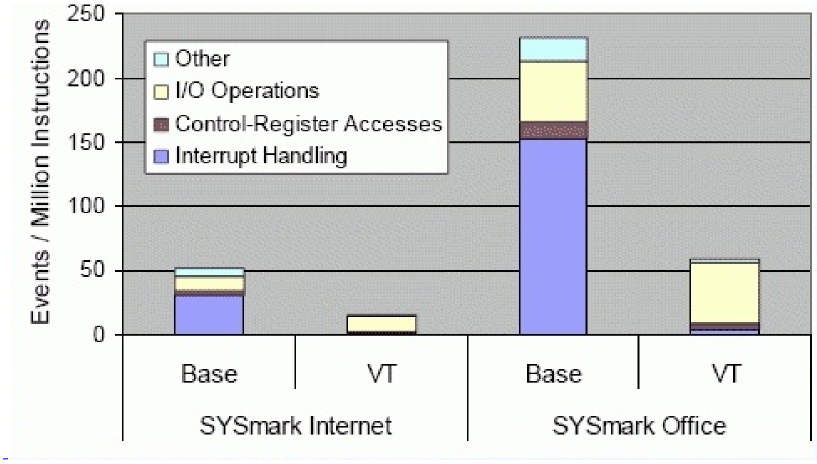

Abbildung 3.6: Leistungsvergleich zwischen herkömmlicher VM-Software (mit *Base* gekennzeichnet) und der Vanderpool-Lösung (mit *VT* gekennzeichnet) (Quelle: [Vils 05b])

unterschiedliches Verhalten der VMs erzeugen.
Unterstützung findet Vanderpool in den gängigsten Virtualisierungslösungen. Sowohl Microsoft, VMware oder XEN verwenden sie teilweise in ihren neuesten Produkten (vgl. [Ahne 07]). Intel hat einen Leistungsvergleich veröffentlicht, der das Verhalten mit und ohne Einsatz ihrer Technologie dokumentiert. Abbildung 3.6 zeigt dies für zwei Tests von SYSmark mit typischen Internet- und Officeaktionen (genauere Informationen zu den Anwendungen sind unter [sys 03] zu finden). Für beide Benchmarks ist das Verhalten jeweils mit einem Säulendiagramm dargestellt, das sich aus „I/O Operations”, „Control-Register” Zugriffen, „Interrupt Handling” und anderen Instruktionen („Other”) zusammensetzt. Anhand des Säulendiagramms mit eingesetzter Technologie (siehe in Abbildung 3.6 für VT) ist vor allem der starke Rückgang des „Interrupt Handling” zu erkennen. Dies liegt daran, dass ein Kontextwechsel nur in kritischen Situationen notwendig ist und die meiste Zeit der Code einer VM direkt auf dem Prozessor ausgeführt wird. Die anderen Instruktionen gehen auch leicht zurück, fallen aber nicht so signifikant auf wie das „Interrupt Handling”. Intel selbst klassifiziert Vanderpool nur als ersten Schritt in Richtung Virtualisierung. Noch wird für die Virtualisierung die entsprechende Software (Host-OS und VM-Software) benötigt. Die Idealvorstellung wird zukünftig sein, dass die Hardware die Virtualisierung gleich selbst erledigt. So lässt Intel in den Vanderpool-Spezifikationen bereits jetzt Spielraum für Erweiterungen [Vils 05b]. In Zukunft sollen neben dem Netzwerk-Controller und dem Storage-Subsystem sogar die Grafikkarte virtualisiert werden (vgl. [Vils 05b]). Dies sind aber bisher nur Ideen und es gibt noch keine Entwicklungen oder gar Produkte in diesem Bereich.

Bei der AMD Prozessortechnologie unter dem Namen „AMD Virtualization” (AMD-V) (früher unter dem Codenamen „Pacifica”) ist die Funktionsweise ähnlich der von Intels neuen Prozessoren. Die Ringtopologie und der Hypervisor sind gleich, sie wurden nur mit anderen Namen besetzt. Die Datenstruktur zur Kontrolle und Informationsspeicherung der VMs heißt bei AMD VMCB (Virtual Machine Control Block), unterscheidet sich aber ansonsten von Intels Datenstruktur nicht. Dennoch gibt es einige Unterschiede zwischen den beiden Architekturen. Dies liegt vor allem daran, dass AMD Prozessoren einen integrierten Memory Controller besitzen, der mit der AMD-V Technologie auch virtualisiert wird (vgl. [Vils 05a]). Jede VM hat ihren eigenen Adressbereich, der unter der Kontrolle des VMM steht. Bei einer Adressanfrage einer VM muss der VMM diese entsprechend auf die zugewiesene physikalische Adresse umleiten. Werden die Daten aus dem Speicher gelesen, so muss die Virtualisierungssoftware erneut die Daten zur virtuellen Maschine umleiten [Vils 05a]. Bei Intels Vanderpool geschieht dies durch die Software und kostet Zeit. AMD kann dies durch seine Architektur hardware-unterstützend erledigen. Dieser „Nested Pages” Modus stellt jeder VM ein eigenes virtualisiertes Register zur Verfügung. In diesem werden die entsprechenden Seiten geladen und gespeichert. Da diese Vorgänge aber hardware-basierend erfolgen, kann damit eine erhöhte Effizienz erreicht werden (vgl. [amd 07]). Ein weiteres Kennzeichen von AMD-V stellt der DEV (Device Exclusion Vector) dar [Vils 05a]. Damit werden DMA (Direct Memory Access) Zugriffe und entsprechende Peripherie, die DMA nutzen, be-

Abbildung 3.7: Ein Blade der Firma Dell - Modell Poweredge 1955 (Quelle: [del 07])

handelt. Wie DMA schon sagt, greifen solche Geräte direkt auf den Speicher zu und zwar ohne den Umweg über die CPU (Ausnahme ist die Initialisierung des Speicherzugriffs). DEV bietet in VMs einen Schutz vor dem Zugriff DMA-fähiger Geräte auf den physikalischen Speicher und überprüft bei jedem DMA Zugriff dessen Gültigkeit [Vils 05a]. Als letzen Unterscheidungspunkt bietet AMD Sicherheitseigenschaften für das „Trusted Computing” [4] (TP) mit Namen „Presidio”. Diese Eigenschaften sind für eine Virtualisierung aber nicht notwendig und bieten daher einen Vorteil gegenüber Intel für mögliche zukünftige Programme, die dies unterstützen und verwenden wollen.
Die Virtualisierungstechnologie von AMD ist mit Intels Vanderpool nicht kompatibel, was an den zu starken Unterschieden in der Architektur liegt. Der integrierte Speicher-Controller bei AMD wird auch effizent genutzt und ist bei Programmen mit hoher Speicherlast performanter als bei Intel (vgl. [Vils 05a]). Bisher gibt es aber keine unabhängigen Tests, die diesen Performanzvorteil darlegen. Auch sei an dieser Stelle noch einmal erwähnt, dass der Leistungsvergleich in Abbildung 3.6 von Intel selbst stammt. Genau wie Intels Vanderpool findet auch AMD-V in allen neuesten Versionen von Virtualisierungsumgebungen teilweise Unterstützung (vgl. [Ahne 07]).

Mit der Weiterentwicklung zur Virtualisierung von Komponenten in der entsprechenden Hardware, gibt es in Zukunft noch großes Potential, diese Technik weiter zu verbessern. Aber auch eine andere Technologie ist in den letzten Jahren aufgetaucht, die immer häufiger in Verbindung mit Virtualisierung genannt wurde. Diese nennt sich „Blades” oder auch „Blade Server” und wird im nächsten Abschnitt genauer vorgestellt.

3.1.5 Blades

Eines der Ziele, dass mit der Hilfe von Virtualisierung erreicht werden soll, ist die Konsolidierung von Servern. Dadurch wird weniger Platz für physikalische Server benötigt. Des Weiteren können ein Abbau an Komplexität (weniger Netzwerkkomponenten, wie Verkabelung) und geringere Betriebskosten erzielt werden. Genau diese Vorteile möchten Blades auch erreichen. Bei Blades handelt es sich um eine kompakte Bauweise von Servern mit eigenständigen Mikroprozessoren, bis zu zwei Festplatten, Arbeitsspeicher und Netzwerkanschlüssen auf dem Mainboard. Dieses Modul wird in ein spezielles Gestell (Rack) eingeschoben und ist dann mit der Backplane verbunden. Das Rack übernimmt zentral die Stromversorgung und die Kühlung (vgl. [Hüls 06]). Die Verkabelung verläuft im idealen Fall intern in einem Blade und so ist keine zusätzliche Verkabelung notwendig. Ziel dieses Konzeptes ist es, platzsparend entweder möglichst viele Server (*High Density*) in einem Rack

[4] Bei TP handelt es sich um eine Allianz aus mehreren namhaften Herstellern im Soft- und Hardwarebereich, die einen Standard für „sichere” Computer-Plattformen entwickeln. So sollen Software-Angriffe als auch Veränderungen durch Konfiguration, Fehlfunktionen, Sicherheitslücken und Einflüsse des eigenen Betriebssystems oder der Anwendungsprogramme eindeutig identifiziert werden können. Aber gerade dieser starke Eingriff und die Auslegung des Wortes „trusted” sorgt für kontroverse Diskussionen.

Abbildung 3.8: Einschub mit mehreren Blades für ein 24U oder 42U Dell Rack (Quelle: [del 07])

unterzubringen, oder möglichst viel Serverleistung (*High Performance*) pro Serverschrank zu erzielen (vgl. [Hüls 06]). Im Idealfall wird bei erhöhtem Ressourcenbedarf ein vorrätiges Blade ins Rack eingeschoben und angeschaltet. Daraufhin steht der Server zur Verfügung und auch im Fehlerfall kann der defekte Server nach demselben Prinzip einfach ausgetauscht werden. Mittlerweile bieten alle großen Hersteller wie Dell, Sun, HP oder IBM ein Bladesystem an. Ein Beispiel für ein Blade und der zugehörige Einschub für ein Rack ist in Abbildung 3.7 und 3.8 zu sehen. An dieser Stelle sei darauf hingewiesen, dass die Hersteller die Blades teilweise sehr unterschiedlich bestücken. Beispielsweise werden bei IBM in der Regel keine Festplatten verbaut, sondern es gibt einen zentralen Plattenspeicher, der für die Blades partitioniert wird. Dadurch können noch kompaktere Blades gebaut werden, die kleiner als das in Abbildung 3.7 gezeigte sind.
Neben den genannten Vorteilen, gibt es einige Kritikpunkte und Schwachstellen bei Blades. So haben zwar IBM und Intel ihre Bladeserver-Spezifikation teilweise offen gelegt, um einen Standard zu definieren, doch sind die Standards zueinander inkompatibel (vgl. [Schm 06]). So ist es notwendig sich auf ein Hersteller festzulegen, wenn eine Bladelösung eingesetzt werden soll. Zusätzlich muss ein Rack mindestens zur Hälfte gefüllt sein, um dieses rentabel zu machen (vgl. [Schm 06]). Solch ein Rack kann aber nicht immer ganz gefüllt werden, denn sobald ein Blade z.B. für PCI Steckplätze erweitert werden soll, kann dies nur mit Hilfe eines „Riser Moduls” geschehen, was meist den Platz eines Blades kostet (vgl. [Hüls 06]). Dies gilt auch für weitere Festplatten oder leistungsstärkere CPUs, da zusätzliche Kühlkörper mehr Platz verbrauchen. Die hohen Erstanschaffungskosten schrecken viele Firmen ab und daher werden Blades meist für gezielte Projekte und Teilsysteme eingesetzt (vgl. [Bote 07]). Neben der Abwägung, ob sich eine Bladelösung rechnet, führen vor allem die Versprechungen und Erwartungen zu Missverständnissen (vgl. [Hüls 06]). Blades teilen sich „nur” dieselbe Stromversorgung und Kühlung, die aber keinen übergeordneten Controller besitzen, der alle Dienste überwacht und im Fehlerfall diese auf ein anderes Blade schiebt. Auch die versprochene Hochverfügbarkeit durch den schnellen Austausch ist nicht gegeben, denn es kann zwar schnell ein defektes Blade ausgetauscht werden, aber dennoch gibt es von vornherein keine gesicherten Informationsverbindungen zwischen den Blades, die im Fehlerfall ein neues Blade aktivieren (vgl. [Hüls 06]). Außerdem eignen sich nicht alle Anwendungen, um diese auf Blades laufen zu lassen. Vor allem speicherintensive Applikationen stoßen an ihre Grenzen, da es in den meisten Blades nicht genügend RAM Steckplätze gibt, um diese entsprechend zu erweitern.
Auf Grund dieser Probleme gibt es sogar einige Firmen, die sich wieder von ihrem Bladesystem trennen (vgl. [Schm 06]). Durch diese Erfahrungen preisen die Hersteller Blades nicht für jedes Rechenzentrum an, sondern bieten mittlerweile Komplettlösungen für bestimmte Bereiche, wie beispielsweise SAP oder Oracle an (vgl. [Hüls 06]). Neue Techniken wie Dual-Core, halten Einzug bei Blades und werden in Zukunft leistungsfähige-

re Server erzeugen. Ob sich diese Technik in Zukunft durchsetzen wird, hängt auch von der Standardisierung dieser Technologie ab, die bisher nur in wenigen Bereichen vorhanden ist (vgl. [Hüls 06]).

Nachdem nun die Virtualisierung mit ihrer Geschichte, ihren Möglichkeiten und ihren Produkten vorgestellt wurde, folgt im nächsten Kapitel ein ausführlicher Einblick in die Virtualisierungsumgebung von VMware. Diese wird für die Realisierung des Konzeptes (vergleiche Kapitel 6) verwendet und bietet vielfältige Funktionen und Möglichkeiten an. Hierbei gibt es neben einigen kostenlosen Programmen das kostenpflichtige *VMware Infrastructure 3* Paket, das viele Funktionen, beispielsweise automatisierte Lastverteilung, bietet.

3.2 VMware

Die VMware Inc. wurde 1998 gegründet und stellte 1999 mit dem Produkt *VMware Workstation* eine Applikation vor, Virtualisierung auf x86 Systemen in akzeptabler Geschwindigkeit zu ermöglichen (vgl. [vmh 07]). Im Januar 2004 übernimmt die EMC Corporation VMware für 635 Millionen US Dollar und bringt 10 Prozent der Anteile am 14. August 2007 an die Börse (vgl. [Zieg 07]). Damit war VMware am ersten Handelstag rund 19,1 Milliarden US-Dollar wert.
VMware bietet für die unterschiedlichen Anwendungsgebiete eine Vielzahl an Produkten im Bereich der Virtualisierung an. Um welche es sich dabei handelt und wie deren Eigenschaften aussehen, wird im folgenden Abschnitt geklärt. Die eingesetzten Produkte verwenden alle die Technik der Hardwarevirtualisierung, wobei die neueste Version von *VMware Workstation* zusätzlich Paravirtualisierung (beide Techniken siehe Abschnitt 3.1.2) verwenden kann.

3.2.1 Produkte

VMware bietet, je nach Bedarf, mehr oder weniger umfangreiche Virtualisierungslösungen an. Es folgt eine Liste mit allen wichtigen angebotenen Produkten, die in zwei Gruppen unterteilt sind. In der Gruppe der Desktop - Virtualisierung geht es um Programme, die für den privaten Gebrauch oder im kleineren Geschäftsumfeld verwendet werden können. In der zweiten Gruppe werden Produkte für den Serverbereich vorgestellt, die vor allem für den Einsatz in Unternehmen gedacht sind. Alle Programme werden danach genau vorgestellt, vor allem in Bezug auf deren Eigenschaften und Einsatz.

1. Desktop - Virtualisierung
   - *VMware Player*
   - *VMware Workstation*
   - *VMware Fusion*
2. Server - Virtualisierung
   - *VMware Server*
   - *VMware Infrastructure*

Seit Oktober 2005 bietet VMware den *VMware Player* kostenfrei an. Dieser ist im Moment in der Version 2.0 sowohl für Windows als auch für Linux vorhanden. Mit Hilfe des Players können virtuelle Maschinen abgespielt werden. Diese müssen aber zuvor entweder mit einem Produkt von VMware (*VMware Workstation*; *VMware Infrastructure*; *VMware Server*) oder Microsoft (*Virtual PC*; *Virtual Server*) erstellt werden (vgl. [ZIM 06]). Zusätzlich bietet VMware bereits vorgefertigte Maschinen auf seiner Homepage (`http://www.vmware.com/appliances/`) zum freien Gebrauch an. Eine nachträgliche Konfiguration der Gäste (Hinzufügen virtueller Festplatten, Zuteilung von mehr RAM, etc.) ist nicht möglich. Unterstützt werden als Gastsysteme die meisten Windowsversionen, Linux, Netware, Solaris und FreeBSD. Der Player muss auf einem Wirtsbetriebssystem (Windows oder Linux) installiert werden, der dann als VMM fungiert (genaueres siehe Abschnitt 3.1.2). Zu den wichtigsten Eigenschaften zählt der Betrieb mehrerer VMs gleichzeitig, Zugriffe auf lokale Geräte des Wirtssystems (wie z.B. CD-/DVD-ROM oder USB 2.0), verschiedene

Netzwerkmodi (um die VMs in unterschiedlichen physikalischen Netzen zu betreiben), der 32- und 64-Bit Support für Wirts- und Gastbetriebssystem und das Kopieren von Dateien per „Drag & Drop” zwischen Wirt und Gast [ZIM 06]. Einsatzgebiete sind sowohl im privaten als auch im geschäftlichen Umfeld denkbar. Neben den klassischen Testumgebungen mit verschiedenen Versionen und Systemen können VMs auch als isolierte Umgebungen verwendet werden. Der einfach zu bedienende *VMware Player* hat zum Beispiel eine VM mit einer kostenfreien Linuxdistribution gestartet, mit der ein sicheres Surfen im Internet oder Homebanking möglich ist. Sollte es einen Virenbefall geben, ist nicht das eigentliche System, sondern die abgekapselte VM betroffen. Auch können Applikationen zuerst in der VM installiert und getestet werden, bevor sie für das eigene System verwendet werden.

VMware Workstation, das im Moment in der Version 6.0 vorliegt, hat neben den Funktionen von VMware Player noch weitere Einstellungsmöglichkeiten. Die kostenpflichtige Software erlaubt es, virtuelle Maschinen zu erstellen und nachträglich zu konfigurieren (vgl. [AHN 07]). Auf diese Weise ist das Ändern der Hardwareeinstellungen und das Hinzufügen von virtuellen Platten möglich. Zusätzlich gibt es die Funktion der *(multiple) Snapshots*, womit mehrere Zustandssicherungen einer VM vorgenommen werden können, um bei Bedarf wieder an den gesicherten Zustand zurückzukehren. Auch die Multiprozessorunterstützung (VirtualSMP) in einer VM ist hier möglich, um dieser beispielsweise mehrere CPU Kerne zuzuordnen (vgl. [ZIM 06]). Für virtuelle Maschinen gibt es zur Verwaltung und Erstellung einige Funktionen, die dies erleichtern. So können VMs zu einem Team zusammengefügt werden, um dies zu einem bestimmten Zeitpunkt an- oder abzuschalten. Mit Hilfe von Vorlagen (Templates) können VMs schnell eingesetzt werden. Auch das Klonen von vorhandenen VMs ist möglich. Ein besondere Eigenschaft ist die Möglichkeit des Mitschitts von Videos (auch Screenshots) innerhalb der virtuellen Maschine. So können Vorgehen oder Testabläufe aufgenommen werden, ohne dass eine zusätzliche Software benötigt wird (vgl. [AHN 07]). Wie bereits erwähnt, bietet *VMware Workstation* zusätzlich die Möglichkeit der Paravirtualisierung an. So ist es hier möglich, über eine eigene Schnittstelle, genannt „Paravirt-ops”, Linux Betriebssysteme zu paravirtualisieren (vgl. [vmh 07]). Bei Paravirt-ops handelt es sich um eine offene Schnittstelle, die ständig erweitert und optimiert werden kann. Insgesamt bietet *VMware Workstation* eine Vielzahl an Funktionen, wobei es vorher zu klären gilt, ob diese auch genutzt werden. Das Erstellen von VMs kann auch über andere kostenfreie Programme (wie z.B. der *VMware Converter 3.0* in der Starter Edition [vmh 07]) geschehen und diese in Kombination mit dem *VMware Player* ohne Aufpreis nutzen.

Bei *VMware Fusion (for the Mac)* handelt es sich um eine Virtualisierungslösung für Intel-basierte Macs, die im August diesen Jahres in der Version 1.0 veröffentlicht wurde. Die Basisplattform für die Virtualisierung ist dieselbe, die auch bei den anderen Produkten eingesetzt wird. Daher werden die gleichen Betriebssysteme unterstützt wie in den anderen VMware-Versionen, darunter auch Windows Vista und Solaris 10 [Seeg 07]. Der Funktionsumfang ist ähnlich wie bei *VMware Workstation*. So gibt es eine 64-bit Unterstützung, das Erstellen von Gastsystemen, eine USB 2.0 Unterstützung und auch die VirtualSMP Unterstützung. Apple hat Intel Core Duo Prozessoren verbaut und daher können dem Gastsystem sowohl ein, als auch zwei Prozessoren zu Verfügung stehen (vgl. [vmh 07]). Interessant für Mac Benutzer ist die Unterstützung von hardwarebeschleunigter 3D Grafik bis DirectX 8.1 unter Windows XP (vgl. [vmh 07]). Hier können Spiele, die es für den Mac nicht gibt, auf einer virtuellen Windows XP Maschine laufen, solange diese DirectX 8.1[5] oder weniger nutzen. Zusätzlich gibt es noch den „Unity-Mode”, der es erlaubt, dass Windows-Programme wie normale Mac-OS-X-Applikationen auf dem Mac-Desktop laufen können. Diese Funktion liefert auch der Hauptkonkurrent *Parallels Desktop*, der bisher als einziger eine umfassende Virtualisierungsumgebung für Max OS-X Nutzer angeboten hat (vgl. [Seeg 06]). Zu diesem tritt auch *VMware Fusion* hauptsächlich in Konkurrenz und verbessert durch eine lange Entwicklung einige Eigenschaften, wie erhöhte RAM Unterstützung (Fusion: 8GB; Parallels: 1,5GB) in Gastsystemen. Zusätzlich wird auch Apples *Boot Camp*[6] unterstützt und erlaubt sogar eine Portierung als Gast in eine VM. Interessantes Detail: *VMware Fusion* unterstützt offiziell Mac OS-X nicht als Gastsystem, da Apple durch seine Lizenz festlegt, dass Mac OS-X nur auf den Intel-Macs selbst läuft [Seeg 06]. Insgesamt bietet VMware ein umfangreiches Paket für den Mac mit vielen interessanten Funktionen. Ob die Performanz der gelieferten Eigenschaften, gerade im 3D Grafik Bereich, auch das Versprochene liefert, kann sich erst in der Zukunft zeigen, wenn das Produkt einige Zeit am Markt ist.

[5] Mittlerweile ist unter Windows Vista bereits DirectX 10 verfügbar.

[6] Bei *Boot Camp* handelt es sich um Software, die es erlaubt Windows XP als zweites Betriebssystem auf einem intel-basierten Mac zu installieren.

Der *VMware Server* in der aktuellen Version 1.0.1 ist der kostenlose Nachfolger des mittlerweile eingestellten *VMware GSX Servers*. Daher finden sich oft noch Verweise auf den ehemals kostenpflichtigen GSX Server, der zwar noch supportet, aber nicht mehr vertrieben wird (vgl. [LAR 07]). Grob lässt sich der *VMware Server* als abgespeckte Version des *VMware Workstation* mit erweiterten Administrationsfunktionen bezeichnen. So werden auch hier dieselben Gastsysteme (32- und 64-bit) unterstützt und es lassen sich VMs erstellen, die dann beispielsweise mit dem *VMware Player* verwendet werden können. Folgende Funktionen sind aber beim *VMware Server* nicht vorhanden: keine Erstellung von Templates, keine Teambildung, d.h. Gruppierung von VMs, keine Videoaufzeichnung innerhalb einer VM, nur ein Snapshot pro VM und keine USB 2.0 Unterstützung (vgl. [AHN 07]). Für das Management sind aber Anknüpfungspunkte bereitgestellt. So kann die Verwaltung der VMs direkt auf dem installierten Rechner vorgenommen werden. Für einen Zugriff über das Netzwerk ist entweder ein web-basiertes Management oder das kostenpflichtige *VMware Virtual Center* (VC) möglich, wobei nur Version 1.4 und nicht Version 2.0 unterstützt wird (vgl. [vmh 07]). Mit Hilfe von VC können Hosts und VMs übersichtlich unter einer einheitlichen Oberfläche verwaltet und gesteuert werden (vgl. [AHN 07]). Dies benötigt aber einen kostenpflichtigen *Virtual Center Management Server* und für jeden verwendeten *VMware Server* einen zu lizenzierenden *Virtual Center Agent*. Sind mehrere *VMware Server* im Einsatz bietet sich das VC an, um alle Hosts und deren virtuelle Maschinen im Überblick zu haben. Diese Möglichkeit gibt es aber nur für das Hostsystem „Windows 2000/2003 Server” und „Windows XP” (vgl. [LAR 07]). Aus diesem Grund kann für Linux nur die web-basierte Lösung verwendet werden.
Den *VMware Server* kostenlos zur Verfügung zu stellen, ist einerseits eine Reaktion auf die kostenlosen Produkte von Microsoft (siehe Abschnitt 3.1.3) und dient andererseits zum Einstieg in das Thema Virtualisierung. Langfristiges Ziel dabei ist, dass die Kunden auf das kostenpflichtige *VMware Infrastructure 3* umsteigen. Dieses bietet zusätzliche Funktionen, die virtuellen Maschinen sind aber kompatibel und lassen sich ohne Probleme migrieren (vgl. [AHN 07]).

Mit der *VMware Infrastructure 3* Umgebung bietet VMware ein Paket auf Data Center Niveau, das eine Vielzahl von Eigenschaften und Programmen mitliefert. Eine genaue Beschreibung der Komponenten und Eigenschaften erfolgt im nächsten Schritt. Die Umgebung liegt in den drei Versionen „Starter”, „Standard” und „Enterprise” vor. Die „Starter” Version beinhaltet einen eingeschränkten ESX Server, das zugrundeliegende Dateisystem VMFS und den *Virtual Center Agent*. Die anderen beiden Versionen haben keine Einschränkungen beim ESX Server, dem Dateisystem und nutzen VirtualSMP. Die „Enterprise” Variante bietet zusätzliche Funktionen im Bereich Hochverfügbarkeit und Backupsicherung, die aber je nach Bedarf auch separat für die anderen Versionen lizensiert werden können (vgl. [vmh 07]).

Mit dem Produkt *VMware Infrastructure 3* ist VMware im Moment der Marktführer bei Servervirtualisierung in Unternehmen (vgl. [Ahne 07]). Diese Virtualisierungsumgebung wird in Kapitel 6 bei der Umsetzung des Konzeptes eingesetzt. Daher erfolgt im nächsten Abschnitt eine detaillierte Beschreibung der Funktionsweise.

3.2.2 Die VMware Infrastructure 3 Umgebung im Detail

Wie bereits erwähnt, gibt es den *VMware Infrastructure 3* in drei Versionen. Im nachfolgenden Text wird immer auf die „Enterprise” Variante eingegangen, da diese alle Funktionen enthält, die für die anderen Versionen auch lizenziert werden können. Die Umgebung setzt sich aus dem ESX Server 3 (aktuell: 3.0.2) und dem Virtual Center 2 (aktuell: 2.0.2) zusammen. Beide Komponenten werden in den nächsten beiden Abschnitten vorgestellt.

Wichtige Eigenschaften von ESX Servern

Die eingesetzte Virtualisierungstechnik beim ESX Server ist die Hardwarevirtualisierung (siehe Abschnitt 3.1.2). Doch als Besonderheit läuft dieser als sogenannter „Bare Metal” Virtualisierer direkt auf der Hardware [Ahne 07]. Dies bedeutet, dass kein bereits installiertes Wirtsbetriebssystem vorhanden sein muss, sondern der ESX Server liefert seinen eigenen Kernel (*VMkernel* genannt) mit dem Virtual Maschine Monitor (siehe

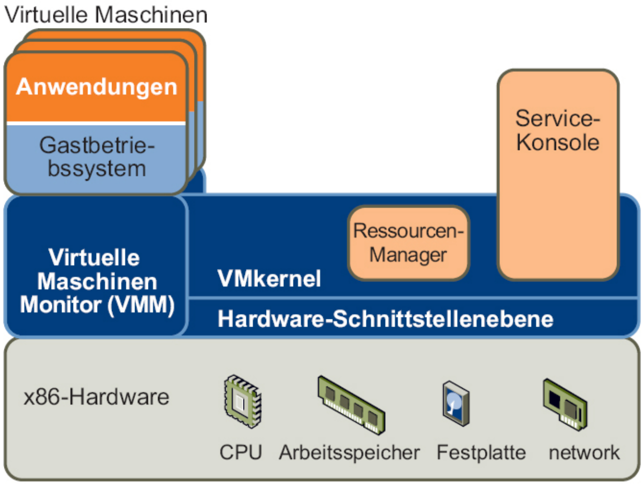

Abbildung 3.9: Architektur des VMware ESX Servers (Quelle: [vmh 07])

Abbildung 3.9). Dieser übernimmt die Ansteuerung und Virtualisierung der physischen Komponenten. Zur Virtualisierung der CPU und des Hauptspeichers verwendet VMware die sogenannte „Binary Translation" (BT) [vmh 07]. Diese funktioniert, wie in Abschnitt 3.1.2 beschrieben, durch Analyse des Codes, Abfangen von privilegierten Operationen und Nachbildung mit anderen Befehlsfolgen. VMware liefert dafür eigene Treiber, weshalb der ESX Server nur auf zertifizierten Systemen läuft (vgl. [AHN 07]). Aktuell werden über 180 Servermodelle von mehr als 17 Herstellern unterstützt [vmh 07]. All diese Systeme bieten wesentliche Funktionen, wie das Multipathing der Fibrechannel-HBAs (Host Bus Adapters), das Teaming der Netzwerkadapter oder die VLAN-Unterstützung der virtuellen Netzwerke [Ahne 07].
Der VMkernel mit seinem VMM arbeitet dabei im Hintergrund und ist nicht sichtbar. Als einzige Verbindung zum Kernel erscheint die Service Console unter der Kontrolle des VMkernel (siehe Abbildung 3.9). Diese ist eine privilegierte virtuelle Maschine auf Basis von Red Hat Linux mit Schnittstellen für die Steuerung des Kernels und der VMs [Ahne 07]. Neben einer Kommandozeile bietet die Service Console zusätzliche Dienste an, wie eine Firewall, den SSH Server oder den Verwaltungsagenten, der für das Virtual Center von Bedeutung ist (siehe nächster Abschnitt 3.2.2). Mit Hilfe des SSH Servers ist es möglich, sich im Netzwerk mittels SSH Protokoll mit der Konsole zu verbinden. Dadurch können alle Befehle zur Verwaltung der VMs mit der Service Console vorgenommen werden, wobei dies gute Linux Kenntnisse für die Kommandozeile voraussetzt. Zusätzlich gibt es, neben einer Webkonsole, für Windows PCs im Netzwerk eine grafische Oberfläche: der *Virtual Infrastructure Client*, kurz VI-Client (siehe Abbildung 3.10). Dieser bietet alle wichtigen Funktionen zum Erstellen und Verwalten von virtuellen Maschinen über die Auswahlmenüs. Zusätzlich gibt es noch Funktionen, wie das Leistungsverhalten von VMs überwachen oder die Kategorisierung der VMs zu sogenannten „Ressourcepools" (siehe die Kategorien „benchmarks", „produktiv" und „test" in Abbildung 3.10). In diesen Pools können Ressourcen wie CPU oder Hauptspeicher für die jeweilige Gruppe unter anderem auf Höchstwerte festgelegt werden, damit zum Beispiel eine Produktivumgebung immer Vorrang vor der Testumgebung hat, falls es bei den Ressourcen des Hosts zu Engpässen kommt (vgl. [Ahne 07]).
Weitere wichtige Eigenschaften des ESX Servers sind im Folgenden genannt: Es gibt auch hier die Multiprozessorunterstützung (VirtualSMP), doch können nicht nur zwei, sondern bis zu vier virtuelle CPUs an die VM durchgereicht werden. Die Grenze des Hauptspeichers liegt bei 16 GB pro VM, vorausgesetzt der Gast unterstützt dies auch. Wie auch *VMware Workstation* beherrscht der ESX Server mehrere Snapshots zur Sicherung mehrerer Systemzustände einer VM. Des Weiteren können virtuelle Platten zu einem laufenden Gast hinzugefügt werden und es ist möglich, CD-Laufwerke oder ISO Images in eine VM durchzureichen (vgl. [Ahne 07]).
Wie bei allen Produkten von VMware besteht eine virtuelle Maschine aus einer oder mehreren virtuellen Platte(n) und der dazugehörigen Konfigurationsdatei. Eine virtuelle Platte ist eine einzige Containerdatei mit der Endung *.vmx*. In diesem Container organisiert VMware das Gastsystem mit den dazugehörigen Daten. Die Dateigröße des Containers entspricht der festgelegten Größe der virtuellen Platte. Daher „wächst" oder „schrumpft" der Container nicht dynamisch, sondern belegt sofort den kompletten Platz (vgl. [vmh 07]). In

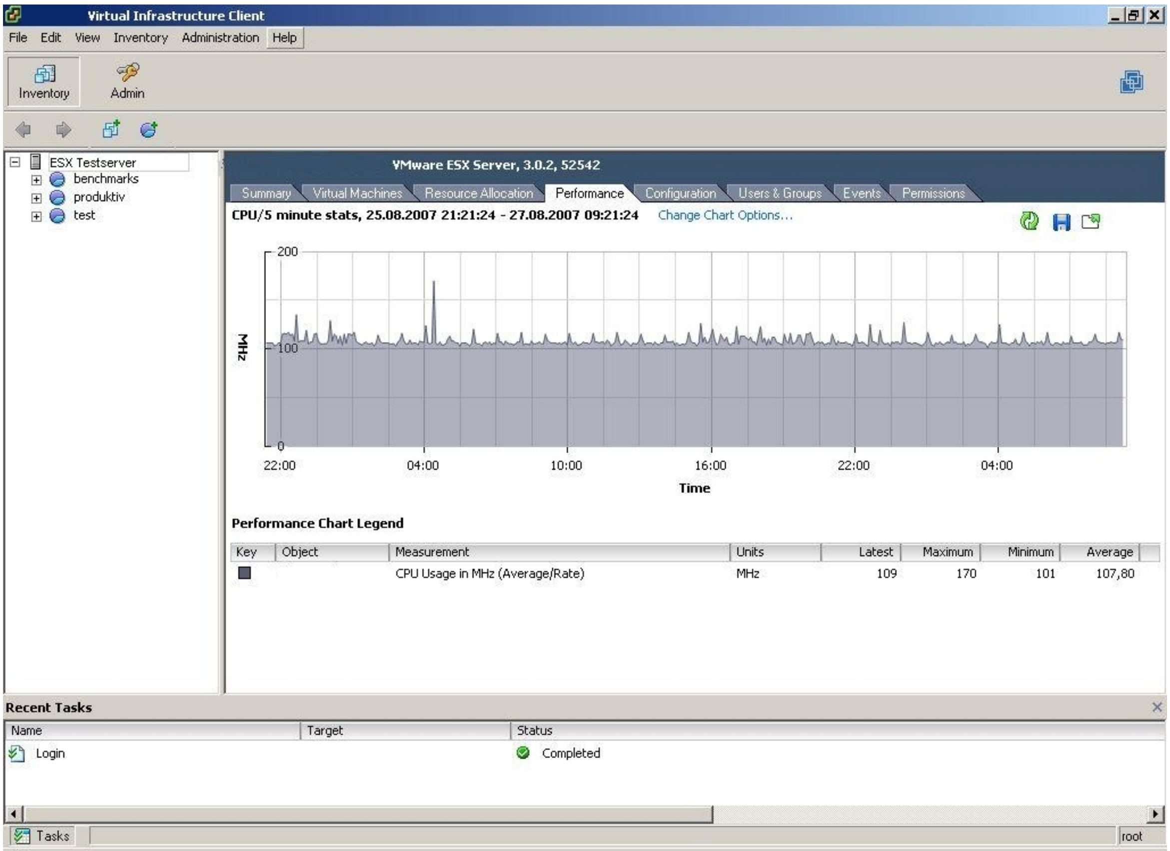

Abbildung 3.10: Screenshot des VI Client zur Verwaltung eines ESX Servers

der Konfigurationsdatei sind, wie der Name schon sagt, alle wichtigen Einstellungen für die VMware enthalten. Darunter fällt z.B. die virtuelle Bootplatte.
Bisher gab es noch keine Informationen, auf welchem Datenspeicher die virtuellen Platten abgelegt werden. So können diese lokal auf dem Server gespeichert werden, doch auch externe Möglichkeiten sind vorhanden. Dies ist auch für einige Funktionen von großer Bedeutung und der ESX Server bietet daher unterschiedliche Möglichkeiten an. Um welche es sich dabei handelt und was die Vor- und Nachteile sind, wird im nächsten Abschnitt geklärt.

Der Datastore und die Möglichkeiten der Anbindung

Neben den beschriebenen Komponenten *VMkernel*, der Service Console und deren umfangreichen Möglichkeiten, liefert der ESX Server auch sein eigenes clusterfähiges Dateisystem, genannt VMFS (Virtual Machine File System), mit. VMFS kann nur auf Datenträgern an SCSI- beziehungsweise RAID-Controllern (die VMware unterstützt) oder auf Logical Units (LUNs) im Storage Area Network (SAN) arbeiten [Ahne 07], aber eine Installation des ESX Servers ist auch auf IDE Platten möglich. In diesen VMFS Partitionen existiert für jede VM ein Ordner, in dem die virtuellen Platten und die Konfigurationsdaten gelagert sind. Dieses Dateisystem erlaubt es, dass mehrere ESX Server gleichzeitig auf denselben Datenspeicher zugreifen können (siehe Abbildung 3.11). So kann ein Administrator eine VM herunterfahren und sofort auf einem anderen Host neu starten, ohne dass die VM erst in eine andere Partition kopiert werden muss. Damit keine VM von zwei Hosts gleichzeitig startet, legt der ESX Server Logdateien für aktive virtuelle Platten an [Ahne 07]. Dieses Verfahren wäre zum Beispiel mit einer NTFS formatierten Datenspeicher nicht möglich, da immer nur ein Server auf die gleiche NTFS Partition zugreifen kann (vgl. [vmh 07]).
Die zweite Möglichkeit ist die Verwendung des NFS (Network File System). Dabei handelt es sich um ein von SUN entwickeltes UNIX Protokoll, das den Zugriff auf Dateien über ein Netzwerk (auf Basis von TCP/IP) ermöglicht (vgl. [Soll 02]). Der ESX Server kann mit diesem Protokoll designierte NAS (Network Attached

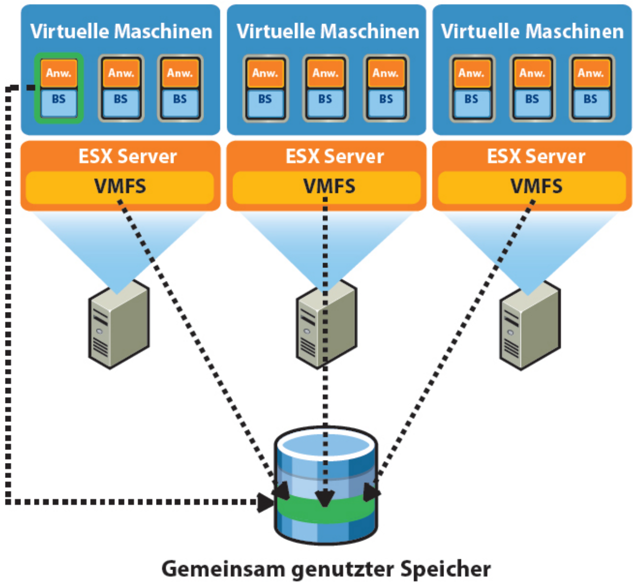

Abbildung 3.11: Mehrfacher Zugriff der ESX Server auf einen gemeinsamen Datenspeicher (Quelle: [vmh 07])

Storage) Datenträger auf einem NAS-Server verwenden (vgl. [vmh 07]). Dieser bindet mittels NFS Protokoll die NAS-Datenträger ein und erstellt für jede virtuelle Maschine ein Verzeichnis. Die virtuellen Platten liegen im Dateisystem des NAS-Datenträger, deshalb kommt dort kein VMFS zum Einsatz (vgl. [Ahne 07]). Der ESX Server unterstützt nur NFS Version 3.

Wenn eine virtuelle Maschine mit den virtuellen Platten kommuniziert, die auf einem Datenspeicher gespeichert sind, geschieht dies über SCSI-Befehle. Da sich die Datenspeicher aber auf verschiedenen Typen von physikalischen Geräten befinden können, werden diese Befehle je nach Protokoll umgewandelt. Um welches Protokoll es sich dabei handelt, hängt von der Anbindung des ESX Server-Systems an ein Speichergerät ab. Der ESX Server unterstützt die Protokolle Fibre Channel (FC), Internet SCSI (iSCSI) und NFS. Die zentrale Anbindung des Datenspeichers (eine LUN im SAN für alle ESX Server) ist eine notwendige Voraussetzung, um die wichtigen Funktionen für Livemigration, Lastverteilung und Hochverfügbarkeit zu nutzen. Diese Funktionen sind aber nur in Verbindung mit dem *VMware Virtual Center* möglich und werden daher erst in Abschnitt 3.2.2 beschrieben.
Bei den folgenden Techniken wird die Anbindung mittels NFS nicht besprochen, da auf diesen Datenträger kein VMFS installiert ist. Dadurch können nicht alle Funktionen des Virtual Centers verwendet werden (vgl. [vmh 07]). Daher werden im Folgenden nur die beiden Anbindungsmöglichkeiten „Fibre Channel" und „iSCSI" vorgestellt.

Anbindung mit Fibre Channel SAN Zuerst muss der Begriff SAN (Storage Area Network) definiert werden: Unter dem Begriff versteht sich ein Netzwerk, in dem angeschlossene Server auf verbundene Speichersubsysteme zugreifen können (vgl. [Soll 02]). So ist es prinzipiell möglich, dass alle Server, die in ein SAN integriert sind, auf alle Speichersysteme zugreifen können. Bei den Zugriffen handelt es sich um blockbasierte Datenzugriffe auf Geräte, die über den SCSI (Small Computer System Interface) Bus miteinander kommunizieren. Der Zugriff erfolgt über das SCSI Protokoll, auf das hier nicht näher eingegangen wird. In einem SAN können mittels LUNs (Logical Unit Number) Speichersubsysteme adressiert werden, ohne jeweils die einzelnen Platten über SCSI, die sich hinter dem Speichersystem befinden, direkt anzusprechen.
In einem SAN entstehen hohe Datenmengen zwischen den Servern und den Speichersystemen, für die ein schnelles Transportprotokoll benötigt wird (vgl. [TrEr 03]). Seit den frühen 90er Jahren hat sich Fibre Channel (FC) immer mehr und mehr durchgesetzt und ist mittlerweile bei der Realisierung von schnellen Speichernetzen kaum wegzudenken (vgl. [TrEr 03]). Aus diesem Grund werden die Begriffe „SAN" und „Fibre Channel"

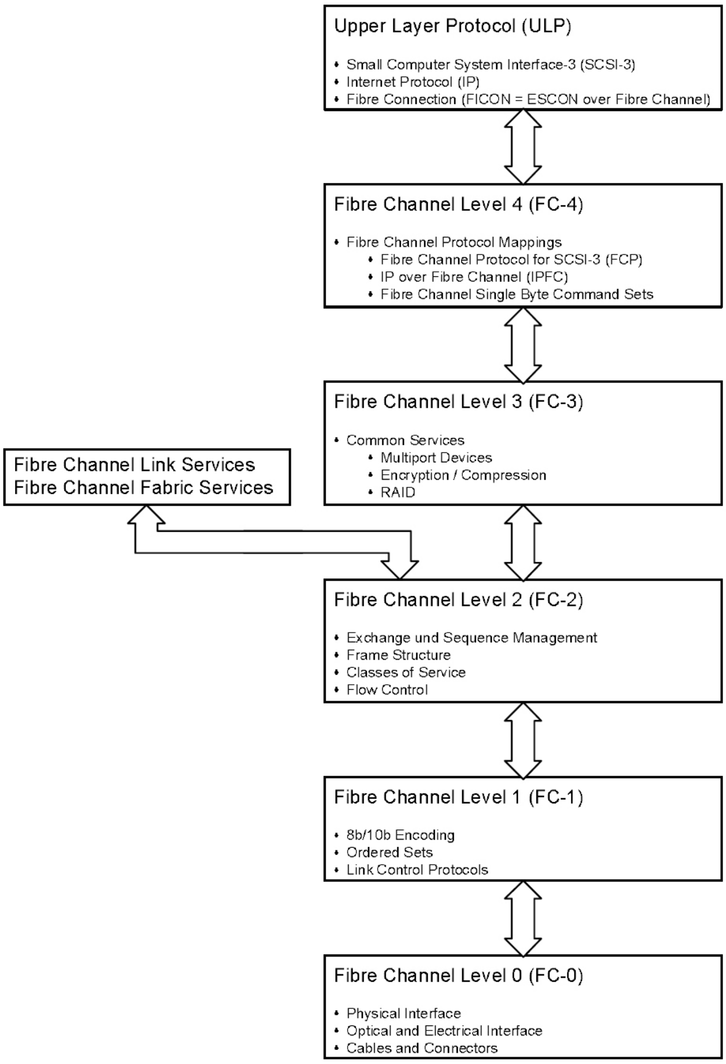

Abbildung 3.12: Der Fibre Channel Protokollturm (Quelle: [TrEr 03])

oft synonym verwendet, aber es sei nochmal darauf hingewiesen, dass es sich bei Fibre Channel um die Übertragungstechnik handelt, mit der ein SAN realisiert wird. Eine andere Technik wäre beispielsweise iSCSI, das im nächsten Punkt behandelt wird. Der Standard der Technologie ist unter [fcs 07] definiert.
Der Fibre Channel Protokollturm untergliedert sich in fünf Schichten (siehe Abbildung 3.12): Die unteren vier Schichten, FC-0 bis FC-3, definieren die grundlegenden Kommunikationstechniken, also die physikalische Ebene, die Übertragung und die Adressierung [TrEr 03]. Die obere Schicht, FC-4, definiert, wie Anwendungsprotokolle (Upper Layer Protocols, ULP) auf das zugrunde liegende Fibre Channel Netz abgebildet werden. Durch den Einsatz von verschiedenen ULPs wird beispielsweise entschieden, ob ein reales Fibre Channel Netz als IP Netz, als Fibre Channel SAN oder für beides eingesetzt wird (vgl. [TrEr 03]). Mit Hilfe der „Link Services" und der „Fabric Services" wird ein Fibre Channel Netz verwaltet und betrieben. Der Fibre Channel Standard definiert drei verschiedene Topologien: Fabric, Arbitrated Loop und Point-to-Point (siehe Abbildung 3.13). Bei Point-to-Point gibt es eine bidirektionale Verbindung zwischen zwei Endgeräten. Arbitrated Loop definiert einen unidirektionalen Ring, in dem immer nur zwei Geräte gleichzeitig mit voller Bandbreite Daten austauschen können. Ein Fabric definiert ein Netzwerk, in dem mehrere Geräte über den Fibre Channel Switch gleichzeitig mit voller Bandbreite Daten austauschen können. Es können auch mehrere FC Switches miteinander verbunden werden, um ein Fabric mit einem anderen zu verbinden (vgl. [TrEr 03]). Zusätzlich ist

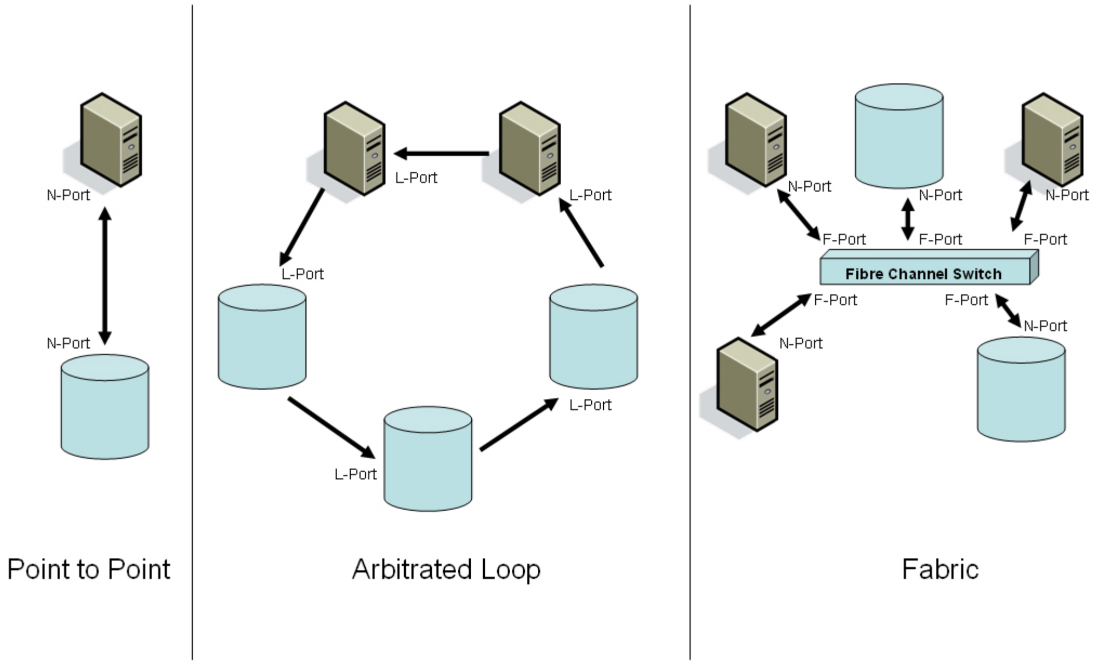

Abbildung 3.13: Die drei definierten Topologien bei FC und deren Porttypen (Quelle: In Anlehnung an: [TrEr 03])

es möglich, ein oder mehrere Arbitrated Loops an ein Fabric anzuschließen. Die Fabric Topologie ist die am häufigsten eingesetzte in Unternehmen [Soll 02].
In allen Topologien müssen die Geräte (Server, Speichergeräte und Switches) über einen oder mehrere Fibre Channel Ports verfügen. In Servern wird der Port über sogenannte Hostbus Adapter (HBAs), z.B. mittels eingebauten PCI Karten, realisiert. Ein Port besteht immer aus zwei Kanälen, einem Eingangs- und einem Ausgangskanal [TrEr 03]. Die Verbindung zwischen zwei Ports nennt sich „Link", wobei bei Point-to-Point und Fabric dieser bidirektional ist und bei Arbitrated Loop unidirektional (siehe Pfeile in Abbildung 3.13). Die Topologien Arbitrated Loop und Fabric werden durch verschiedene, zueinander inkompatible Protokolle realisiert. Dabei gibt es verschiedene Porttypen (siehe Abbildung 3.13) mit unterschiedlichen Fähigkeiten. Ein N-Port (N=Node) beschreibt die Fähigkeit eines Ports, als Endgerät (Server, Speichergerät), auch Knoten genannt, in der Fabric Topologie oder als Partner in der Point-to-Point Topologie teilzunehmen [TrEr 03]. Der F-Port (F=Fabric) ist im FC Switch das Gegenstück zum N-Port. Der F-Port weiß, wie er die Daten, die ein N-Port an ihn sendet, durch das Fibre Channel Netz an das gewünschte Endgerät weiterleiten kann. Wie bereits erwähnt, verwendet Arbitrated Loop andere Protokolle zum Datenaustausch. Ein L-Port (L=Loop) beschreibt die Fähigkeit eines Ports, als Endgerät (Server, Speichergerät) in der Arbitrated Loop Technologie teilzunehmen. Neuere Geräte sind nicht mehr mit L-Ports sondern mit NL-Ports (NL=Node-Loop) ausgestattet, der sowohl die Fähigkeiten eines N-Ports, wie eines L-Ports hat. Zusätzlich gibt es noch weitere Porttypen, wie den E-Port (E=Expansion), der zwei FC Switches miteinander verbindet (vgl. [Soll 02]).
Dies gibt nur einen kleinen Überblick über die SAN und Fibre Channel Technologie, die zur Verbindung eines zentralen Datastores mit mehreren ESX Servern verwendet werden kann. Die Vorteile eines zentralen Speichers in Kombination mit VMFS sind der mehrfache Zugriff auf den Datenspeicher und die Zeitersparnis, da kein Kopieren von einem Datenspeicher auf den anderen notwendig ist. Die beschriebene Topologie zeigt aber auch, dass hier eine komplette Hardwarestruktur benötigt wird. So braucht jedes angeschlossene Gerät eine Hostbus Adapterkarte, die mittels Glasfaser- oder Kupferkabel mit einem FC Switch (bei einem Fabric) verbunden werden müssen. Diese Technologie beinhaltet einen Mehraufwand an Kosten, die sich aber durch hohe Datengeschwindigkeiten auf weite Entfernungen, geringe Übetragungsfehlerraten und geringe Latenzzeiten auszeichnet. Ein großes Problem von Fibre Channel SAN ist die Interoperabilität. Wünschenswert ist die Verbindung von heterogener Hardware, beispielsweise unabhängig davon, welche HBA Karte im Server ent-

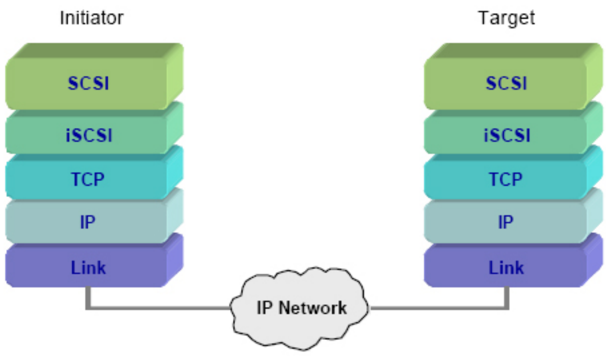

Abbildung 3.14: Der Protokollturm von iSCSI (Quelle: [iSC 07])

halten ist. Eine HBA Karte kann aber von mehreren Herstellern mit verschiedener Firmware ausgestattet sein, was zu Problemen bei der Verbindung führen kann (vgl. [TrEr 03]). Aus den Gründen der hohen Anschaffung und der möglichen Probleme der HBAs, hat sich in den letzten Jahren eine neue Technik entwickelt, die es ermöglicht SCSI-Daten in TCP/IP-Pakete zu verpacken und über IP-Netze zu transportieren (vgl. [TrEr 03]). Eine genaue Erklärung und welche Vor- und Nachteile diese Technologie bringt, wird im nächsten Abschnitt gegeben.

kostengünstigere Alternative: iSCSI Bei iSCSI (Internet SCSI) handelt es sich um ein von der Storage Networking Industry Association (SNIA) standardisiertes Protokoll, dass es ermöglicht das SCSI Protokoll über ein Netzwerk zu übertragen (vgl. [iSC 07]). Damit können Storage-Systeme über TCP/IP an einen Server angeschlossen werden. Durch die Verwendung des TCP/IP Protokoll kann die Kommunikation über die vorhandene Ethernetverkabelung, die üblichen Netzwerkkarten und Switches laufen(vgl. [AHN 07]). Um die Übertragung zu ermöglichen, tunnelt iSCSI die SCSI Befehle über die TCP Schicht (siehe Abbildung 3.14). Dabei werden die SCSI Daten aufbereitet und an die untere Schicht (TCP) weitergegeben (vgl. [iSC 07]). Die Abbildung des Protokollstapel erfolgt auf der einen Seite im *Initiator* und auf der anderen Seite im *Target* (siehe Abbildung 3.14). Ein *Initiator* ist meist eine Hardwarekomponente, nämlich der HBA. Dieser verfügt über einen eigenen Prozessor, der das gesamte Protokollhandling übernimmt (vgl. [AHN 07]). Als weitere Möglichkeit gibt es auch einen *Software-Initiator*. Dieser wird als Treiber im Betriebssystem eines Clients installiert und verwendet eine verfügbare Netzwerkkarte, um darüber mit dem Ziel, dem *iSCSI Target*, zu kommunizieren. Softwarelösungen gibt es sowohl für Windows, als auch für viele Linux Distributionen [AHN 07]. Bei einem *iSCSI Target* handelt es sich um den Ort, an dem die Daten liegen, auf die alle angebundenen Rechner zugreifen wollen. Dieses *Target* kann beispielsweise ein dediziertes SAN mit iSCSI Schnittstelle sein [AHN 07]. Diese HBA Schnittstelle kann wie beim *Initiator* durch eine Softwarelösung ersetzt werden. Dabei läuft die Software als Anwendung und gibt einen Teil der Plattenkapazität des Servers als LUN im Netzwerk frei. Auf diese LUN kann dann beispielsweise der ESX Server zugreifen, ohne dass er Kenntnisse über die dahinter liegende Technik hat oder benötigt.
Die Vorteile von iSCSI sind vor allem der kostengünstigere Einsatz, da teilweise vorhandene Netzkomponenten verwendet werden können. Zusätzlich können durch einen Softwareinsatz von *Target* und *Initiator* weitere Kosten eingespart werden. Für ein gutes Leistungsverhalten muss aber ein abgetrenntes Netz eingesetzt werden, also eigene Netzwerk-/iSCSI-Karten, einen getrennten Switch und eigene Verkabelung (vgl. [ZIM 06]). Dabei wird mit der Verwendung von TCP/IP ein Verfahren verwendet, das (fast) überall vorhanden ist und eine Anbindung zwischen weit entfernten Geräten ermöglicht. Hier liegt aber auch ein Problem von iSCSI, denn das Ethernet ist nicht für große Datenmengen ausgelegt, wie das bei Fibre Channel der Fall ist. So kann im 1 GBit Ethernet, die Datenrate deutlich unter der vom 1 GBit FC sein. Dennoch ist die Datenrate für die meisten Anwendungen im Virtualisierungsbereich ausreichend (vgl. [AHN 07]). Mit der Entwicklung von 10 GBit Ethernet wird aber iSCSI in Zukunft interessanter werden, denn dann können ausreichende Datenraten erreicht werden. Aus diesen Gründen bietet VMware bei seinen ESX Servern auch diese Möglichkeit der Verbindung zum Datenspeicher an, da dies in Zukunft eine echte Alternative zu Fibre Channel sein kann (vgl. [ZIM 06]).

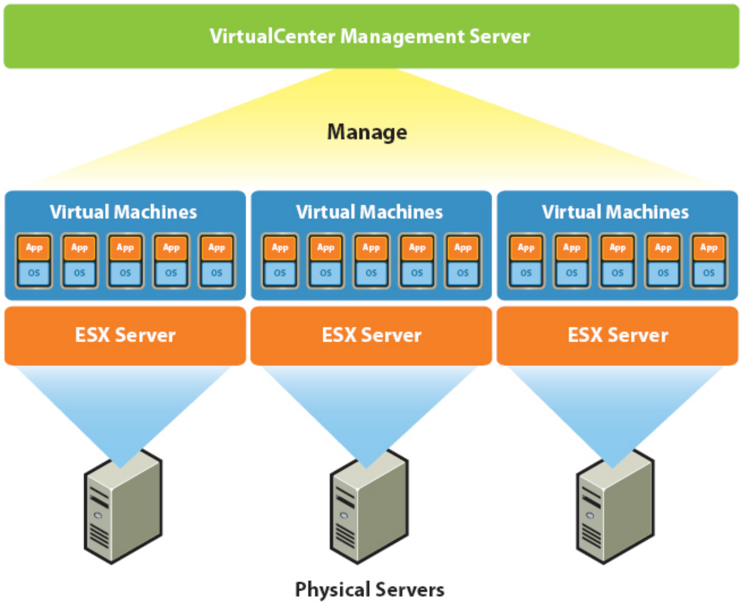

Abbildung 3.15: Zentrale Steuerung der ESX Server mit *VMware Virtual Center* (Quelle: [vmh 07])

Nach der Vorstellung von Fibre Channel und iSCSI wurden alle wichtigen Komponenten und Eigenschaften des ESX Servers vorgestellt. Abschließend sei nochmal darauf hingewiesen, dass es sich bei einer zentralen Speicherung um einen klassischen „Single Point of Failure” handelt. Um hier (Hoch-)Verfügbarkeit zu schaffen, müssen geeignete Redundanz- und Backupstrategien verwendet werden. VMware bietet hier eine gewisse Unterstützung, um die Sicherung von virtuellen Maschinen zu erleichtern. Diese erweitert aber bereits vorhandene Backuplösungen und bringt keine eigenständige Software mit. Dieses Problem wird in der Anforderungsanalyse nochmal genauer beleuchtet.
Welche Möglichkeiten sich durch die zentrale Speicherung für die ESX Server ergeben, zeigt der nächste Punkt. Im Zusammenhang mit dem *Virtual Center* bietet VMware einige Möglichkeiten an, die nur in Kombination mit der FC SAN/iSCSI Technologie möglich sind (vgl. [vmh 07]).

VMware Virtual Center im Überblick

Mit dem VI Client lassen sich, wie zuvor beschrieben, die ESX Server jeweils einzeln betreuen und verwalten. Mit dem *VMware Virtual Center* (VC) kommt eine Komponente dazu, die es erlaubt alle ESX Server unter einem Managementserver zu verwalten (siehe Abbildung 3.15). Dazu muss ein VC Server auf Basis von Windows 2003 Server installiert werden. Zusätzlich wird eine Datenbankverbindung (zu Microsoft SQL Server 2000 oder Oracle 9iR2) für die Verwaltung benötigt (vgl. [Ahne 07]). Dieser VC Server kommuniziert mit den VC Agenten, die in den ESX Servern integriert sind. Nach der Einrichtung können alle ESX Server mit dem VI Client kontrolliert werden. Dazu verbindet sich der Client nicht mehr direkt mit einem ESX Server (was weiterhin möglich ist), sondern mit dem VC Server. Mit Hilfe des VC lassen sich die Maschinen besser verwalten, falls aber der VC Server ausfallen sollte, können weiterhin die Hosts einzeln angesteuert werden, ohne dass eine virtuelle Maschine vom Ausfall betroffen ist. Die Virtual Center Oberfläche (siehe Abbildung 3.10 auf Seite 25) ähnelt der Oberfläche für einen einzelnen ESX Server, bietet aber nun weitere Funktionen. Virtual Center integriert alle Hosts in ein sogenanntes Datacenter [Ahne 07]. In einem Datacenter können auch wieder Ressource Pools angelegt werden, wobei diesmal Gruppen von VMs definiert werden können, unabhängig auf welchem Server sie laufen. Des Weiteren kommen hier die Funktionen für Livemigration, Lastverteilung und Hochverfügbarkeit zum Einsatz. Diese sind nur bei mehreren Hosts in Verbindung mit Virtual Center möglich. Außerdem muss eine zentrale Speicherung der virtuellen Maschinen vorliegen (genaueres siehe vorheriger Abschnitt).

Die Migration von einem laufenden Gast von einem Host auf einen anderen, wird hier *VMotion* genannt. Die Funktion erzeugt eine Art Snapshot vom Hauptspeicher des Gastes und kopiert dann den RAM Inhalt auf den Zielhost. Der Gast bleibt während dieser Zeit aktiv, Hauptspeicherzugriffe protokolliert der VMM in einer Bitmap [vmh 07]. Nach der Übertragung, die vor der endgültigen Migration möglichst viele Speicherseiten auf den Zielhost kopiert, „friert” *VMotion* den Gast ein, überträgt die übrigen geänderten Speicherseiten mitsamt der ausgelesenen Prozessorregistern und „taut” den Gast auf dem Zielhost wieder auf (vgl. [Ahne 07]). Diese Unterbrechung ist nur ein kurzer Moment, da durch die zentrale Lagerung der virtuellen Platten kein Kopieren notwendig ist. Um *VMotion* einzusetzen, müssen aber die beiden Hosts die gleiche Porzessorarchitektur verwenden, denn nur so können die Prozessorregister ausgelesen und 1:1 kopiert werden. Ist diese Voraussetzung vorhanden, kann *VMotion* für jede VM eingesetzt werden, um sie auf einen beliebigen Host (wenn dieser auf den gleichen Datenspeicher zugreift) zu verschieben. Dies kann zum Beispiel bei einem Ressourcenengpass notwendig sein oder wenn für Wartungsarbeiten, der Host heruntergefahren werden muss. Das System der VM muss nicht extra heruntergefahren werden, sondern kann im Livebetrieb verschoben werden.
Auf Basis dieser Technik arbeitet auch die Lastverteilung bei VMware, das Distributed Ressource Scheduling (DRS) genannt wird. DRS bietet für die bereits beschriebenen Einsatzmöglichkeiten von *VMotion* einige Einstellungsmöglichkeiten, um die Vorgänge zu automatisieren. So können VMs bei definierten CPU oder RAM Schwellenwerten auf einen anderen freien Host verschoben werden. Dies kann beim Starten der VM, als auch im laufenden Betrieb geschehen. DRS kann dies selbst vornehmen oder dem Administrator eine Empfehlung per Email schicken, der dann entscheidet, wie weiter vorzugehen ist (vgl. [Ahne 07]). Die VMs können auch priorisiert werden, so dass bestimmte Maschinen immer zuerst oder auch zuletzt verschoben werden, je nach gewünschter Einstellung. Auch Wartungsarbeiten werden erleichtert, denn so werden durch den Aufruf des sogenannten „Maintenance Modus” alle VMs auf andere Hosts verschoben, ohne dass dies für jede einzelne Maschine manuell vorgenommen werden muss. Dieser Host erscheint in diesem Modus für die restlichen ESX Server als nicht aktiv, damit keine VMs auf den Host verschoben werden können. Auf Grund von DRS wird vom einzelnen Host abstrahiert, denn es ist nicht mehr wichtig, auf welchem Host eine virtuelle Maschine läuft, sondern dass eine gleichmäßige Lastverteilung vorliegt, unabhängig wo die VM ursprünglich erstellt wurde. Dies gilt aber nur, wenn so ein „Hostpool” gewünscht und entsprechend konfiguriert ist.
Neben DRS gibt es noch eine weitere Funktion, die auf Basis von *VMotion* arbeitet. Diese nennt sich schlicht *High Availability* (HA) und bietet eine Ausfallsicherung für die Hostmaschinen an. Alle ESX Server in einem HA Cluster sind miteinander (z.B. über den FC Switch) verbunden und schicken sich alle zehn Sekunden ein „Lebenszeichen”, einen sogenannten „Heartbeat” (vgl. [vmh 07]). Durch den gemeinsamen Datenspeicher weiß jeder Host, welche virtuelle Maschine auf welchem Host läuft. Fällt nun ein Host aus, erhalten die restlichen Server kein Lebenszeichen mehr. Nach einer kurzen Wartezeit (es werden gewisse Latenzzeiten beim Taktsignal gegeben) startet nun HA in Kombination mit DRS die virtuellen Maschinen mit Hilfe von *VMotion* auf den übrigen Rechnern. Auch hier können die virtuellen Maschinen priorisiert werden, um wichtige VMs zuerst auf den anderen Hosts zu starten. Dies könnte zum Beispiel der Virtual Center Server sein, der auch als VM installiert ist (vgl. [Ahne 07]). Während eines Hostausfalls kommt es zu einer kurzen Downtime der virtuellen Maschinen, denn erst, wenn der nicht zu erreichende Host bemerkt wird und die VM auf einem anderen Host wieder gestartet wird, ist diese auch wieder erreichbar. Zu beachten ist, dass HA Hosts überwacht, virtuelle Maschinen aber nicht. Gibt es einen Ausfall in einer VM, kann und wird das nicht durch HA abgedeckt. Hier muss beispielsweise eine geeignete Cluster Software auf den Gästen installiert werden, die eine hohe Verfügbarkeit für die Gäste gewährleistet (vgl. [AHN 07]).
Neben den Funktionen *VMotion*, DRS und HA bietet das Virtual Center noch weitere nützliche Möglichkeiten, wie konfigurierbare Alarmmeldungen, rollenbasierte Rechteverwaltung und das automatisierte Klonen neuer VMs über zuvor angelegte Templates (vgl. [Ahne 07]). Virtual Center konfektioniert geklonte Windows Gäste automatisch mittels Sysprep[7] und versieht sie mit IP Adressen [AHN 07].

Nachdem nun die wichtigsten Funktionen und Möglichkeiten der *Virtual Infrastructure 3* Umgebung vorgestellt wurde, ist diese komplett. Zusätzlich bietet VMware aber noch weitere Programme an, die in Kombination sehr sinnvoll sind. Im nächsten Schritt wird daher das Programm *VMware Converter* vorgestellt, der es unter anderem ermöglicht, physikalische Maschinen zu virtualisieren.

[7] Bei Sysprep handelt es sich um ein Tool von Microsoft, mit dem geklonte Maschinen angepasst werden. So erhält die geklonte Maschine beispielsweise eine neue SID (Security Identifier) und es führt eine erneute Hardwarererkennung aus (vgl. [sys 01]).

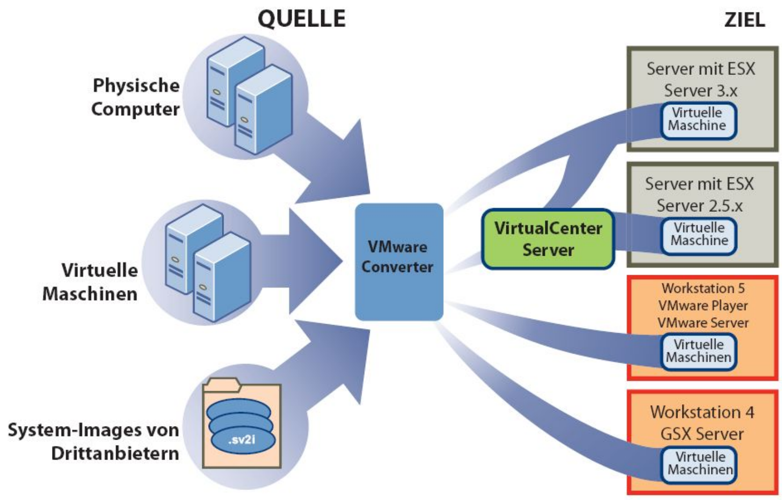

Abbildung 3.16: Die Einsatzmöglichkeiten des *VMware Converter 3.0* (Quelle: [vmh 07])

Konvertierung physikalischer Maschinen

Eines der Ziele von Virtualisierung ist die Konsolidierung der Server, um vorhandene physikalische Server als VMs in einer virtuellen Umgebung laufen zu lassen. Dazu muss entweder eine VM neu angelegt werden, in der dann das gewünschte Gastbetriebssystem installiert und konfiguriert wird oder mit Hilfe von Programmen kann ein bereits bestehender Server in eine VM migriert werden. Dies verursacht wesentlich weniger Aufwand, als eine VM neu zu installieren und einzurichten. Handelt es sich um alte Server, sind meist auch nicht mehr alle Treiber und Programme vorhanden, um eine Neuinstallation zu bewerkstelligen. Aus diesen Gründen bietet VMware ein Programm an, das eine Migration von einem physikalischen zu einem virtuellen Server (P2V - physical to virtual) vornimmt. Der *VMware Converter 3.0* ist in der „Starter Edition" frei verfügbar oder kann als „Enterprise Edition" lizensiert werden und löst den Vorgänger *P2V Assistant* ab. Die „Enterprise Edition" bietet gegenüber der freien Version die Möglichkeit, mehrere Migrationen gleichzeitig vorzunehmen und es kann auch eine Migration mittels Boot CD vorgenommen werden (vgl. [vmh 07]). Die Installation des Konverters erfolgt auf einem gängigen Windowssystem und benötigt keine zusätzlichen Programme oder Einstellungen. In Abbildung 3.16 sind die Quellen und Ziele dargestellt. So kann sowohl ein physikalischer Server, virtuelle Maschinen als auch Systemabbildungen von Drittanbietern importiert werden. Bei den physikalischen Servern werden nur bestimmte Windowssysteme (Windows NT4, Windows XP (32/64-Bit), Windows 2000/2003 (32/64-Bit) Server) unterstützt. Virtuelle Maschinen können aus den meisten aktuelleren VMware Produkten importiert werden. Ausnahme bilden erstellte Maschinen mit *VMware Fusion* (vgl. [vmh 07]). Zusätzlich ist eine Importierung von VMs aus *Virtual PC 7*, allen *Virtual Servern* Versionen, Festplattenimages von *Symantec Backup Exec System Recovery* und *Norton Ghost 9* möglich. Als Ziel kann sowohl ein ESX Server in der Version 2.5.x (nur über Virtual Center) oder 3.x (direkt oder über ein Virtual Center) verwendet werden, als auch andere VMware Versionen (siehe Abbildung 3.16). Bei der Konvertierung können die Gastsysteme für die virtuelle Maschine angepasst werden, wie zum Beispiel vorhandene Festplatten nach Wunsch anzupassen. Auch Sysprep wird unterstützt, um eine weitere Konfiguration des Gastes vorzunehmen (vgl. [Ahne 07]). Wie die Abbildung 3.16 zeigt, können so auch vorhandene VMs für den *VMware Player* konvertiert werden, wenn beispielsweise eine VM für mehrere Schulungsrechner zur Verfügung stehen soll.
Zu den Nachteilen gehört, dass VMware den Konverter derzeit nur auf Windows-Umgebungen beschränkt. Daher ist kein Import von Linux oder Solaris möglich. Außerdem werden die Grafiktreiber nach der Importierung nicht immer richtig erkannt und die VM läuft nur in der Standard VGA Auflösung (vgl. [AHN 07]). Dies ist aber ein Problem, das im Serverbereich vernachlässigbar ist. Mit der Installation der VMware Tools im Gast werden diese Probleme meist beseitigt (vgl. [AHN 07]).
Insgesamt bietet der Konverter eine nützliche Erweiterung für das VMware Umfeld. Dennoch ist ein wichtiger Punkt bisher nicht berücksichtigt worden. So ist bisher das Problem der Datensicherung nur angedeutet, aber noch nicht vertieft worden. Grundsätzlich kann die bisher verwendete Backupsoftware auch für die Gäste

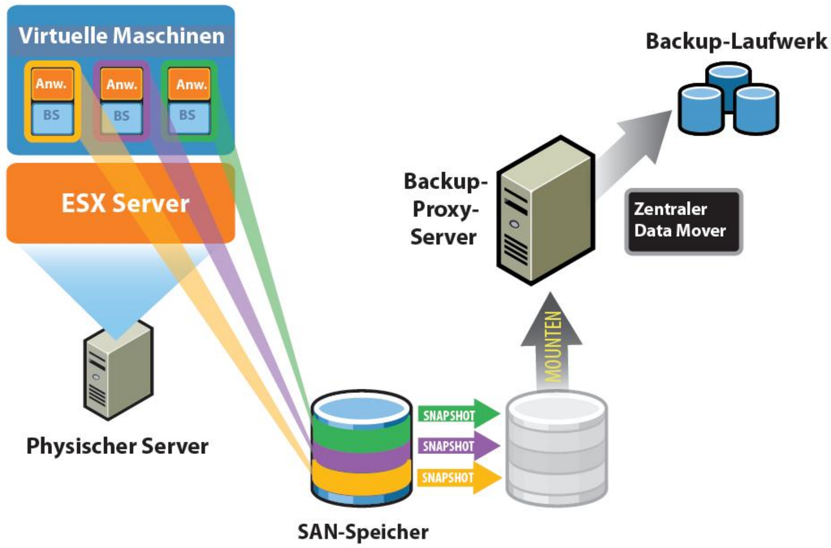

Abbildung 3.17: Die Funktionsweise von *VMware Consolidated Backup* (Quelle: [vmh 07])

genutzt werden. Über die eingerichteten Backup Agenten auf den VMs kann eine Sicherung übers Netzwerk vorgenommen werden (vgl. [Ahne 07]). Dieser Vorgang kostet Systemressourcen, da die Sicherung im Gastbetriebssystem läuft. VMware bietet hier eine Erweiterung, um die Datensicherung zu erleichtern und nicht im Gast auszuführen.

Datensicherung der VMs mit VMware Consolidated Backup

Wie bereits beschrieben sitzt sich eine VM aus einer oder mehreren virtuellen Platten zusammen, wobei die Platte jeweils aus einer Containerdatei besteht. Dadurch ist eine Datensicherung einer virtuellen Maschine einfach zu bewerkstelligen, da es ausreicht diese Containerdatei und die entsprechende Konfigurationsdatei der virtuellen Maschine zu sichern. Bei einem Ausfall oder Verlust der VM, können die entsprechenden virtuellen Platten zurückkopiert werden und die virtuelle Maschine kann auf einem ESX Host oder über das Virtual Center wieder gestartet werden. Diese Art der Sicherung kann mit den bereits verwendeten Backuplösungen verwendet werden. Hier gilt es zu beachten, dass die virtuelle Maschine ausgeschaltet werden muss (Cold Backup) und deshalb während der Backupzeit nicht zur Verfügung steht (vgl. [Ahne 07]). Zusätzlich gibt es die Möglichkeit des Hot Backups, bei dem der Administrator einen Snapshot der VM erzeugt (vgl. [Ahne 07]). Während des Erstellens greifen alle Schreiboperationen auf sogenannte Redo Logs zu, so dass beim Kopieren der virtuellen Platte die Konsistenz bewahrt bleibt. Ein ESX Server beherrscht das spätere Verschmelzen des aufgelaufenen Redo Logs mit der virtuellen Platte im laufenden Betrieb, sobald die Sicherung beendet ist. Für diese Technik gibt es einige Produkte von Fremdherstellern, die diese Datensicherung automatisieren (vgl. [Ahne 07]). Bei beiden Methoden erfolgt die Sicherung über das Netzwerk, was zu einer hohen Belastung führen kann. Daher sollte eine Sicherung zu bestimmten Zeiten (z.B. Nachts) durchgeführt werden, damit die Netzwerkkapazität für andere Anwendungen und Server nicht zu stark eingeschränkt wird. Mit dem Programm von VMware, namens *VMware Consolidated Backup* (VCB) in der Version 1.0.3 werden die Daten über das SAN (Fibre Channel und seit Version 1.0.3 auch iSCSI) und nicht über das Netzwerk (LAN) gesichert. VCB besteht aus einem Set von Skripts und Werkzeugen, die den Zugriff auf die virtuellen Platten der VM über das SAN ermöglichen (vgl. [Ahne 07]). Für diese Aufgabe wird ein „Backup Proxy Server" benötigt, der mit Windows 2003 Server installiert werden muss. Dieser hat Zugriff auf die gleichen LUNs wie die ESX Server. Mit dem Skript zur Backupvorbereitung werden Snapshots der virtuellen Maschinen (im laufenden Betrieb) erstellt und direkt vom SAN zum Backup Proxy Server gemountet (siehe Abbildung 3.17). Dazu wird zuerst die VM in den Snapshot Modus geschaltet. Dies kann für jede beliebige Maschine vorgenommen werden, bei Windows Systemen mit NTFS wird das Dateisystem eingefroren (das sogenannte „Quiescing"), um anschließend

die komplette virtuelle Platte zu sichern (vgl. [Ahne 07]). Das notwendige Redo Log während des Sicherungsvorgangs wird vom Virtual Center initiiert und verwaltet (vgl. [Ahne 07]). Der eigentlichen Kopiervorgang wird entweder von einem selbsterstellten Kopierskript oder einer Backupsoftware vorgenommen. Einige Hersteller bieten Kompatibilitätsmodule für VCB an, um es in ihre Software einzubinden. Dadurch können die Skripte besser verwaltet und gestartet werden (z.B. Automatisierung der Skripte zu gewissen Zeiten). Nach der Sicherung werden die gemounteten Snapshots mit dem Skript zur Backup-Nachbearbeitung getrennt und der Snapshot Modus für die virtuellen Datenträger wird deaktiviert. Danach verschmilzt der Virtual Center das Redo Log mit der VM. Bei VCB gilt zu beachten, das für Datenbanken eigene Skripte verwendet werden müssen, da hier sonst nicht die Konsistenz gewährleistet werden kann (vgl. [AHN 07]).
Neben der kompletten Sicherung einer VM gibt es auch die Möglichkeit der (inkrementellen) Datei- oder Verzeichnissicherung, wenn ein Windowssystem vorliegt. VCB erkennt Volumes innerhalb der Snapshots virtueller Maschinen und mountet erkannte Volumes an vordefinierten Knotenpunkten auf dem Proxy Server (vgl. [vmh 07]). Jeder Knotenpunkt entspricht einem Laufwerksbuchstaben eines Volumes auf der virtuellen Maschine. Die Backup Software des Drittanbieters erkennt diese Volumes und erstellt ein Backup auf Dateiebene. Welche Dateien oder Verzeichnisse zu sichern sind, wird vorher in der Backup Software festgelegt. Dieses Verfahren kann aber zu Schwierigkeiten führen, da das System gemountete virtuelle Platten nur lesen und die Software deshalb anstelle des Archiv-Bits (Schreiben eins Bits, ob die Datei schon gesichert wurde) nur das Änderungsdatum verwenden kann [Ahne 07].
Die Wiederherstellung erfolgt entweder auf den Proxy Server oder direkt in die VM. Die Wiederherstellung auf den Proxy Server wird durch die Backupsoftware vorgenommen, der die Daten oder die virtuelle Maschine entsprechend dorthin kopiert. Die Daten können dann manuell auf den Datenspeicher oder in die VM (bei Datenwiederherstellung) kopiert werden. Im Virtual Center werden die VMs neu registriert und auf einem ESX Host gestartet. Soll eine Datensicherung direkt in eine VM vorgenommen werden, so muss ein entsprechender Agent installiert sein, der dann durch die Skripte die Daten wiederherstellen kann (vgl. [vmh 07]). Die Wiederherstellung läuft auf jedem Fall über das Netzwerk (LAN) und nicht mehr über das SAN (vgl. [Ahne 07]).
Insgesamt bietet *VMwares Consolidated Backup* eine interessante Erweiterung für die herkömmlichen Backupprogramme, da es durch die Verbindung über das SAN das Netzwerk nicht belastet und durch den Snapshot Modus virtuelle Maschinen im laufenden Betrieb sichern kann. Nachteil ist auch hier die fehlende Unterstützung für Linuxsysteme. So kann zwar jede Maschine gesichert werden, aber auf Dateiebene ist dies nur für einige Windowssysteme möglich. Da Linux ein anderes Dateisystem als NTFS benutzt, ist auch kein Sperren von diesem möglich, um eine garantierte Konsistenz zu erhalten. Zusätzlich muss bedacht werden, dass es sich nur um eine Erweiterung für einige, ausgewählte Backup Programme handelt. Wird die bereits eingesetzte Backup Software nicht unterstützt, kann auch VCB nicht eingesetzt werden (vgl. [AHN 07]).

Mit VCB sind jetzt alle wichtigen Funktionen und Zusatzprogramme von *VMwares Infrastructure 3* vorgestellt worden. Dies hat gezeigt, dass es eine Vielzahl von Einstellungen und Möglichkeiten gibt, um die Virtualisierungsumgebung zu steuern und zu verwalten. In Abbildung 3.18 ist ein abschließender Überblick aller Funktionen für die jeweilige Version zu sehen. Die Erstanschaffungskosten sind gerade für die umfangreiche Enterprise Edition sehr hoch (ab ca. 5.700 US-Dollar), bieten aber das Komplettpaket, das vor allem in Windowsumgebungen überzeugen kann. Demgegenüber steht immer noch die fehlende Unterstüzung für Linux. So kann weder der VI Client, noch der VC Server unter Linux installiert werden. Auch der Konverter und VCB funktioniert nicht im vollen Umfang mit Linuxservern, wie dies bei Windowssystemen der Fall ist. Zusätzlich darf nicht vergessen werden, dass eine Hochverfügbarkeit, mit der viel Werbung gemacht wird, nicht für die virtuellen Maschinen, sondern „nur" für die ESX Server gilt. Für die VMs müssen eigene Konzepte und Lösungen bedacht werden (vgl. [Ahne 07]). Zuletzt sei noch darauf hingewiesen, dass regelmäßig Patches für den ESX Server erscheinen, die diesen fortlaufend verbessern. Leider gibt es keine automatische Update-Funktion oder Hinweise, wann ein Patch erscheint. Dies kann nur durch ständiges Besuchen der Homepage ([vmh 07]) herausgefunden werden. Die Installation eines erschienenen Patches ist auch dann noch relativ kompliziert, denn er muss heruntergeladen, auf den ESX kopiert, dort entpackt und dann installiert werden. Dies muss für jeden Patch einzeln vorgenommen und kann nicht automatisiert werden. So sind für die letzte ESX Server Version (3.0.1) 53 Patches veröffentlicht worden (vgl. [vmh 07]), was bei mehreren Hosts zu einer zeitaufreibenden Beschäftigung führt.

Als abschließender Punkt zu den bisher vorgestellten Produkten, gibt es in Abbildung 3.19 eine zusammenfassende Übersicht der wichtigsten Eigenschaften und Unterscheidungen von *VMwares ESX Server*, *Microsofts*

Package Summary			
PRODUKTE	VMWARE INFRASTRUCTURE STARTER	VMWARE INFRASTRUCTURE STANDARD	VMWARE INFRASTRUCTURE ENTERPRISE
ESX Server	• • Nur NAS oder lokaler Speicher • Bereitstellung auf einem Server mit bis zu vier physischen CPUs und bis zu 8 GB physischem Arbeitsspeicher	•	•
VMFS	• • Nur auf lokalem Speicher • Enthält kein Cluster-Dateisystem	•	•
VirtualCenter Agent	•	•	•
Virtual SMP		•	•
VMotion			•
VMware HA			•
VMware DRS			•
VMware Consolidated Backup			•

Abbildung 3.18: Vergleich zwischen den erhältlichen Versionen von *VMware Infrastructure 3* (Quelle: [vmh 07])

Virtual Server und *XEN*. Mit diesem Überblick ist die Besprechung der wichtigsten Virtualisierungsumgebungen abgeschlossen. Nachdem nun die Produkte von VMware detailiert vorgestellt wurden, ist nun deren Funktionsweise bekannt und wird in Kapitel 6 in der Praxis angewandt. Die zuvor beschriebenen Funktionen für ein Management von virtuellen Maschinen orientierte sich an dem Produkt von VMware (den *Virtual Server*). Als Abschluss dieses Kapitels kommt es zu einer allgemeineren Betrachtung, was überhaupt Management in diesem Bereich bedeutet und welche Punkte dabei zu beachten sind.

3.3 Management der virtuellen und physikalischen Maschinen

Der Begriff „Management" ist ein oft verwendeter Begriff und wird in unzähligen Bereichen eingesetzt. Im IT Bereich wird unter diesem Begriff meist die Planung, Inbetriebnahme und Wartung der IT Infrastruktur verstanden. Hinter diesen Begriffen verbergen sich weitere detailliertere Vorgehensweisen und Abläufe, wie diese Aufgaben zu bewerkstelligen sind. Bei der Planung einer Virtualisierungsumgebung spielt die Verwaltung der physikalischen und der neu hinzukommenden virtuellen Maschinen eine wichtige Rolle. Durch die Virtualisierung kommt eine neue Ebene hinzu, die sich kaum mehr in das bisherige System eingliedern lässt. So enthält bisher ein Server eine bestimmte Anwendung, die bekannt ist und deren Reaktionen nachvollziehbar sind. Für das Management wird meist SNMP (Simple Network Management Protocol) eingesetzt, das zur Konfiguration und Überwachung von netzwerkfähigen Geräten dient. Das Protokoll definiert dazu die Kommunikation zwischen sogenannten Managern und Agenten. Der Manager ist die Arbeitskonsole des Administrators, während die Agenten direkt auf den Systemen und Netzkomponenten laufen, die überwacht oder konfiguriert werden sollen [Ecke 02]. Der Manager kann über vorab definierte „Managed Objects" Daten auslesen und verändern. Tritt bei einem Gerät ein unerwartetes Ereignis ein (eine sogenannte Trap), sendet der Agent unaufgefordert eine Nachricht an den Manager. In bestimmten Zyklen wird der Status der Geräte vom Manager automatisch abgefragt. Sollte im schlimmsten Fall keine Antwort zurückkommen, kann der Administrator zum Beispiel per Email darüber benachrichtigt werden. Virtuelle Geräte haben meist keine SNMP Unterstützung und können daher nicht in diese Struktur aufgenommen werden (vgl. [GKea 03]). Dabei wäre es von Vorteil, wenn es Managementprogramme gäbe, die den kompletten Status von sowohl physikalischen, als auch virtuellen Maschinen überwachen, abfragen und verändern können. Ganz aktuell bieten einige Serverhersteller, wie IBM mit dem *Systems Director Virtualization Manager* (vgl. [ibm 07]), Programme an, die mittels webbasiertem

Produkt	ESX Server	Virtual Server	XEN
Hersteller / Version	VMware / 3	Microsoft / 2005 R2	www.xen.org / 3.0
Wirtsbetriebssystem	RedHat Linux Wirtsbetriebssystem ist im ESX Server enthalten	Windows	Linux
Gastsysteme	Windows (32 / 64 Bit), Linux, Novel, Solaris	Windows (32 Bit), Linux	Windows (32 / 64 Bit), Linux, BSD, OpenSolaris
Virtuelle Hardware	NIC, SCSI, IDE, Parallel, Seriell	NIC, SCSI, IDE, Parallel, Seriell	NIC, SCSI, IDE, Parallel, Seriell, USB
Leistungsverlust Gast	3 - 18%	12 - 25%	bis 5%
Support für Vanderpool / AMD-V	Ja	Ja (mit ServicePack 1)	Ja
Kommandozeilenunterstützung	Ja	Ja	Ja
GUI Administration	Ja	Ja	Nein / in Entwicklung (Beta)
Managementprogramm für mehrere Server	Ja (Virtual Center - kostenpflichtig)	Ja (System Center Virtual Machine Manager - kostenpflichtig)	Ja (Drittanbieterproduke wie Enomalism - Open Source)
Sicherung der Gäste	Imagebasiert	Imagebasiert	Imagebasiert
Snapshots	Ja	Ja	Nein
Max. Anzahl Prozessoren	16	32	32
Max virtuelle Prozessoren / Gast	4	1 / momentan kein SMP der Gäste möglich	max. 32
Max. virtueller RAM	16 GB	3,6 GB	16 GB
NICs / Gast	4	4	>4
Installation Gast	Cdrom, Templates	Cdrom	Cdrom, Templates
Livemigration auf anderes Wirtsystem	Ja	Nein	Ja
Vervielfältigung der Gastbetriebssysteme (Cloning)	Manuell, Drittanbieterprodukte	Manuell, Drittanbieterprodukte	Manuell
Ressourcenüberwachung der Gäste	Ja	Ja	Ja
Lizensierung	Pro CPU	kostenlos	GPL / Open Source

Abbildung 3.19: Übersicht aktueller Produkte und deren Eigenschaften (Quelle: In Anlehnung an [Fert 06])

User Interface die Verwaltung virtueller und physischer Systeme über multiple Plattformen hinweg ermöglichen und dadurch vereinfachen. Mit dem Verkauf für die Öffentlichkeit Ende diesen Jahres wird sich zeigen, ob diese Programme so eingesetzt werden können, wie vollmundig versprochen wird. Ob es dann Managementprogramme für jede gängige Virtualisierungsumgebung geben wird oder es zu einigen Kollaborationen, wie bei VMware mit HP (vgl. [vmh 07]) kommen wird, ist bisher noch unklar. Im Moment erfolgt noch eine Trennung zwischen dem physikalischen Host und den virtuellen Maschinen. In den nächsten Abschnitten wird genauer auf diese Problematik eingegangen.

3.3.1 Administration der verwendeten physikalischen Server

Wie bereits erwähnt, ist SNMP in vielen Rechenzentren das eingesetzte Protokoll, um eine Überwachung mit den physikalischen Maschinen vorzunehmen. Dies kann auch immer noch verwendet werden, denn sowohl bei Virtualisierungsumgebungen, die auf ein Betriebssystem setzen, als auch die „Bare Metal" Variante von VMware bieten die gängigen Hersteller für alle Betriebssysteme Managementtools auf Basis von SNMP an. So bietet beispielsweise HP für sein *HP System Management* auch einen Agenten für das ESX Betriebssystem an, der dann mit dem Manager kommuniziert und Statusmeldung über das System gibt (vgl. [hph 07]). Bei der Überwachung mittels SNMP geht es vor allem um ausgefallene Komponenten (wie Netzwerkkarte, HBA Karte, etc.), die eine Einschränkung des Servers nach sich ziehen. Auch ist es teilweise möglich den ausgehenden Netzverkehr mittels Monitor zu beobachten. Der Datenstrom kann aber nicht mehr auf eine bestimmte Anwendung zurückgeführt werden (vgl. [GKea 03]). Handelt es sich nicht um eine virtualisierte Umgebung, ist dem Administrator bekannt, welche Anwendung, zum Beispiel ein Exchange Server, darauf läuft. Dabei sind Verhalten und gewisse Reaktionen bekannt und bei einem starken Anstieg des Datenverkehrs, kann dies ein alamierendes Zeichen sein, dass ein möglicher Virus großen Datenverkehr verursacht. Dies ist in einer Virtualisierungsumgebung nicht mehr der Fall, denn eine Lokalisierung eines erhöhten Datenaufkommens kann nicht auf eine bestimmte Anwendung zurückgeführt werden. Denn es laufen mehrere virtuelle Maschinen mit unterschiedlichen Programmen, die dafür verantwortlich sein können. Hier wird die Kontrolle des Datenstroms in die virtuellen Maschinen übergeben, denn diese müssen genau überwacht werden (siehe Abschnitt 3.3.4). Auch durch Lastverteilung kann eine auf diesem Host erstellte Maschine längst verschoben worden sein, was

wiederum keine Aussage über die Applikation zulässt. Daher führt die Virtualisierung zu einem geringeren Wert an Informationen (vgl. [GKea 03]). Die Wichtigkeit der Informationen nimmt aber teilweise noch zu. So befindet sich durch die Konsolidierung der Server mehrere virtuelle Maschinen auf einem physikalischem Host. Bei Ausfall dieses Servers sind eine Vielzahl an VMs mit den verbundenen Anwendungen betroffen, als dies ohne Einsatz von Virtualisierung der Fall wäre (vgl. [Rode 07]). Daher muss hier eine strenge Überwachung des Serverbetriebs vorgenommen werden und es gilt geeignete Ausfallszenarios zu planen. VMware bietet beispielsweise mit der HA Funktion (vgl. Abschnitt 3.2.2) bei *Virtual Infrastructure 3* eine Möglichkeit an, das bei einem Hostausfall die virtuellen Maschinen nach kurzer Zeit wieder auf einem anderen Host gestartet werden.
Auch im Wartungsfall (Erweiterung physikalischer Komponenten, Festplattenaustausch, etc.) müssen zusätzliche Informationen mit Hilfe der Virtualisierungsumgebung beschafft werden, denn das Herunterfahren des Servers betrifft nicht nur eine Anwendung, sondern mehrere, die entweder alle einzeln heruntergefahren oder entsprechend auf andere Server migriert werden müssen. Deshalb benötigt der Administrator sowohl die Informationen (z.B. per SNMP) von physikalischem Server, als auch von der entsprechenden Virtualisierungsumgebung. Erst dann können nach einer Abwägung, die entsprechenden Eingriffe (Austausch einer Komponente o.ä.) vorgenommen werden.
Als letzter Punkt sei die gesteigerte Sicherheitsanforderung erwähnt. In jeder Virtualisierungsumgebung gibt es eine Komponente, die die Verwaltung der VMs übernimmt. So ist beispielsweise bei XEN die Dom0 das privilegierte System, das vollen Hardwarezugriff besitzt und die die VMs koordiniert (vgl. [XEN 07]). Erhält nun ein unautorisierter Anwender den Zugriff zum Dom0 System, verfügt er nicht nur über die eingedrungene Maschine, sondern kann auch die virtuellen Maschinen verschieben, herunterfahren oder löschen. Daher muss der Zugriff zum Gastbetriebssystem und zu weiteren Systemen streng überwacht werden. Aber nicht nur bei Angriffen auf ein System, sondern auch durch unbewusstes Handeln innerhalb einer VM kann es Folgen für den Host haben. Einer der Vorteile von Virtualisierung, ist die Möglichkeit heterogene Systeme in VMs auf einem physikalischen Host zu installieren. Dies kann aber auch zu Nachteilen oder Problemen führen, wenn z.B. Systeme oder Anwendungen in eine VM installiert werden, die besonders anfällig für Angriffe von außerhalb sind (vgl. [Rode 07]). Der Angriff kann dann auf den gesamten Host Einfluss nehmen, wenn hier keine Vorsichtsmaßnahmen getroffen werden. Daher haben viele IT-Abteilungen sehr strenge Vorschriften für den Einsatz und die Konfiguration physikalischer Server. Nur getestete Konfigurationen dürfen in Produktivumgebungen eingesetzt werden [Rode 07]. Diese müssen auch für Hosts mit virtuelle Umgebungen umgesetzt werden. Für Tests und Entwicklungen können eigenständige, voneinander getrennte Strukturen aufgebaut werden, die sich nicht gegenseitig beeinflussen können. VMs haben keine physikalischen Zugangsberechtigungen (Chipkarte für Serverraum, etc.), wie voneinander getrennte Maschinen in unterschiedlichen Räumen. Neben Einhalten gewisser Vorsichtsmaßnahmen gilt es die Wirtssysteme immer auf den neuesten Stand zu halten, damit Eindringlinge bekannte Sicherheitslücken nicht ausnutzen können. Auch sichere und für Andere nicht herauszufindende Passwörter tragen zum Schutz bei. Die erhöhte Sicherheit bei dem Zugriff auf einen Host mit mehreren VMs muss streng befolgt werden, denn bei einem erfolgreichen Angriffsversuch, ist eine Kontrolle über alle sich dort befindenden virtuellen Maschinen möglich.
Nachdem nun die Verwaltung der Hosts und die zu beachtenden Gefahren besprochen wurden, erfolgt im nächsten Punkt eine Vorstellung des Managements von virtuellen Maschinen.

3.3.2 Zentrale Administration virtueller Maschinen

Die Aufgaben bei der Verwaltung von virtuellen Maschinen orientieren sich an den verschiedenen Phasen des Dienstlebenszyklus (vgl. [HAN 99a]). Diese bestehen aus „Planning", „Negotiation", „Provisioning", „Operation/Change" und „Withdrawal". Für den vorliegenden Fall können diese verwendet werden, da auch virtuelle Maschinen einen ähnlichen Zyklus durchlaufen. Die erste Phase („Planning") muss zwar im Vorfeld durchgeführt werden, spielt aber in diesem Abschnitt keine Rolle. Auch der nächste Schritt, das Aushandeln („Negotiation") verschiedener Parameter, wird hier nicht weiter betrachtet. Für den operativen Ablauf sind vor allem die nächsten Phasen von Bedeutung. Diese werden im Folgenden vorgestellt und an die vorhandene Situation angepasst.
Provisioning: In dieser Phase geht es um die Installation, Konfiguration und Testen der virtuellen Maschine. So muss zuerst eine virtuelle Maschine erzeugt werden, die dann mit einem Betriebssystem installiert wird. Beim Erstellen von VMs wird festgelegt, wie die virtuelle Hardware aussieht, wie der Name der VM ist oder in welches Netzwerk sie eingebunden werden soll. Die virtuellen Hardwarekomponenten richten sich an den

zugrundeliegenden Host (es kann nicht mehr RAM zugewiesen werden, als physikalisch vorhanden ist) und an der verwendeten Virtualisierungsumgebung. So unterstützt beispielsweise Microsofts *Virtual Server* bisher keine Multiprozessoren. Aus diesem Grund erhält eine VM bei diesem Produkt nur einen Prozessorkern (vgl. [Fert 06]). Zusätzlich muss ein Name vergeben werden, der zur besseren Zuordnung dem späteren Maschinennamen entspricht. Solch ein Name muss eindeutig sein und gegebenenfalls der Firmenpolitik (oft gibt es Namenskonventionen für Server, um diese anhand des Namens besser zuordnen zu können) entsprechen, wenn dieser später im Netzwerk aktiv sein soll. Neben dem Maschinennamen, ist es von Bedeutung, dass die VM in einem bestimmten Netzwerk arbeitet. Meistens können bei den Virtualisierungsumgebungen auch virtuelle Netzwerke eingerichtet werden, um bestimmte VMs von anderen Maschinen zu trennen. Die Virtualisierungssoftware kümmert sich darum, dass diese softwarebasierte Trennung auch gewährleistet wird. Nachdem alle wichtigen Einstellungen vorgenommen wurden, existiert eine virtuelle Maschine, die ab sofort zur Installation des Gastsystems bereit steht. In der erstellten VM kann daraufhin mittels Boot CD ein Betriebssystem installiert werden. Dies läuft genauso ab, wie es der Administrator von einem herkömmlichen System gewohnt ist. Das Gastsystem wird dabei auf eine virtuelle Platte installiert, die meist als Containerdatei vorliegt (die Platte kann auch aus mehreren Dateien bestehen). Der Speicherort dieser Containerdateien inklusive entsprechender Konfigurationsdaten muss vorher geklärt werden. So spielt es für manche Funktionen eine Rolle, ob es sich um einen gemeinsamen Datenspeicher handelt, auf den alle eingerichteten Hosts Zugriff haben oder ob die VMs auf unterschiedlichen Datenspeichern liegen. Befindet sich die virtuelle Platte nicht auf einem gemeinsamen Datenspeicher, kann es bei der Migration auf einen anderen Host zu längeren Verzögerungen kommen. Dies liegt daran, dass alle Daten der VM (virtuelle Platte(n), Konfigurationsdateien, etc.) erst kopiert oder verschoben werden müssen. Im Folgenden wird davon ausgegangen, dass die virtuellen Maschinen zentral gespeichert werden, auf den die konfigurierten Hosts alle Zugriff haben.

Oft ist gewünscht, dass vorhandene physikalische Server zu virtuellen Servern (P2V) migriert werden. Dies spart Zeit und Konfigurationsaufwand, wenn das vorhandene System importiert werden kann und nicht erst eine Neueinrichtung erfolgen muss. Aus diesem Grund zählt diese Funktion auch zur zentralen Steuerung von VMs. Je nach Virtualisierungsumgebung gibt es eine Unterstützung sowohl für physikalische, als auch virtuelle Maschinen. So soll es nicht nur möglich sein, einen Host zu migrieren, sondern auch virtuelle Maschinen von anderen Systemen in eine zentrale Verwaltungsstruktur einzubinden. Beim Import des physikalischen Hosts kann die VM, auf Basis der bisherigen Maschine, die Einstellungen identisch übernehmen. Gegebenenfalls kann eine Optimierung vorgenommen werden, falls beispielsweise weniger Hauptspeicher benötigt wird, als in der alten Hardware vorhanden war. Unabhängig, ob die VM importiert oder neu eingerichtet wurde, es stehen daraufhin die VMs bereit und lassen sich über einen entsprechenden Befehl aktivieren.

Eine weitere Aufgabe ist das Klonen von virtuellen Maschinen, inklusive deren Einstellungen und virtuellen Platten. Dies ist eine wichtige Funktion, die beim Management von virtuellen Maschinen benötigt wird. So kann flexibel auf Anforderungen (z.B. Schulungsrechner mit Applikation X wird benötigt) reagiert werden. Die VMs können dann entweder in die bisherige Verwaltungsstruktur aufgenommen werden oder für eigenständige Programme (z.B. dem *VMware Player*) exportiert werden. Des Weiteren können so auch Testumgebungen im Serverbereich erstellt werden. Diese können in einem eigenen virtuellen Netz laufen, deren Kontrolle aber immer noch über das zentrale Management läuft. Neben dem Klonen ist als letzte Möglichkeit, die Erstellung von VMs aus zuvor angelegten Templates (Vorlagen) zu nennen. Auf der Basis eines Templates entsteht in kurzer Zeit eine virtuelle Maschine, die bereits mit grundlegenden Funktionen ausgestattet ist. Die VM muss im nächsten Schritt noch für den entsprechenden Einsatz angepasst werden (Konfiguration der IP Adresse, Servername, etc.) und kann daraufhin verwendet werden. Mit dieser Funktion ist eine einfachere Bereitstellung von VMs möglich.

Operation/Change: In der nächsten Phase geht es um den laufenden Betrieb und die Konfiguration von virtuellen Maschinen. Die Gewährleistung des Betriebs erfolgt durch Support, Monitoring, Identifikation von Fehlern, Behebung dieser Fehler und weiteren Punkten. Dazu eignet sich am Besten eine zentrale Verwaltungskomponente. Diese kann beispielsweise über unterschiedliche Symbole oder entsprechenden Text anzeigen, ob eine Maschine in Betrieb ist oder nicht. Zur besseren Verwaltung oder Lastverteilung (siehe nächster Abschnitt) können die Maschinen auf unterschiedlichen Hosts gestartet werden. Um nicht nur einzelne Informationen von einer VM zu erhalten, sondern auch auf sie zugreifen zu können, muss es möglich sein, entweder über eine integrierte Konsole oder mittels eines entsprechenden Programms die VM aufzurufen. Dies muss sowohl für alle VMs als auch für alle unterstützenden Betriebssysteme der Virtualisierungsumgebung möglich sein. Auch im Fehlerfall müssen entsprechende Mechanismen eingesetzt werden, um Probleme schnell zu identifizieren. Liegen alle notwendigen Informationen vor, muss mit Hilfe einer Lösungsstrategie der Fehler beseitigt werden können. Dazu bietet die Verwaltungskomponente eine komfortable Übersicht aller VMs,

um schneller das Problem zu beheben. Andererseits können durch die neue Technologie Fehler auftreten, die davor unbekannt waren. Daher darf das Fehlermanagement nicht unterschätzt werden und es muss zuvor entsprechendes Wissen über die Technologie erlangt werden.
Falls das Management diese Funktion unterstützt, ist ein weiterer wichtiger Punkt die Verwendung von Snapshots. So kann mit deren Hilfe der Betriebszustand einer VM gesichert werden. Im Bedarfsfall erfolgt eine Rücksetzung auf den zuvor gespeicherten Sicherungspunkt. So kann vor einer Installation ein Snapshot erstellt werden, um im Fehlerfall an die ursprüngliche Stelle zurückzukehren. Dies ist aber eine Funktion, die nicht alle Produkte anbieten.
Ein weiterer wichtiger Punkt ist die Option, laufende VMs auch noch zu einem späteren Zeitpunkt erweitern zu können. So soll es möglich sein, neu erstellte virtuelle Festplatten zu einer VM hinzuzufügen oder eine VM mit mehr Hauptspeicher auszustatten. Diese Möglichkeit ist wichtig, um virtuelle Maschinen möglichst flexibel einzusetzen und optimieren zu können. Es wäre denkbar, die Daten einer Anwendung auf eine neu hinzugefügte virtuelle Platte speichern zu lassen. Danach wird diese Platte wieder entfernt und mittels der eingesetzten Backuplösung gesichert. Im Bedarfsfall kann die virtuelle Platte an eine andere beliebige VM angebunden werden und die Daten stehen zur Verfügung.
Withdrawal: In der letzten Phase geht es im weiteren Sinne um die Freigabe der Betriebsmittel. Virtuelle Maschinen verbrauchen in den bisherigen Phasen Ressourcen, sei es Plattenspeicher oder im laufenden Betrieb die der CPU und des Hauptspeichers. Diese müssen im letzten Schritt wieder freigegeben werden, um daraufhin für weitere VMs zur Verfügung zu stehen. Die erste Möglichkeit ist das Ausschalten einer VM, damit sofort Ressourcen bereitstehen, die an anderer Stelle dringender benötigt werden. Des Weiteren kann für eine VM eine bestimmte Laufzeit festgelegt worden sein. Nach Beendigung muss die Maschine über die Verwaltungskomponente entfernt werden. Ob die VM zuvor gesichert werden soll oder ob diese problemlos gelöscht werden kann, muss beim Erstellen mit den entsprechenden Personen vereinbart werden. Je nachdem, ob die Maschine vorübergehend oder dauerhaft deaktiviert wird, muss ein festgelegtes Verfahren (z.B. erst die Sicherung dann das Löschen der VM) im letzten Schritt durchgeführt werden. Damit ist der Zyklus abgeschlossen.

Alle wichtigen Phasen und deren Aufgaben wurden nun genau besprochen. Dabei ist auf zwei besondere Punkte bisher nicht genau eingegangen worden. Dies ist erstens die Lastverteilung und die dadurch notwendige Verschiebung von VMs (in der „Operation” Phase). Außerdem muss hier wie bei den physikalischen Hosts die Sicherheit bedacht werden. Die spielt in allen zuvor genannten Phasen eine wichtige Rolle und wird im übernächsten Abschnitt genau behandelt. Zuvor wird aber auf die Lastverteilung genauer eingegangen.

3.3.3 Lastverteilung

Die Lastverteilung ist eine wichtige Funktion bei der Verwaltung von mehreren virtuellen Maschinen. So kann beispielsweise ein System während des Jahres kaum Ressourcen verbrauchen, benötigt aber gegen Ende wesentlich mehr Leistung. Durch eine flexible Zuteilung kann der VM mehr Ressourcen zur Verfügung gestellt werden. Dies kann entweder durch die „Change” Phase (siehe vorheriger Abschnitt) geschehen oder die VM muss auf einen Host mit ausreichenden Ressourcen verschoben werden. Wird die zugeteilte Leistung nicht mehr benötigt, wird die VM auf den vorherigen Host zurück geschoben. Danach stehen die freigewordenen Ressourcen wieder zur Verfügung. Die einfachste Methode dies durchzuführen, besteht darin, die virtuelle Maschine herunterzufahren, diese auf den anderen Host zu verschieben und dort die VM wieder zu starten. Durch den Aufbau einer VM müssen nicht eine Vielzahl von Dateien verschoben werden. Meist handelt es sich nur um wenige Dateien, aus denen die VM besteht (virtuelle Platte(n), Konfigurationsdateien, Sicherungspunkte). Liegen die virtuellen Maschinen in einem zentralen Datenspeicher, muss keine Migration erfolgen, sondern die Managementkomponente verwaltet, auf welchem Host die VM gestartet wird. Informationen über die VMs können dort vom Administrator eingesehen werden, um mögliche weitere Lastverteilungen vorzunehmen. Neben dieser unkomfortablen Lösung (dass die Maschine erst heruntergefahren werden muss) gibt es auch die Möglichkeit die VM im laufenden Betrieb zu verschieben. Dieser Vorgang wird Live- oder Onlinemigration genannt (vgl. [AHN 07] und [Fert 06]) und sorgt für geringere Ausfallzeiten, da die Maschine nicht mehr ausgeschaltet werden muss. Auch hier ist der zentrale Datenspeicher von Vorteil, denn es entfällt das Kopieren, das viel Zeit sparen kann. Optional kann die Livemigration automatisiert werden. So wird bei einem überschrittenen Wert (z.B. „CPU Auslastung über 70 Prozent”) die VM auf einen anderen Host migriert. Zusätzlich ist es von Vorteil, wenn die Granularität der Lastverteilung entsprechend eingestellt werden kann. So kann das

Managementsystem nur Informationen (z.B. per Email) von überschrittenen Schwellwerten herausgeben oder es darf nur bestimmte VMs migrieren. In einer vollautomatisierten Konfiguration übernimmt das System die komplette Lastverteilung nach vordefinierten Einstellungen. Des Weiteren kann die Lastverteilung vor dem Aktivieren einer VM prüfen, auf welchem Host gerade die meisten Ressourcen vorhanden sind und diese dann dort Starten. Dazu müssen der Managementkomponente die Informationen der Ressourcen aller Hosts und der darauf laufenden VMs vorliegen. Durch diese Lastverteilung entsteht nach und nach eine Entkoppelung der physikalischen Server. Es ist nicht mehr von Bedeutung auf welchen Server genau eine VM läuft, sondern es stehen in der Virtualisierungsumgebung gewisse Ressourcen zur Verfügung und diese sollen bestmöglich aufgeteilt und genutzt werden. Dennoch soll ein Server nicht hundertprozentig durch die VMs ausgelastet werden (ein gewisser Puffer an Ressourcen auf jedem Host ist von Vorteil). Bei den gängigen Virtualisierungslösungen gibt es meist nur noch Ressourcenpools (sowohl bei XenSource, als auch bei VMware), die für die VMs gewisse Ressourcen bereitstellen, unabhängig, wie sich die VMs auf den physikalischen Servern dann verteilen. Beispielsweise kann in einem Host eine Komponente ausfallen, wodurch für alle VMs weniger Ressourcen zu Verfügung stehen. Das Managementsystem muss daraufhin eine Verteilung der VMs vornehmen, um den Vorgaben der Ressourcenpools zu entsprechen.
Bei der Livemigration darf aber die Belastung des Hosts nicht vernachlässigt werden. Erfolgt eine Migration einer VM, so muss die Virtualisierungsumgebung eingreifen, um alle Informationen, wie Registereinträge der CPU, die Daten im Hauptspeicher und andere Punkte auszulesen. Diese müssen dann auf das andere Hostsystem übertragen werden. Für diesen Vorgang wird in der Regel das Gastsystem kurz angehalten, damit die Integrität der Daten gewährleistet werden kann. Nach erfolgreichem Verschieben wird das System wieder gestartet und läuft weiter. Dieser Eingriff stellt daher eine gewisse Belastung durch die Kontextwechsel dar, die bei jeder Livemigration vorhanden sind. Je öfter dies geschieht, desto eher kann es zu Beeinträchtigungen für die restlichen Maschinen kommen.
Insgesamt zeigt sich durch die Möglichkeit der Livemigration und der Lastverteilung, dass eine Zuordnung von VMs zu einem bestimmten Host nicht mehr nötig ist. Diese Vorteile des flexiblen Handelns und der optimierten Auslastung bringt aber auch zusätzliche Gefahren für die Sicherheit. Welche Aspekte dabei zu beachten sind und welche Aufgaben der Managementkomponente dabei zufallen, wird im nächsten Abschnitt besprochen.

3.3.4 Sicherheit virtueller Maschinen

Der Begriff „Sicherheit” ist wie das Wort „Management” ein vielgenutzter Begriff, hinter dem sich eine Vielzahl an Problemen, Konzepte und Bedeutungen verbergen. Wird von Sicherheit bei virtuellen Maschinen gesprochen, so gibt es mehrere Punkte, die dabei von Bedeutung sind. Zuerst muss eine VM genauso wie eine physikalischer Rechner gegen Angriffe von Außerhalb geschützt werden, beispielsweise durch einen Virenscanner. Insgesamt befindet sich der Host mit den VMs in einer bestimmten Netzstruktur wieder. Die Kommunikation nach Außen funktioniert genauso, wie dies bei den anderen Servern der Fall ist. Das Internet kann beispielsweise über einen Proxyserver aufgerufen werden und die virtuellen Server sind daher nach Außen nicht sichtbar. Des Weiteren lässt eine Firewall nur bestimmte Ports durch und filtert mögliche Angriffe von Außen. In der Regel befinden sich die Hosts und die VMs innerhalb dieses geschützten Netzes. Auch die Speicherung der virtuellen Platten und Daten geschieht meist auf einem Datenspeicher im internen Netz. Wenn aber eine VM auf eine externe Ressource zugreift, kann dieser Zugriff schwer überwacht werden. Dies führt zu einem Sicherheitsrisiko. Daher werden oft externe Zugriffe unterbunden oder durchlaufen mehrere Sicherheitssysteme wie eben Firewalls, Intrusion Prevention oder Access Control (vgl. [ref 06]). Die Probleme, die durch sogenannte „Intra-host Threats” (vgl. [ref 06]) entstehen, sind ungleich größer und schwieriger abzufangen. Ein physikalischer Host kann über zahlreiche virtuelle Server, Applikationen und Nutzer/Administratoren verfügen (vgl. [ref 06]). Dadurch ist eine sichere Verwaltung komplex und es müssen strenge Regeln eingehalten werden. So kann über einen zentralen Verzeichnisdienst Rechte eingerichtet werden, um den Zugriff auf einen virtuellen Server zu privilegieren. Dies erleichtert die Verwaltung, wenn nicht für jede VM ein eigenes Benutzerkonto eingerichtet werden muss. Mit einer strikten Rechtevergabe können teilweise die VMs geschützt werden. Dennoch kann es Nutzer (aber auch Applikationen) geben, die eine Bedrohung zu angrenzenden virtuellen Maschinen übermitteln können. Deshalb müssen virtuelle Maschinen gegenüber ihren unmittelbaren Nachbarn geschützt werden. Fehlt ein effektiver Schutz gegenüber den Nachbarn, kann das zur Verbreitung von Viren, Datendiebstahl, Denial of Service und sonstigen Konsequenzen führen. Obwohl Virtualisierungslösungen eine logische Partitionierung von virtuellen Maschinen vornehmen, die mit

einer räumlichen Trennung zweier physikalischer Maschinen vergleichbar ist, lässt sich diese softwarebasierte Trennung überwinden. Angreifer können über einen „Back Door Entry" ins System gelangen (vgl. [ref 06]). Neuste Gefahrenquellen stellen Rootkits dar, die für virtuelle Umgebungen große Bedrohungen darstellen (vgl. [Bach 07]). Das Rootkit „Blue Pill" verschiebt das laufende Betriebssystem des Hosts in eine virtuelle Umgebung. Danach hat das verschobene Betriebssystem keinerlei Möglichkeiten mehr, das Rootkit zu erkennen, da es außerhalb seines Wahrnehmungshorizonts läuft [Bach 06]. Daneben gibt es noch andere Rootkits, die nach einem ähnlichen Prinzip arbeiten. Ist das Hostsystem infiziert, kann die Kontrolle darüber übernommen werden. Damit sind alle virtuellen Maschinen betroffen, die über das Hostsystem gesteuert werden. Die Gefahr durch Rootkits wird daher „in den nächsten fünf Jahren relevante Ausmaße annehmen." [Schm 07].
Aber auch wenn eine VM und nicht der komplette Host infiziert ist, könnte diese auf andere lokale VMs einen Angriff starten, indem die virtuellen Netzwerk Ressourcen genutzt werden. Eine virtuelle Maschine kann beispielsweise das virtuelle Netzwerk mit Schadcode oder Netzlast überfluten, so dass ein legitimierter Zugriff durch andere virtuelle Maschinen unmöglich wird [ref 06]. Der Netzverkehr könnte von der infizierten VM auch abgehört oder manipuliert werden. Aufgrund dieser Gefahren heraus ist es notwendig, dass der Administrator über alle aktiven Komponenten, Dienste und Kommunikationswege informiert ist. Dies ist eine komplexe Aufgabe, wobei die Verwaltungskomponente unterstützend helfen kann. Viele Informationen sind hier gespeichert, wie der verwendete Datenspeicher oder Logdateien über die Auslastung von VMs. Ungewöhnliches Verhalten, z.B. ein signifikanter Anstieg der Netzlast einer VM, kann möglicherweise auf einen Virenbefall hindeuten. Logdateien sollten nicht nur über die Auslastung der VM, sondern auch über alle Veränderung an der VM geführt werden. Des Weiteren werden alle Benutzer bei der Anmeldung an einer VM registriert. Dies kann von Nutzen sein, wenn spätere Probleme nachvollzogen werden müssen. Grundsätzlich sollten Änderungen nur bestimmte Administratoren vornehmen dürfen. Die Rechte der User sollten soweit eingeschränkt sein, dass diese für systemkritische Änderungen nicht autorisiert sind.
Insgesamt gibt es im Bereich Sicherheit bei virtuellen Maschinen vieles zu beachten, das durch herkömmliche Sicherheitskonzepte nicht abgedeckt ist. Gerade die Gefahr durch die Rootkits wird in Zukunft für große Probleme sorgen. Zwar bieten die Managementkonsolen teilweise Möglichkeiten an, Zugriffe und Sicherheiten zu gewährleisten, aber dieser Schutz ist unzureichend. So gibt es einige Drittherstellerprogramme, die ein Sicherheitskonzept für virtuelle Umgebungen anbieten. Diese gehen dabei auf die oben beschriebenen Gefahren ein und bringen angepasste Sicherheitslösungen mit. Ein Vertreter ist beispielsweise *Reflex VSA* (virtual security appliance) von Reflex Security Incorporated (vgl. [ref 06]).

Mit diesem Punkt ist das Grundlagenkapitel abgeschlossen. Dabei wurden auf die Aufgaben und Probleme beim Verwalten von virtuellen Maschinen eingegangen. Dies sind wichtige Eckpunkte, die bei einer späteren Produktauswahl von Bedeutung sind. Auf Basis der Informationen, wie Virtualisierung funktioniert, welche Arten es gibt und welche versteckten Probleme dabei auftreten können, kann im nächsten Kapitel die Anforderungsanalyse vorgenommen werden. Jetzt ist es möglich, realistische Anforderungen an eine Virtualisierung zu stellen, wenn der Aufbau dahinter bekannt ist. Wie diese Anforderungen aussehen und wie ein strukturiertes Vorgehen möglich ist, zeigt das nächste Kapitel.

4 Anforderungsanalyse

Welche Probleme und Schwierigkeiten bei einer heterogenen Infrastruktur auftreten können, wurde bereits in Kapitel 2 angesprochen. Diese gilt es zu lösen und daher werden gewisse Anforderungen an die Virtualisierungsumgebung gestellt. Die beiden entscheidenden Punkte sind die Kosteneinsparung und eine bessere Servicequalität, die mit Hilfe von Virtualisierung erreicht werden sollen. Dies sind aber zwei allgemeine Anforderungen, die keine konkrete Überprüfung zulassen. Daher muss eine genaue Anforderungsanalyse erfolgen, die detaillierte Anforderungen benennt und vorstellt. Dabei müssen diese einfach formuliert, eindeutig, machbar und prüfbar sein (vgl. [Kitz 04]). Ob die Anforderungen auch machbar und prüfbar sind, muss sich in der Praxis herausstellen. Ein mögliches Anwendungsszenario wird in Kapitel 6 vorgestellt, das sich auf eine bestimmte Ausgangssituation bezieht. Die in diesem Kapitel ermittelten Anforderungen werden sich an einen allgemeineren Fall richten. Ein Großteil der Anforderungen wird sich mit dem speziellen Szenario decken.
Aus diesem Grund wird zuerst die Ausgangssituation für den Fall der Astrium GmbH vorgestellt (Abschnitt 4.1). Dabei wird auf deren IT Infrastruktur eingegangen, wie diese aussieht und welche Probleme daraus resultieren. Zusätzlich gibt es gewisse Vorgaben und Ziele, die an die Virtualisierung gestellt werden. Einige dieser Ziele werden durch die allgemeinen Anforderungen im folgenden Abschnitt 4.2 abgebildet. Hier werden alle wichtigen Punkte vorgestellt, zusammengefasst und kategorisiert, die sich teilweise in den bisherigen Szenarien schon herausgestellt haben. Eine besondere Anforderung ist die Abbildung der Use Cases mit Hilfe der *IT Infrastructure Library* (kurz: *ITIL*), die in Abschnitt 4.3 besprochen wird. Dabei folgt zuerst eine allgemeine Vorstellung der ITIL und welche Bereiche hier von Bedeutung sind. Die vorgestellten Methoden und Verfahren werden daraufhin auf die Use Cases angewandt. Der Ablauf der Use Cases ist dadurch an der ITIL angelehnt (vgl. [ITIL 02]) und bietet einen theoretischen Rahmen für das weitere Vorgehen. Dies ist der letzte Punkt und die Anforderungsanalyse ist damit abgeschlossen. Die gewonnenen Informationen fließen daraufhin in das Konzept in Kapitel 5 ein.

4.1 Der Anwendungsfall Astrium GmbH

Die Vorteile der Virtualisierung wurden schon mehrfach besprochen und bieten daher für viele Firmen unterschiedlichste Einsatzmöglichkeiten. Eine Virtualisierungsumgebung kann sowohl in der Entwicklung für Testumgebungen, als auch zur Serverkonsolidierung eingesetzt werden, was bei großen Firmen meistens eine sinnvolle Erweiterung ist. Die Astrium GmbH ist ein typischer Vertreter, der mit den Problemen einer komplexen IT Infrastruktur zu kämpfen hat. Dies liegt nicht nur an der Größe der Firma, sondern auch an den Fusionen und Trennungen in der Firmengeschichte. Im Idealfall muss dies für die IT Landschaften auch gelten, dass diese verschmolzen und wieder getrennt werden. Dies ist aber in der Praxis wesentlich schwerer durchzuführen, wenn sich für die Mitarbeiter nichts ändern soll, die Anwendungen dauerhaft verfügbar sein und unterschiedliche Hardware und Netztopologien zusammengeführt werden sollen. Dies ist auch in anderen Firmen ähnlich, denn der Mitarbeiter möchte, dass das System läuft und er seine Anwendungen nutzen kann. Wie das im Detail funktioniert und was für Probleme es gibt, ist für ihn nicht von Bedeutung.
Für den Anwendungsfall Astrium GmbH wird zuerst kurz die Firmengeschichte in Abschnitt 4.1.1 vorgestellt. Zusätzlich erfolgt eine Einordnung in die Firmenstruktur, in der die Realisierung vorgenommen wird. In Abschnitt 4.1.2 wird die Ausgangssituation beschrieben, welche IT Landschaft vorliegt. Diese ist ähnlich zum generischen Szenario aus Kapitel 2, hat aber einige Besonderheiten, wie eine veraltete NT4 Domäne, die aber noch genutzt wird. Aus dieser Infrastruktur ergeben sich mehrere Aufgaben, von denen zwei Use Cases besonders von Bedeutung sind. Diese werden im letzten Schritt in Abschnitt 4.1.3 genau vorgestellt.

4.1.1 Die Firma Astrium GmbH

Die Astrium GmbH, eine 100-prozentige Tochtergesellschaft der EADS (European Aeronautic Defence and Space Company), ist spezialisiert auf zivile und militärische Raumfahrtsysteme, sowie weltraumgestützte Dienstleistungen. Im Jahr 2006 erzielte EADS Astrium einen Umsatz von 3,2 Milliarden € und beschäftigte rund 12.000 Mitarbeiter in Frankreich, Deutschland, Großbritannien, Spanien und den Niederlanden. Das Kerngeschäft gliedert sich in drei Bereiche: die beiden Business Units Astrium Space Transportation für Trägerraketen und Weltraum-Infrastrukturen, Astrium Satellites für Satelliten, Antennen, Optikinstrumente und Bodensegmente, sowie die 100-prozentige Tochter Astrium Services für die Entwicklung und Lieferung satellitenbasierter Dienstleistungen (vgl. [ast 07a]).
Die momentan bekannteste Anwendung von Astrium ist die Entwicklung des „Galileo-Systems". Das europäische Satellitennavigationssystem Galileo, das bis zum Ende des Jahrzehnts einsatzbereit sein soll, wird aus einer Konstellation von 30 Satelliten bestehen, die unter ziviler Kontrolle für eine weltweite Abdeckung sorgen werden (vgl. [ast 07b]). Dies gilt als Konkurrenzprodukt zum bekannten NAVSTAR-GPS (Global Positioning System), das vom US-Verteidigungsministerium entwickelt wurde (vgl. [gps 07]).
EADS ist ein global führender Anbieter in der Luft- und Raumfahrt, im Verteidigungsgeschäft und den dazugehörigen Dienstleistungen. Im Jahr 2006 lag der Umsatz bei rund 39,4 Milliarden €, die Zahl der Mitarbeiter bei mehr als 116.000 (vgl. [ast 07a]).

Die Realisierung des Konzeptes (siehe Kapitel 6) wurde bei Astrium Satellites in der Abteilung „Data Center Services (*DCS*)" durchgeführt. Diese ist eine Unterabteilung von „IT Operations", in der neben *DCS* die Abteilungen „Network & Telecommunications" und „End user services" organisiert sind. Der Abteilung *DCS* kommen laut Intranet unter anderem folgende Aufgaben und Pflichten zu:

- Betreiben und Instandhalten der Serverlandschaft und Plattenspeicher
- Dauerhafte Bereitstellung bestimmter Firmendienste, wie Email, SAP, Intranet und andere Firmensysteme
- Gewährleistung von Hochverfügbarkeit und schnellen Antwortzeiten gegenüber allen Astrium Usern
- Handhabung von Daten in Bezug auf Eingabe, Aktualisierung, Lagerung und Wiederherstellung
- Durchführung von *IMAC* (Install, Move, Add, Change) Tätigkeiten für alle Firmendienste
- Gewährleistung von Verfügbarkeit und Integrität von Daten
- Einhaltung von festgelegten Sicherheitsrichtlinien
- Messung, Dokumentation und Weitergabe von Dienstqualitäten
- Koordination von 'Third-Party' Anbietern für bestimmte Dienste

In dieser Abteilung ist die Umsetzung eines Virtualisierungskonzepts möglich, wobei die festgelegten Vorgaben von *DCS* eingehalten werden müssen. Beispielhaft sei hier erwähnt, dass insbesondere die dauerhafte Bereitstellung von Firmendiensten und die damit verbundene Hochverfügbarkeit ein wichtiger Punkt ist, der im späteren Konzept einfließen muss. Organisatorische Absprachen mit anderen Abteilungen, z.B. bei der Einrichtung entsprechender Netzwerkverbindungen für die Server können ohne Probleme durchgeführt werden. Damit steht einer Umsetzung des Konzeptes nichts mehr im Wege.
Im nächsten Punkt wird auf die zugrundeliegende Server-Infrastruktur eingegangen und wie eine Optimierung nach einer Virtualisierung aussehen könnte.

4.1.2 Ausgangssituation der IT Infrastruktur

Die vorhandene Infrastruktur zeichnet sich durch eine heterogene Serverlandschaft mit unterschiedlichen Betriebssystemen aus. Dies liegt vor allem an der Firmengeschichte von Astrium, in deren Vergangenheit es mehrere Fusionen und Trennungen von Geschäftsbereichen gab. Dies spiegelt sich in der IT Struktur wider, die nicht jede Umstellung bestmöglich umsetzen konnte. Es gab mehrere temporäre Lösungen, die teilweise

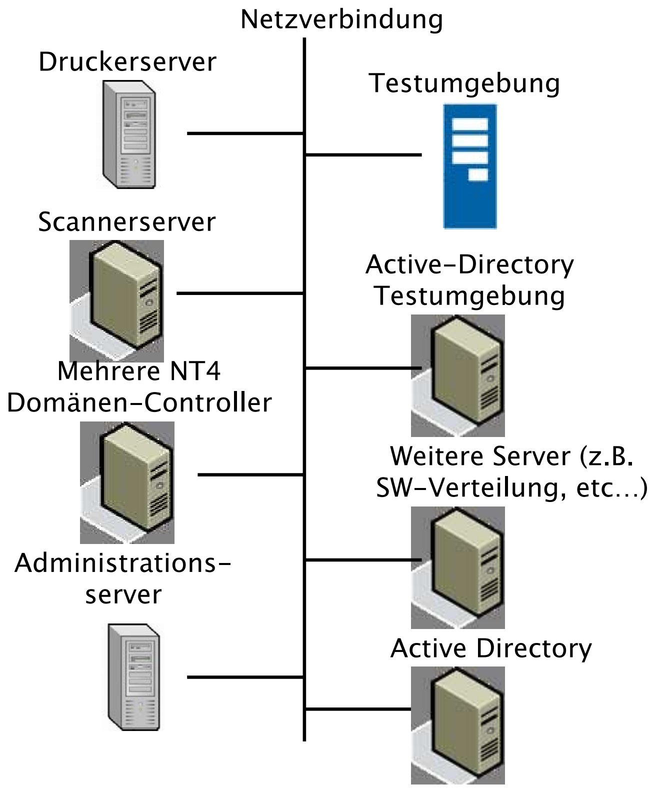

Abbildung 4.1: Ausgangslage der IT Infrastruktur bei der Astrium GmbH

bis heute Bestand haben. Des Weiteren benötigen die laufenden Projekte diverse Hard- und Softwareanforderungen, um in den unterschiedlichen Bereichen von Astrium, wie Satellitennavigation, Antennenforschung oder Optikentwicklung die jeweilige Umgebung simulieren zu können. So müssen Systeme erhalten bleiben, deren Unterstützung oder Weiterentwicklung seit Jahren nicht mehr möglich ist, aber der aktuelle Bestand weiterhin benötigt wird. Dies zeigt sich vor allem in der fortwährenden Nutzung von mehreren Servern mit dem Betriebssystem *Windows NT4 Server*. Dieses Betriebssystem befindet sich vor allem noch auf einem Druckerserver, mehreren Domänencontrollern, Administrationsservern und Testumgebungen im Einsatz. Doch auch ältere Softwareverteilungsserver und eine Active Directory Testumgebung (beide auf Basis von *Windows 2003 Server*) sind vorhanden, die nur selten zum Einsatz kommen.
Zusätzlich erfolgt die Administration der Server über unterschiedliche Managementkonsolen. Dadurch wird die Verwaltung der Server komplexer, da eine Anmeldung auf verschiedene Konsolen vorgenommen werden muss. Das entsprechende Monitoring erfolgt dann über mehrere Fenster und mit unterschiedlichen Systemen, was eine Reaktion im Fehlerfall durch Unübersichtlichkeit verzögern kann.
Neben der minimalen Auslastung der Server spielt auch deren Alter eine Rolle. So laufen viele Dienste auf alter Hardware, deren Ausfallwahrscheinlichkeit sich durch die lange Laufzeit stark erhöht. Dies steht im Widerspruch mit den Pflichten von *DCS*, die eine dauerhafte Bereitstellung der Firmendienste gewährleisten sollen (siehe Abschnitt 4.1.1). Als Zusammenfassung der bisherigen beschriebenen Punkte, ist dies nochmal in Abbildung 4.1 schematisch zusammengefasst.
Ein weitere Schwierigkeit ist, dass die Möglichkeit der Erweiterung von neuen Servern bisher langwierig und unflexibel ist. „Spontane" Anfragen von Projektleitern bezüglich Serverkapazitäten oder eigenen Servern können bisher nicht in der optimalen Zeit erledigt werden. So ist kein Pool an freien Servern vorhanden und wenn die Hardware beschafft wurde, muss einige Zeit an Installation und Administration aufgewendet werden. Erst dann kann der Server vom Projektleiter genutzt werden. Dies ist mit der momentanen Belastung der Mitarbeiter schwer möglich, kostet des Weiteren Platz im Rechenzentrum, der nur eingeschränkt verfügbar ist. Zusätzlich ist bisher kein Abrechnungssystem für bestimmte Projekte vorhanden, da die bisherige Kostenverteilung über eine Pauschale für alle Abteilungen erfolgt. Ein mögliches Abrechnungssystem wird in dieser Arbeit nicht vorgestellt, da eine Vielzahl von Faktoren und Berechnungsmodi notwendig sind, um eine

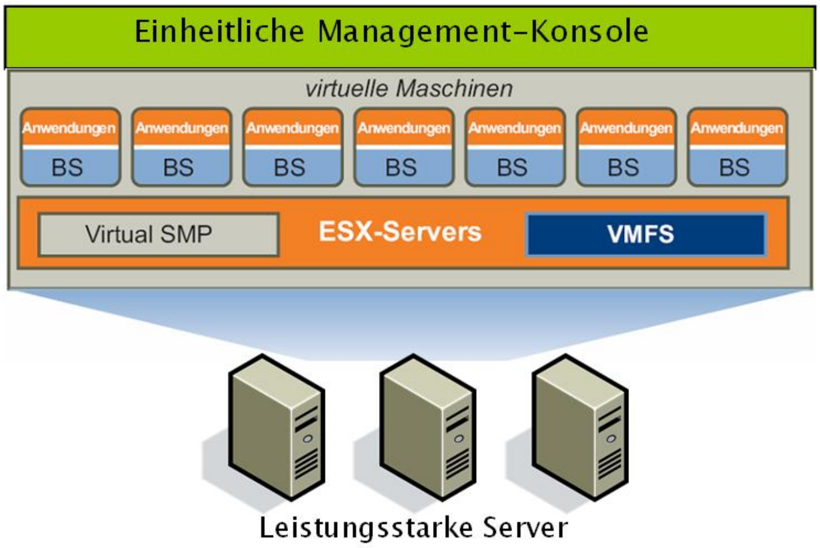

Abbildung 4.2: Gewünschte IT Infrastruktur, die nach der Virtualisierung erreicht werden soll (Quelle: In Anlehnung an VMware Dokumentation [vmh 07])

möglichst exakte und auf die Benutzer angepasste Kostenmodellierung zu gewährleisten. Dies ist ein Thema für eine eigenständige Arbeit, sei aber der Vollständigkeit halber erwähnt.
Zur Lösung dieser Situation werden zwei bestimmte Use Cases im nächsten Abschnitt vorgestellt, die zu einer Verbesserung der Situation führen.

4.1.3 Use Cases zur Verbesserung der IT Landschaft

Die zuvor beschriebene Serverlandschaft zeigt eine Vielzahl von Problemen auf. Durch die Virtualisierung sollen die eingesetzten Server verringert und vereinheitlicht werden. Eine mögliche ideale Umsetzung ist in Abbildung 4.2 zu sehen, bei der alle vorhandenen Server virtualisiert sind und diese nur noch auf wenigen leistungsstarken physikalischen Servern laufen. Zur Verwaltung aller Hosts und deren VMs dient eine zentrale Managementkonsole, die alle wichtigen Punkte übernimmt. Diese Grafik lässt mehrere Punkte außer Acht, die teilweise noch nicht besprochen wurden. So eignet sich nicht jeder Server zur Virtualisierung, weil dieser aus sicherheitsrelevanten Gründen oder auf Grund starker Auslastung, eine eigene physikalische Hardware besitzen muss. Außerdem wurde bereits in Abschnitt 3.3 darauf hingewiesen, dass ein einheitliches Management für den Host und den zugehörigen VMs kaum möglich ist. Zwar gibt es neuere Entwicklungen in diese Richtung (siehe Abschnitt 3.3), aber bisher muss die Verwaltung für die Hosts und VMs noch getrennt betrachtet werden.
Da eine ideale Infrastruktur wie in Abbildung 4.2 nicht möglich ist, gilt es die aktuelle Infrastruktur bestmöglich zu optimieren. Daher werden zwei Anwendungsfälle (Use Cases) vorgestellt, mit denen eine verbesserte IT Infrastruktur erreicht werden kann. Der Aufbau und die Struktur der Use Cases werden nach einem definierten Schema erstellt (vgl. [COC 03]). Wichtig für die Use Cases ist folgende Aussage: „Die Granularität kann verschieden sein. Auf sehr hohem Niveau beschreibt ein Anwendungsfall lediglich sehr grob und abstrakt, was passiert. Die Technik des Anwendungsfall-Schreibens kann jedoch bis auf die Ebene von IT-Prozessen verfeinert werden, so dass das Verhalten einer Anwendung detailliert beschrieben wird. Dies widerspricht der ursprünglichen Intention von Use Cases, ist aber manchmal zweckmäßig [COC 03].“ Dies bedeutet, dass die folgenden Use Cases keine genauen Abläufe beschreiben, sondern es folgt eine grobe Skizzierung, wie vorgegangen wird. Die genaue Umsetzung der Use Cases anhand des Konzeptes erfolgt in Kapitel 6.

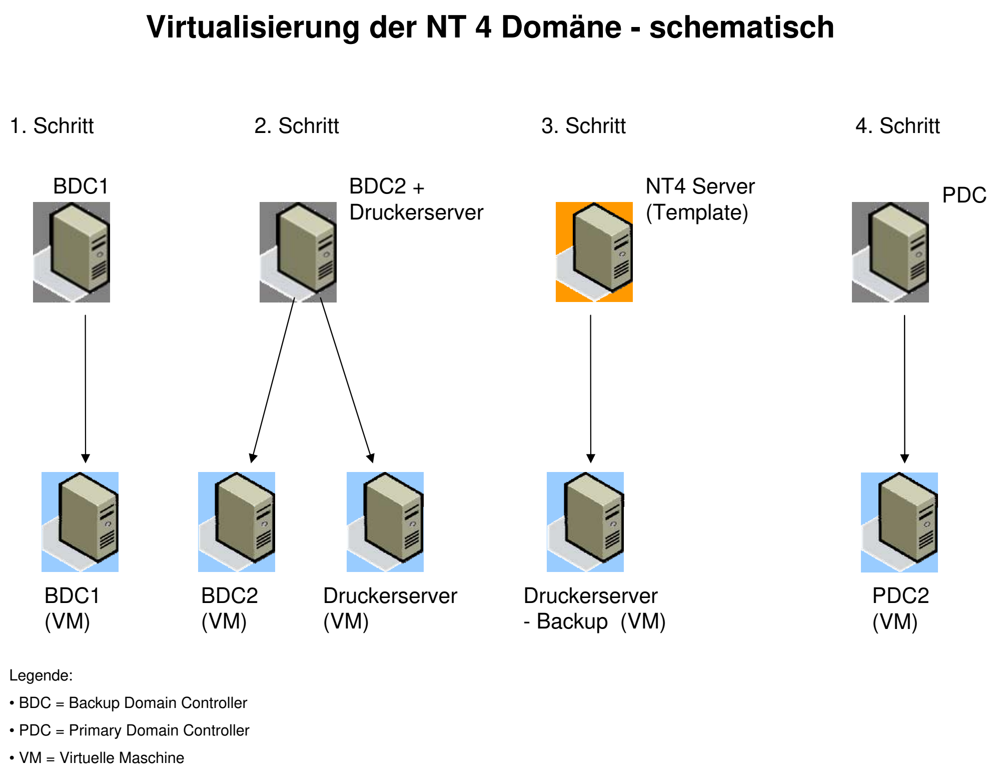

Abbildung 4.3: Grafische Darstellung des Use Cases zur Virtualisierung der NT4 Domäne

Use Case 1: Virtualisierung einer NT4 Domäne

Im ersten Use Case handelt es sich um die Virtualisierung einer alten NT4 Domäne. Dabei wurde die Domäne vor einiger Zeit abgelöst, läuft aber immer noch parallel, weil sie für bestimmte Teilbereiche noch benötigt wird. Basis dafür ist eine veraltete, unsichere Hardware, die kaum die bereitstehenden Ressourcen der Server nutzt. Die Server sind bisher an mehrere Managementkonsolen angeschlossen, wodurch diese Domäne nicht einheitlich betreut werden kann. Wie in Abbildung 4.3 zu sehen ist, handelt es sich um einen primären Domänencontroller (PDC) und zwei Backup Domänencontroller (BDC). Zusätzlich ist bei der Virtualisierung dieser Server zu beachten, dass eine der Maschinen gleichzeitig als Druckerserver arbeitet. Gibt es nun Probleme mit dem Druckerserver, schlimmstenfalls einen Ausfall der Maschine, so betrifft dies auch den BDC (et vice versa). Mit Hilfe der Virtualisierung soll dieses Problem gelöst werden, indem jede Funktion auf einer eigenen virtuellen Maschine läuft. Eine geeignete Aufteilung muss entsprechend vorgenommen werden. Des Weiteren wird ein neuer virtueller Server auf Basis von NT4 erzeugt, der für interne Abläufe benötigt wird. Nach Ablauf des Use Cases laufen im Erfolgsfall alle physikalischen Server als virtuelle Maschinen. Der Anwendungsfall wird nach dem Schema von [COC 03] vorgestellt:

Name:
Virtualisierung und Optimierung der kompletten NT4 Domäne

Beschreibung:
Es gilt, die komplette vorhandene NT4 Domäne zu virtualisieren und die bisherigen Server alle als VMs laufen zu lassen. Dies wird Schritt für Schritt durchgeführt, um die Server einzeln in die virtuelle Umgebung aufzunehmen.

Akteure:

- Administrator (übernimmt die Virtualisierung und ggf. Neukonfiguration)
- User (benutzen ununterbrochen die zur Verfügung stehenden Dienste der Server und müssen ggf. über Ausfallzeiten benachrichtigt werden)

Auslöser:
Die alte und unsichere Hardware soll durch eine stabilere Umgebung ersetzt werden. Durch den Abbau an Hardware verringert sich die Komplexität im Rechenzentrum. Zusätzlich ist eine Zeiteinsparung (⇒ Kosteneinsparung) durch einfachere Administration der VMs möglich.

Vorbedingungen:
Die Virtualisierungsumgebung muss bereits installiert und entsprechend konfiguriert sein. Die Server und die darauf laufenden Betriebssysteme können mit der eingesetzten Umgebung virtualisiert werden. Des Weiteren eignen sich die Server auf Grund ihrer geringen Systemauslastung und Hardwareanforderungen zur Virtualisierung. Kommt es zu geplanten Ausfallzeiten wird der User entsprechend vorher informiert.

Nachbedingungen:
Die volle Funktionalität muss bei allen VMs gewährleistet sein. Der User darf daher keine negativen Unterschiede zur vorherigen Situation bemerken. Diese VMs müssen unter einer Managementkonsole administrierbar und ansteuerbar sein. Alle Schritte, die zu der virtualisierten NT4 Domäne geführt haben, sind nachvollziehbar dokumentiert.

Ablaufschritte:
Der Ablauf der Virtualisierung läuft in 4 Schritten ab. Diese werden im Folgenden beschrieben:

1. Virtualisierung eines BDC Servers (siehe Schritt 1 bei Abb. 4.3) (⇒ dient als erster Test, da im Fehlerfall kein Dienstausfall zu befürchten ist.)
2. Virtualisierung eines zweiten Servers und Aufspaltung des Drucker- und des BDC-Servers (siehe Schritt 2 bei Abb. 4.3) (⇒ jeder Dienst erhält einen eigenen virtuellen Server (wg. Ausfallsicherheit).)
3. Verwendung eines Templates auf Basis von *Windows NT4 Server* für einen Backupserver (siehe Schritt 3 bei Abb. 4.3) (⇒ wird für interne Umstellungen benötigt)
4. Virtualisierung des PDC Servers (siehe Schritt 4 bei Abb. 4.3) (⇒ kein physikalischer Server ist mehr vorhanden. Alle Server sind virtualisiert.)

Ausnahmen:

- Sollte nach 1.) die Virtualisierung nicht erfolgreich sein, muss ggf. geprüft werden, ob die verwendete Virtualisierungstechnologie weiter verwendet werden soll.
- Sollte nach 2.) die Aufspaltung nicht funktionieren, muss überlegt werden, ob diese anders gewährleistet werden kann oder ob diese überhaupt durchgeführt wird.
- Bei 4.) muss überlegt werden, ob alle Maschinen virtualisiert werden sollen oder ob eine physikalische Maschine zur Sicherheit vorhanden bleiben soll (bzgl. „Single Point of Failure” der wenigen physikalischen Server, auf denen die VMs laufen).

Der komplette schematische Ablauf der einzelnen Schritte wird grafisch in Abbildung 4.3 vorgestellt.

Im nächsten Abschnitt wird der zweite Use Case vorgestellt.

Use Case 2: Bereitstellung von virtuellen Servern auf Basis von Templates

Im zweiten Use Case geht es um die Verbesserung der Service Qualität auf Grund einer flexiblen Reaktion bei der Anfrage von Hardwarekapazitäten. Bisher ist dies schwer möglich, denn es erfordert eine lange Vorlaufzeit durch die Bestellung, Aufbau, Installation und Konfiguration der entsprechenden Hardware. Auch eine Erweiterung von bereits vorhandenen Kapazitäten ist mit der momentanen IT Landschaft nicht möglich. Deshalb kann auf einen Kapazitätsengpass momentan nicht so reagiert werden, wie es teilweise notwendig ist. Aus diesem Grund werden die Server entsprechend dimensioniert, so dass sie auch bei starken Auslastzeiten nicht an ihre Grenzen stoßen. Die meiste Zeit nutzen sie aber ihre Ressourcen nicht aus, können aber auch nicht für andere Aufgaben eingesetzt werden. Im hier vorliegenden Fall wäre es wünschenswert, wenn bei Anfrage eines Projektleiters, nicht genutzte Ressourcen bereitgestellt werden können. Der konkrete Anwendungfall sieht dann folgendermaßen aus:

Name:
Bereitstellung von virtuellen Servern für Projektanfragen

Beschreibung:
Bei Anfrage von Projekten für Serverkapazitäten, die für bestimmte Simulationen, Tests oder Entwicklungsumgebungen benötigt werden, können nun einfach und schnell entsprechende Server (falls Kapazitäten vorhanden sind) bereitgestellt werden. Ein entsprechendes Kostenmodell muss dazu überlegt werden (ist aber nicht Gegenstand der Arbeit).

Akteure:

- Administrator (erhält die Anfrage und richtet, falls möglich, die gewünschten Kapazitäten ein)
- Projektleiter (benötigt meist schnell einen Server, um notwendige Programme, Tests, etc. ausführen zu können)

Auslöser:
Anfrage eines Projektleiters nach einem Server

Vorbedingungen:
Der Administrator hat erfolgreich geprüft, dass die benötigten Kapazitäten im Moment und für den gewünschten Zeitraum zu Verfügung stehen. Des Weiteren ist eine entsprechende Kostenabrechnung und gewisse Dienstgütevereinbarungen (SLAs - Service Level Agreements) zwischen beiden Seiten (Administrator und Projektleiter) erfolgreich geklärt und vertraglich festgehalten worden. Die Bereitstellung des Servers erfolgt nach dem Dienstgut „best effort". Ein Servertemplate ist in der Virtualisierungsumgebung vorhanden (ansonsten siehe „Alternative Ablaufschritte").

Nachbedingungen:
Der Projektleiter hat entsprechenden Zugriff auf den Server und kann dort seine festgelegten Tätigkeiten ausführen. Der bereitgestellte Server erfüllt die vorher festgelegten Kriterien (bzgl. Hauptspeicher, Prozessor, Sekundärspeicher, Ausfallsicherheit, etc.).

Ablaufschritte:

1. Das Template wird in der Managementkonsole zu einer VM umgewandelt und die Einstellungen der neuen VM werden entsprechend der festgelegten Kriterien (SLAs) vorgenommen
2. Die VM wird gestartet, um die Funktionalität zu testen und richtet die Zugriffsrechte im zugrundeliegenden Betriebssystem für den Projektleiter ein
3. Der Projektleiter erhält die entsprechenden Informationen für den Server (Name des Servers, Zugangsdaten, etc.) und überprüft, ob die zuvor festgelegten Punkte (SLAs) übereinstimmen
4. Der Projektleiter gibt dem Administrator ein positives Feedback zurück

   Erweiterungspunkte:
   Nach Ablauf des Vertrages wird die VM wieder entsorgt:

5. Der Administrator teilt dem Projektleiter mit, dass die Laufzeit vorbei ist
6. Der Projektleiter überprüft, ob alle Daten auf Netzlaufwerken gesichert sind und gibt das OK zur Entsorgung des Servers (laut Firmen-Policy dürfen sich keine Daten auf den lokalen Platten des Servers befinden, sondern es müssen alle Projektdaten auf Netzlaufwerke gespeichert werden. Eine entsprechende Datensicherung erfolgt über die Backupstrategien der Netzlaufwerke.)
7. Die VM wird über die Management Konsole heruntergefahren und nach einer vordefinierten Zeit (ggf. wie im Vertrag definiert wurde) gelöscht oder, falls vertraglich festgehalten, zuvor komplett gesichert (⇒ die Ressourcen stehen nach dem dauerhaften Herunterfahren für andere VMs zur Verfügung)

<u>Alternative Ablaufschritte:</u>
sollte noch kein Template mit dem gewünschten Server-Betriebssystem vorhanden sein, muss dieses erstellt werden, damit die Vorbedingung erfüllt ist:

1. Erzeugung einer VM in der Managementkonsole
2. Konfiguration der gewünschten Einstellungen und Auswahl des zu installierenden BS
3. Installation des Betriebssystems anhand dessen Handbuches
4. Konfiguration des Netzwerkes, der Zugriffssteuerung etc. nach der Installation das BS
5. Umwandlung der VM in ein Template
6. Dokumentation bzgl. des neuen Templates aktualisieren (⇒ Ab sofort steht nun das Template mit dem gewünschten Betriebssystem bereit)

Mit den beiden Use Cases ergeben sich gewisse Anforderungen, die erreicht werden sollen. Zusätzlich gibt es noch weitere Anforderungen, die an die Virtualisierung gestellt werden, die bisher noch nicht genannt worden sind. Um welche es sich dabei handelt und wie diese zu bewerten sind, wird im nächsten Abschnitt behandelt.

4.2 Anforderungen an ein Virtualisierungskonzept

Wie bereits mehrfach erwähnt, ist die größte Anforderung an die Virtualisierung die Kosteneinsparung und eine verbesserte Servicequalität. Dies sind aber sehr vage Begriffe und müssen noch detaillierter aufgeteilt werden. Zusätzlich ist nicht jede Anforderung gleich wichtig, so dass eine Gewichtung für jede Anforderung eingeführt werden muss. Dementsprechend kann bei einer Umsetzung festgestellt werden, ob diese erfolgreich war, wenn alle wichtigen Anforderungen erfüllt wurden. Ist eine der weniger priorisierten Anforderungen nicht erfüllt worden, ist dies von geringerer Bedeutung, als wenn eine wichtige Anforderung nicht abgedeckt wurde. Daher werden die kommenden Anforderungen in drei Gruppen unterteilt: alle Anforderungen der ersten Gruppe (I) sind unverzichtbar und sollten diese nicht alle erfüllt werden können, gilt das Virtualisierungskonzept als gescheitert. In der zweiten Gruppe (II) befinden sich alle Anforderungen die als „sehr wichtig” betrachtet werden. Diese müssen nicht enthalten sein, sind aber für ein praxistaugliches Konzept von Bedeutung, denn ohne diese Anforderungen wird es kaum eingesetzt. Die letzte Gruppe (III) beinhaltet Anforderungen, die das Konzept sinnvoll ergänzen und abrunden. Diese erleichtern das Arbeiten, sind aber nicht unbedingt notwendig. Neben dieser Einordnung erfolgt eine Kategorisierung der spezifischen Anforderungen in vier Hauptanfoderungen: Dies sind die Kategorien „Kosteneinsparung”, „Einfacheres Management”, „Flexiblere Reaktion” und „Service Qualität”. Nicht alle Anforderungen sind eindeutig zuweisbar, da eine verbesserte Handhabung einerseits zu einer verbesserten Servicequalität führen kann, andererseits es sich um eine Kosteneinsparung handelt, wenn der Administrator weniger Zeit für das Management aufwenden muss. Dennoch wurde die Kategorisierung so gewählt, um einen besseren Überblick zu gewinnen und um aufzuzeigen, welche unterschiedlichen Ansprüche an die Virtualisierung gestellt werden. Im nächsten Absatz werden alle Kategorien mit ihren jeweiligen Anforderungen genannt. In Klammern steht die jeweils zugeordnete Gruppe. Nach der Auflistung wird jede Kategorie im Detail betrachtet:

Kategorie	Anforderung mit zugeordneter Gruppe
Kosteneinsparung:	• Verwendung von mehreren Betriebssystemen und VMs auf einem physikalischen Server (I) • Abbau von Server und Hardwarekomponenten (II)
Einfacheres Management:	• Zeiteinsparung durch einfachere und komfortablere Handhabung der VMs über eine zentrale Konsole (I) • Komplette und funktionierende Konvertierung von physikalischen Servern und deren Dienste (II) • Klonen von virtuellen Maschinen (II) • Verschiebung von VMs im laufenden Betrieb (III) • Individuelle Vergabe von Benutzerrechten in der Managementkonsole (III) • Sichere Konfiguration und sicheres Testen bestimmter Funktionen (durch vorheriges Erstellen von Snapshots) (III)
Flexiblere Reaktion:	• Schnellere Bereitstellung von Servern bei Anfragen oder in Stoßzeiten (II) • Individuelle Konfiguration der virtuellen Maschinen nach deren Anforderungen (auch nach der Installation einer VM kann z.B. der Hauptspeicher noch angepasst werden, wie dies auch bei einem physikalischen Server passieren kann) (II) • Verwendung von Templates für bestimmte Betriebssysteme und Konfigurationen (III)
Service Qualität:	• Gleiche Funktionalität der virtuellen Maschinen gegenüber den bisherigen Maschinen (I) • Zuverlässige Sicherung und Rücksicherung von virtuellen Maschinen (I) • Gewährleistung der Sicherheit jeder VM (sie wird nicht von anderen VMs beeinflusst) (I) • Trotz mehrerer VMs auf einem physikalischen Server sind die wenigen Netzwerkschnittstellen kein „Flaschenhals” für die jeweiligen Anwendungen (I) • Das Leistungsverhalten der virtuellen Maschinen weist keine signifikanten Unterschiede gegenüber den physikalischen Maschinen auf (II) • Gewährleistung von Hochverfügbarkeit der Hosts und der VMs (II) • Bessere Lastverteilung der virtuellen Server (II) • Notwendige Updates der Virtualisierungsumgebung können ohne Beeinträchtigung der virtuellen Maschinen installiert werden (II) • Erstellen eines neuen virtuellen Servers soll in Anlehnung an ITIL vorgenommen werden (II) • Erfolgreiche Anbindung von verschiedenen Datastores (lokale Platte, SAN Anbindung, iSCSI Verbindung) (III)

Tabelle 4.1: Liste der Anforderungen in den vier Kategorien (In Klammern ist die jeweilige Gruppe genannt)

Bevor auf die einzelnen Kategorien und die zugehörigen Gruppen eingegangen wird, sei an dieser Stelle nochmal darauf hingewiesen, dass die Gruppierung sich an der Virtualisierung einer heterogenen Infrastruktur orientiert. Für dieses Szenario sind bestimmte Anforderungen von größerer Bedeutung, als in anderen Fällen. So ist es bei einem Einsatz von verschiedenen Betriebssystemen von großer Bedeutung, dass diese auch alle als virtuelle Maschinen laufen. Geht es um die Virtualisierung einer Simulationsumgebung, die grundsätzlich nur ein Betriebssystem verwendet, ist der Punkt von weitaus geringerer Bedeutung. Daher ist bei der Priorisierung im Folgenden zu beachten, dass sich dies auf den Anwendungsfall einer heterogenen Landschaft, wie in Abschnitt 2.1 besprochen, bezieht.

In der ersten Kategorie geht es um die direkte Kosteneinsparung durch den Abbau von Komponenten und durch die Konsolidierung von Servern. Mit diesem Vorteil werben alle Virtualisierungslösungen, doch muss dies etwas differenzierter betrachtet werden. Wenn es mit dem Virtualisierungskonzept nicht möglich ist, mehrere VMs mit unterschiedlichen Betriebssystemen auf einem physikalischen Host zu betreiben, dann ist das Konzept gescheitert. Dies ist auch der Grund, warum diese Anforderung der Gruppe I zugehört. Der Punkt bezüglich Abbau von Hardwarekomponenten ist nicht ganz so einfach, wie es scheint. Zwar werden im Idealfall viele alte Server virtualisiert und bei Erfolg entsorgt, doch müssen oft zuerst leistungsstarke Server gekauft werden, die dann mehrere VMs aufnehmen können. Zusätzlich kommt eine Verkabelung dieser Server mit dem Datenspeicher (meist: Fibre Channel) hinzu, wodurch neue Hardwarekomponenten (spezielle Kabel und Switches) ins Spiel kommen. Auch werden nur Server virtualisiert, die die meiste Zeit kaum ihre Kapazitäten nutzen. Hosts, die ihre zugrundeliegende Hardware voll ausnutzen, werden auch weiterhin als eigenständige Server betrieben, da sie sonst als VM ein Großteil der Ressourcen nutzen. Dies macht eine Virtualisierungsumgebung ineffektiv wenn auf dem Host nur ein bis zwei VMs laufen können. Aus den genannten Gründen der Erstanschaffung und Zusatzverkabelung wird der Abbau von Hardwarekomponenten der zweiten Gruppe zugeordnet. Damit ist dies immer noch ein sehr wichtiger Punkt, der in der Praxis eine große Rolle spielt, aber nicht essenziell für die Virtualisierung ist.

Mit der zweiten Kategorie wird das Management der virtuellen Maschinen bedacht. Dabei ist die zentrale Managementkonsole von größter Bedeutung, denn dadurch können die VMs wesentlich einfacher überwacht, gesteuert und verwaltet werden. Dieser Punkt ist indirekt die größte Kosteneinsparung und hätte daher auch zur ersten Kategorie gehören können. Dies liegt daran, dass durch einen geringeren Zeitaufwand auch weniger „Manpower" benötigt wird, um die Server zu administrieren. Für den Administrator ist aber eine leichtere Handhabung von Bedeutung, denn so bleibt ihm mehr Zeit für andere Aufgaben und er hat im Fehlerfall über die Managementkonsole alle VMs im Überblick. Dies ist ein unverzichtbarer Punkt und gehört daher in die erste Gruppe. Die nächsten beiden Anforderungen in der oberen Liste sind für die Einrichtung und den Betrieb der Virtualisierungsumgebung von Bedeutung. Mit entsprechenden Konvertern können die physikalischen Server direkt in eine VM umgewandelt werden, wodurch auch wieder Zeit und dadurch Geld gespart wird. Der Aufwand ist wesentlich geringer, als wenn die VM neu installiert und eingerichtet werden muss. Dasselbe gilt für das Klonen von VMs, indem identische Server nicht jedes Mal neu installiert werden müssen. Daher werden diese Ansprüche zu Gruppe II zugeordnet. Die letzten drei Anforderungen dieser Kategorie sind der Gruppe III zugeordnet, da diese als Abrundung einer Virtualisierungsumgebung gesehen werden. Das Verschieben von VMs vereinfacht die Handhabung beispielsweise im Wartungsfall, wenn die VM nicht erst heruntergefahren und auf einem anderen Server wieder hochgefahren werden muss. Dasselbe gilt für die Vergabe von Benutzerrechten, die eine individuellere Administration ermöglicht. Dies kann im Notfall aber auch anders gelöst werden. Das sichere Testen durch Snapshots ist eine einfache Methode, um gefahrlos Applikationen oder Patches zu testen. Dies kann beispielsweise auch auf einer geklonten Maschine durchgeführt werden, die im Fehlerfall wieder gelöscht werden kann.

Bei der „flexibleren Reaktion" handelt es sich um eine Unterkategorie von „Service Qualität". Eine bessere Reaktion auf Kapazitätsanfragen durch Benutzer steigert verständlicherweise deren Arbeitsqualität. Auch bei Ressourcenengpässen kann ein Server geklont und entsprechend eingesetzt werden. Diese Optimierung bei der Reaktion ist eine wichtige Anforderung und wird daher in Gruppe II eingegliedert. Eine weitere Optimierung kann nicht nur durch die Bereitstellung neuer VMs gewährleistet werden, sondern auch, indem die vorhandene virtuelle Maschine angepasst wird. Ist für eine bestimmte Zeit die Kapazität unzureichend, kann die VM durch Erhöhung des RAMs oder durch den Zugriff auf einen weiteren CPU-Kern mehr Ressourcen erhalten. Auch das Hinzufügen einer weiteren virtuellen Platte kann hilfreich sein, wenn erhöhtes Datenaufkommen zu erwarten ist. Dies gilt auch für den entgegengesetzten Fall, wenn eine VM bei der Installation mehr Ressourcen erhalten hat, als sie eigentlich benötigt. Die VM kann entsprechend angepasst werden und es stehen für andere virtuelle Maschinen wieder mehr Ressourcen zur Verfügung. Diese ständige Anpassung spiegelt einen wichtigen Bedarf wider, der daher in die zweite Gruppe aufgenommen wird. Eine sinnvolle Ergänzung zur Steigerung der Flexibilität, ist die Erstellung von Templates. Für bestimmte Betriebssysteme, die im Unternehmen oft verwendet werden, ist es sinnvoll, eine Rohfassung dieses Betriebssystems anzulegen. Bei Bedarf wird aus dem Template eine VM erzeugt und entsprechend angepasst. Daraufhin kann noch schneller auf standardisierte Anfragen reagiert werden. Dies ist eine sinnvolle Erweiterung, die in die dritte Gruppe fällt.

Wie in der Auflistung zu sehen ist, beinhaltet die letzte Kategorie die meisten Anforderungen der Gruppe I. Dies hängt damit zusammen, dass sich die Steigerung von Service Qualität auch wieder indirekt auf die Kostensenkung auswirkt. Denn durch ein verbessertes Angebot gibt es in der Regel weniger Ausfallzeiten (dadurch weniger Leerlaufzeiten für die Benutzer) und performantere Applikationen, die ein schnelleres Arbeiten ermöglichen. Der erste Punkt der Liste ist daher unverzichtbar, denn wenn die VM nicht dieselbe Funktionalität wie eine physikalische Maschine ermöglicht, ist dies eine Einschränkung der Service Qualität. Auch muss es eine zuverlässige Datensicherung geben, die sowohl sicher speichert, als auch im Notfall korrekt wiederherstellt. Daher muss ein Sicherungskonzept für die virtuellen Maschinen vorhanden sein, denn der Verlust von Daten (trotz Sicherungskonzept) ist nicht akzeptabel. Neben der Sicherung muss auch die Sicherheit der VMs gewährleistet sein. Dabei gibt es mehrere Punkte zu beachten, die bereits in Abschnitt 3.3.4 besprochen wurden. So gilt es beispielsweise zu gewährleisten, dass eine VM nicht von einer anderen VM ungewollt beeinflusst wird. Als letzte Anforderung der ersten Kategorie dürfen die Netzwerkanschlüsse kein Flaschenhals für die Server und deren Anwendungen sein. So muss gewährleistet sein, dass der Netzverkehr entsprechend eingeteilt wird und es bei einem besonders starken Anstieg ggf. Warnmeldungen an den Administrator gibt. Blockiert eine VM durch Überlastung den Netzverkehr, kommt dies einem „Denial of Service" für andere Server gleich. Daher muss mindestens gewährleistet werden, dass ein Server immer erreichbar ist, auch wenn bei zu vielen VMs auf einem Host der Netzverkehr eingeschränkt sein kann. Die bisher genannten Anforderungen sind notwendig, um eine Virtualisierung einzusetzen. Die folgenden vier Anforderungen gehören der Gruppe II an und sind für einen praxistauglichen Einsatz von großer Bedeutung. Über die Gewährleistung von Hochverfügbarkeit wurde bereits indirekt in Abschnitt 3.3 gesprochen. So bietet das Management idealerweise Verfahren der Hochverfügbarkeit für Hosts und VMs an. Ein Ausfall eines Hosts ist meist wesentlich schlimmer, da dadurch mehrere VMs betroffen sind, dennoch muss sowohl für den Host, als auch für die VM Hochverfügbarkeit herrschen, um entsprechende Service Qualität anzubieten. Auch bei der Lastverteilung handelt es sich um eine Verbesserung der Qualität, denn es herrscht weniger die Gefahr, dass mehrere betriebene VMs an die Grenzen des physikalischen Hosts stoßen. Eine besonderer Punkt ist die Anforderung, dass der Ablauf der Virtualisierung eines neuen Servers sich an der ITIL orientieren soll. Was dies bedeutet und was dabei beachtet werden muss, wird in einem gesonderten Abschnitt behandelt (siehe 4.3). Als letzte Anforderung dieser Kategorie gilt die erfolgreiche Anbindung an verschiedene Datenspeicher. Dies ist sinnvoll, wenn nicht nur eine teure SAN / Fibre Channel Verbindung aufgebaut werden soll, sondern für bestimmte Bereiche auch eine Anbindung mittels iSCSI ausreicht. Mit der Entscheidung, welche Anbindung verwendet werden soll, gestaltet sich die Virtualisierungsumgebung flexibel und lässt je nach Situation die erwünschte Möglichkeit zu.

Insgesamt bieten die hier vorgestellten Anforderungen einen großen Katalog, an dem sich ein Virtualisierungskonzept messen muss. Durch die unterschiedliche Gewichtung können diese auch später verschieden bewertet werden. So ist durch die Gruppeneinteilung festgelegt, dass sich die erste Gruppe unverzichtbar im Konzept wiederspiegeln muss. Ohne Gruppe zwei ist eine praktische Umsetzung kaum möglich, die Anforderungen können aber im äußersten Notfall und mit entsprechenden Einschränkungen in der Funktionalität weggelassen werden. Gruppe drei bietet sinnvolle Ergänzungen, die bei der Produktauswahl eine bestimmte Richtung vorgeben können. Wird durch ein Produkt die Anforderung der dritten Gruppe erfüllt, muss erwogen werden, ob es dies auch wert ist. Meist sind diese Ergänzungen mit Zusatzkosten verbunden, wodurch mittels Kosten-/Nutzenrechnung festgestellt werden muss, ob sich der Zukauf lohnt.
Wie bereits erwähnt, lautet eine der Auflagen, die Virtualisierung mit Hilfe von ITIL zu gestalten. Bisher fehlt aber eine Erklärung, um was es sich bei ITIL handelt und warum ITIL Prozesse eine verbesserte Service Qualität versprechen. Diese und weitere Punkte werden im nächsten Abschnitt vorgestellt und diskutiert.

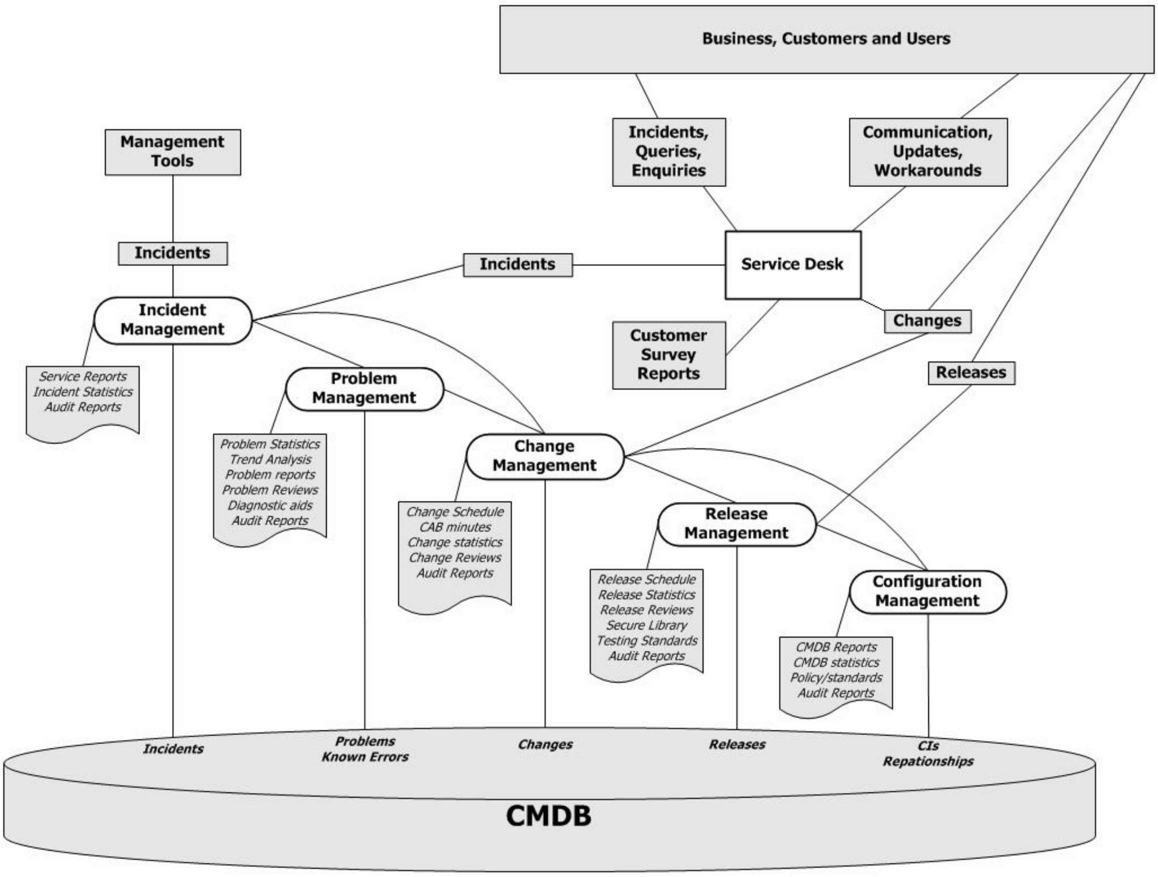

Abbildung 4.4: Überblick über die einzelnen Schritte und Verbindungen bei „Service Support" (Quelle: [ITIL 07])

4.3 Gestellte Anforderung: Abbildung der Use Cases nach ITIL

Im vorherigen Abschnitt lautete die Anforderung: „Erstellen eines neuen virtuellen Servers soll in Anlehnung an ITIL vorgenommen werden". Dies wird für die vorliegende Arbeit noch erweitert, denn auch die speziellen Use Cases der Astrium GmbH (siehe Abschnitt 4.1.3) werden mit der ITIL abgebildet. So wird gezeigt, dass mit Hilfe von ITIL nicht nur die allgemeine Anforderung, sondern auch konkrete Anwendungsfälle entsprechend modelliert werden können. Bevor es aber soweit ist, wird im nächsten Punkt zuerst die ITIL vorgestellt. Diese beinhaltet eine Vielzahl an Prozessen und stellt ein „Best Practise" Framework für das IT Service Management dar. Es muss eine Einordnung in die hier notwendigen Bereiche erfolgen. Im darauffolgenden Abschnitt wird der Ablaufprozess bei der Virtualisierung beschrieben, so dass er mit der ITIL in Einklang steht. Welche Vorteile dies bringt und welche Erweiterungen gegebenenfalls gemacht werden müssen, wird entsprechend beschrieben. Im letzten Abschnitt erfolgt dann die Einteilung der Use Cases nach ITIL. Hier ändern sich manche Abläufe, doch insgesamt sind diese sehr ähnlich zu dem zuvor beschriebenen Prozess. Mit dieser Zuordnung ist diese besondere Anforderung ausreichend behandelt worden und die ermittelten Informationen fließen in das Konzept ein.

4.3.1 ITIL - IT Service Management

Auf Grund der niedrigen Qualität von IT Services veranlasste die britische Regierung in den 80er Jahren eine Verbesserung. Die CCTA (Central Computer and Telecommunications Agency; jetzt OGC (Office of Governance Commerce)) erhielt den Auftrag, ein Verfahren für den zweckmäßigen und wirtschaftlichen Einsatz von IT Mitteln in den Ministerien und anderen Organisationen der britischen Regierung zu entwickeln [ITIL 02].

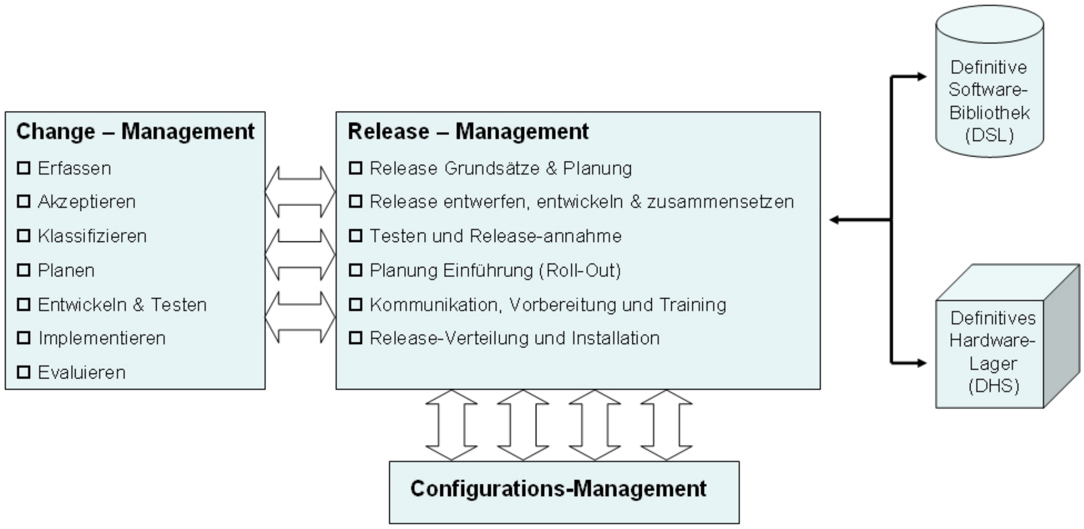

Abbildung 4.5: Abläufe und die jeweiligen Beziehungen von Change- und Release-Management (Quelle: [ITIL 02])

Dabei wurde nach Verfahren gesucht, die unabhängig von bestimmten Firmen oder Dienstleistern waren. Das Ergebnis dieses Auftrages wurde in der ITIL (Information Technology Infrastructure Library) festgehalten. ITIL ist aus einer Sammlung von „Best Practices" entstanden, die im Bereich der IT Services Anwendung fanden [ITIL 07]. Es handelt sich um ein Regelwerk, dass die für den Betrieb einer IT Infrastruktur notwendigen Prozesse beschreibt. Diese Prozesse bestehen aus ausführlichen Checklisten, Aufgaben, Verfahren und Zuständigkeiten, die je nach Bedarf in der IT Organisation angepasst und angewandt werden können. Wie bereits erwähnt, orientiert sich die ITIL nicht an einer bestimmten Technologie, sondern beschreibt die Prozesse so allgemein wie möglich. Welche Technik zum Einsatz kommt, um die Prozesse umzusetzen, entscheidet die jeweilige IT Organisation für sich. Einige Firmen, wie HP, Microsoft oder IBM, bieten daher Tools und Programme an, die auf Basis von ITIL arbeiten (vgl. [BHea 03]). Die ITIL wurde seit den 80er Jahren mehrfach überarbeitet und liegt mittlerweile in der Version 3 (V3) vor. Diese ist vor kurzem erschienen und hat eine Vielzahl an Prozessen gegenüber der Vorgängerversion verändert. Da die Version 2 (V2) lange Zeit Bestand hatte und es zu V3 bisher noch keine ausreichende Dokumentation gibt, beziehen sich folgende Aussagen immer auf Version 2. Wird in den nächsten Abschnitten von ITIL Prozessen gesprochen, dann gilt dies gegenüber V2 (Informationen über die Unterschiede können unter [ITIL 07] eingesehen werden).
ITIL V2 beschreibt ein Prozess Framework für das IT Service Management (ITSM) zur Planung, Steuerung, Kontrolle und Koordination aller IT relevanten Aktivitäten und Ressourcen mit dem einzigen Ziel, die operativen und strategischen Vorhaben eines Unternehmens zu erreichen [ITIL 07]. Ziele des Service Management sind die Ausrichtung der IT Service auf aktuelle und zukünftige Anforderungen des Unternehmens, Optimierung der Qualität und Reduzierung der langfristigen Kosten der Service Tätigkeit (vgl. [ITIL 07]). Dabei unterteilt sich ITSM in drei Ebenen: Die strategische, die taktische und die operationelle Ebene (vgl. [ITIL 07]). Die für die nächsten Abschnitte wichtige Ebene ist die operationelle und nennt sich in ITIL „Service Support". Dieser steht für den effizienten Betrieb von IT Dienstleistungen. Die wirkungsvolle Betreuung von IT Services wird durch die Verknüpfung folgender IT Prozesse gewährleistet: Incident, Problem, Configuration, Change und Release Management. Ein genauer Zusammenhang zwischen den verschiedenen Prozessen ist in Abbildung 4.4 zu sehen. Besonders hervorzuheben sind die Prozesse des Problem und des Change Managements. Diese beiden Teilbereiche bestehen aus mehreren Punkten, die in wechselseitiger Beziehung zueinander stehen (siehe Abbildung 4.5). Wie in der Abbildung zu sehen ist, enthalten diese eine Vielzahl von Möglichkeiten und Abläufen, die für eine VM genauer betrachtet werden müssen.

4.3.2 Lebenszyklus für einen virtuellen Server

Wie bereits besprochen ist das Ziel von ITIL, Abläufe in Prozesse zu fassen, um eine bessere Servicequalität zu bieten. Wichtiger Nebeneffekt ist durch den festgelegten Ablauf, dass alle Informationen in (mehreren) Datenbanken gespeichert sind. So entfallen umständliche Listen, die der Administrator führen muss. Durch diese Vorgänge gehen keine Informationen verloren. Die komplette IT Infrastruktur ist entsprechend in der Datenbank (bei ITIL: CMDB (Configuration Management Database)) modelliert, dadurch lassen sich Veränderungen besser dokumentieren. Durch entsprechende Suchanfragen an die CMDB können Schwachstellen und Probleme ermittelt werden, ohne dass Informationen nicht berücksichtigt wurden (vgl. [ITIL 02]). Dies ist beispielsweise bei der Einführung einer Virtualisierungslösung von Vorteil, wenn anhand dieser Datenbank ermittelt werden kann, wo ein Einsatz sinnvoll ist. Der Aufwand zur Einrichtung einer CMDB richtet sich an den gewünschten Informationsumfang, der dort gespeichert werden soll. Wenn jede Hardwarekomponente im Unternehmen (wie Bildschirme, Drucker, Kabel, PCs, Server, etc.) aufgenommen werden soll, ist dies wesentlich komplexer, als wenn die Datenbank z.B. nur für das Rechenzentrum erstellt wird. Doch auch dies ist keine leichte Aufgabe, aber für die Verwendung bei der ITIL unerlässlich[1].
Bevor der Lebenszyklus eines virtuellen Servers anhand der ITIL vorgestellt wird, muss noch ein Detail geklärt werden. Alle Veränderungen oder Anfragen müssen korrekterweise über das Service Desk laufen und dieses informiert auch die Personen über die erfolgten Veränderungen. Dieser sogenannte „Single Point of Contact" (SPOC) (vgl. [BHea 03]) nimmt alle Anfragen entgegen und leitet dies an die entsprechende Stelle weiter. Dies gilt auch für Kapazitätsanfragen oder bei neuen Servern, die diese Anfragen an das Change Management weitergeben (siehe Verbindung zwischen „Service Desk" und „Changes" in Abbildung 4.4). In den folgenden Abläufen wird zur Vereinfachung die Veränderung direkt vom Administrator gestellt. Für die Vollständigkeit kann bei Bedarf aber am Anfang und auch am Ende der Schritt über das Service Desk hinzugefügt werden.

Existiert nun der Bedarf eines neuen virtuellen Servers wird ein Request for Change (RfC) vom Administrator an das Change Management (kurz: ChM) gestellt (vgl. [ITIL 02]). Dieses erfasst die eingegangene Anfrage und bereitet für das Einrichten der VM alles vor (z.B. Überprüfung der gewünschten Kapazitäten). Möglicherweise kann eine Zuordnung der Abwicklung erfolgen, so dass nicht der Administrator selbst, sondern ein anderer Mitarbeiter die Erstellung der VM vornimmt. Sind alle Randbedingungen geklärt und akzeptiert, wird der eigentliche Vorgang an das Release Management (kurz: ReM) übergeben. Wie in Abbildung 4.5 zu sehen, besteht eine wechselseitige Beziehung zwischen diesen beiden Prozessen. Gibt es auftretende Probleme, muss das ChM diese bewerten und darauf neu reagieren. Diese Informationen werden dann an das ReM zurückgegeben, das die Implementierung weiter vornimmt. Ist die Erstellung des Servers abgeschlossen, übernimmt das ChM eine letzte Überprüfung, ob auch alles korrekt umgesetzt wurde. Diese Evaluierung kann je nach Bedarf mehrere Stunden oder auch Wochen dauern, bis alle Punkte getestet und überprüft worden sind. So kann es vorkommen, dass der erstellte Server erst mehrere Tage getestet werden muss, bevor sicher davon ausgegangen werden kann, dass dieser auch funktioniert. Lief alles zufriedenstellend ab, gehen alle relevanten Informationen an das Configuration Management (CoM) (siehe Verbindung in Abbildung 4.4). Das CoM pflegt die neuen Serverdaten in die CMDB ein. Ein mögliches neues Attribut (bei ITIL: Configuration Item (CI)) kann eingeführt werden, das den Server als VM deklariert. Weitere Informationen könnten die Virtualisierungsumgebung (XEN, VMware, etc.) oder Lebensdauer der VM sein. Sind alle Daten eingepflegt, schließt das CM mit einem Post Information Review (PIR). In diesem PIR sind abschließend noch einmal alle wichtigen Daten über den neuen Server aufgeführt. Diese gehen an den Administrator, der das RfC initiiert hat. Damit ist die Erstellung und Einrichtung eines virtuellen Servers abgeschlossen. Hinter jeder Managementkomponente stehen selbstverständlich Mitarbeiter, die die jeweilige Aufgabe durchführen. In kleineren Unternehmen werden manche Schritte von derselben Person bearbeitet. So kann beispielsweise die Aktualisierung der Informationen im CoM von derselben Person vorgenommen werden, die den RfC behandelt. Dennoch sollte das Vorgehen so eingehalten werden, um nach ITIL einen optimalen Ablauf zu gewährleisten. Der komplette Ablauf ist in Abbildung 4.6 grafisch dargestellt.
Wie vorher erwähnt, könnte eines der Attribute (CI) Informationen über die Lebensdauer des virtuellen Servers enthalten. Ist diese abgelaufen, erhält der Administrator via CMDB die Information, dass die entsprechenden Kapazitäten wieder freigegeben werden müssen. Der folgende Prozess läuft ähnlich zu dem vorherigen Ablauf. Mit einem RfC erhält das Change Management die Informationen über den Server und wie mit diesem zu

[1] Auf die genaue Erstellung einer CMDB wird hier nicht weiter eingegangen. Ein mögliches Konzept des Aufbaus einer CMDB in einem Rechenzentrum wird unter [Sage 06] vorgestellt.

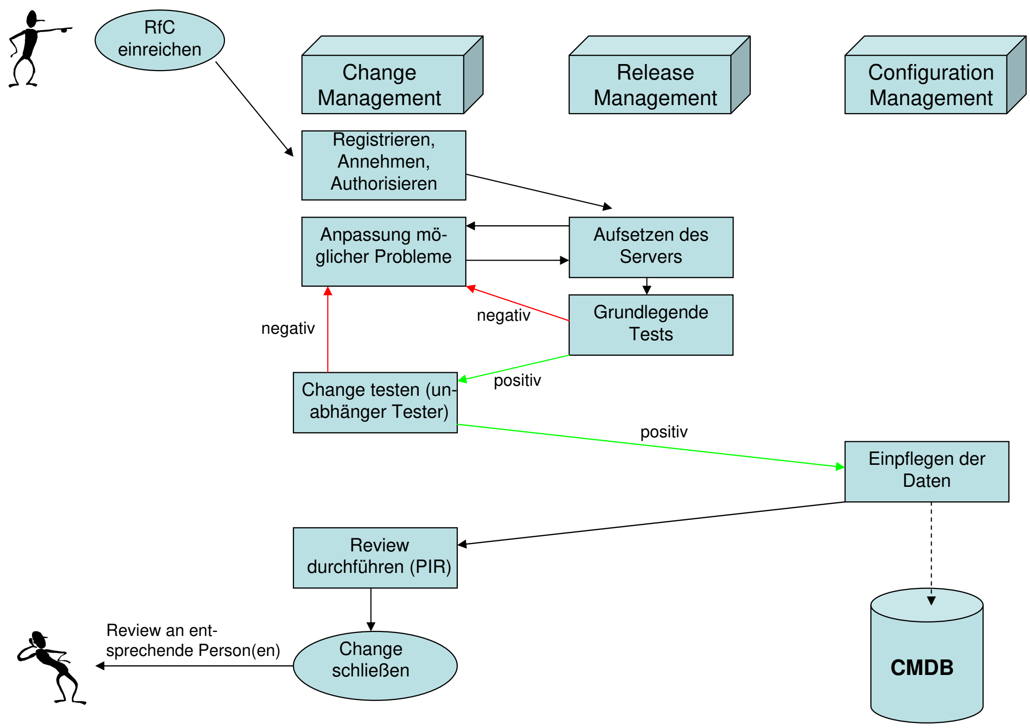

Abbildung 4.6: Die einzelnen Prozessschritte für einen neuen virtuellen Server nach ITIL (Quelle: in Anlehnung an [ITIL 02])

verfahren ist. Hier kann festgelegt werden, ob die virtuelle Maschine komplett gesichert werden muss oder ob die notwendigen Daten zuvor auf die Netzlaufwerke kopiert wurden. Der eigentliche Vorgang wird wieder an das Release Management gegeben, dass die mögliche Sicherung und dann die Löschung der VM vornimmt. Im Austausch mit dem ChM wird überprüft, ob auch alles korrekt durchgeführt wurde (z.B. ob die Ressourcen wieder zur Verfügung stehen). Nach erfolgreicher Prüfung wird dem Configuration Management mitgeteilt, die CMDB zu aktualisieren. Im Abschluss wird vom ChM ein Review durchgeführt, das der Administrator (der das RfC gestellt hat) erhält und der Change ist damit abgeschlossen. Alle Informationen wurden aktualisiert, die Ressourcen stehen wieder zur Verfügung und alle notwendigen Personen sind informiert.
Mit Hilfe dieser Prozesse ist das Erstellen eines neuen virtuellen Servers auf Basis der ITIL geschehen. Daher muss dies das spätere Konzept (siehe Kapitel 5) berücksichtigen, da sonst die Anforderung aus Abschnitt 4.2 nicht erfüllt ist. Als weitere Bedingung, für den speziellen Fall der Astrium GmbH, werden die zuvor beschriebenen Use Cases aus Abschnitt 4.1.3 an diesen Ablauf angepasst. Dazu müssen einige Punkte erweitert werden, doch insgesamt kann der Ablauf aus Abbildung 4.6 übernommen werden.

4.3.3 Die Use Cases anhand der ITIL

Der erste Use Case bei Astrium (siehe Abschnitt 4.1.3) behandelt die Virtualisierung einer kompletten NT4 Domäne. Diese Virtualisierung wird in vier Schritten durchgeführt und muss an die ITIL Prozesse angepasst werden. Im ersten Schritt wird ein Domänencontroller (BDC) in eine virtuelle Maschine umgewandelt. Dazu wird vom Administrator ein RfC an das Change Management geschickt, in dem es um die Migration des Servers geht (P2V), des Weiteren, bei erfolgreicher Migration, um die Entsorgung der alten Hardware. Nach Klärung der Rahmenbedingungen (auf welche Virtualisierungsumgebung, welchen Konverter, etc.) erhält das

Release Management die Aufgabe, dies durchzuführen. Im Zusammenspiel mit dem Change Management wird dies zu einer erfolgreichen Migration gebracht. Das Configuration Management erhält die Informationen, dass es sich ab sofort um einen virtuellen Server handelt (Name, IP Adresse, etc. bleiben gleich) und pflegt diese Daten entsprechend in die CMDB. Zusätzlich kann es zu einer Entsorgungsnachricht kommen, denn die alte physikalische Hardware wird nicht benötigt. Dazu müssen möglicherweise andere Datenbanken informiert werden, die beispielsweise für die Buchhaltung und deren Inventar von Bedeutung sind. Sind die Daten eingetragen und entsprechend weitergegeben worden, wird wieder das ChM informiert. Hier läuft nun der Test, ob auch alles so funktioniert wie gewünscht. Wie zuvor erwähnt, kann diese Phase längere Zeit dauern. So muss sich die virtuelle Maschine erst in der Produktivumgebung bewähren, bevor die Entsorgung der physikalischen Maschine vollzogen werden kann. Mögliche auftretende Probleme können noch eingearbeitet werden, solange der Change noch offen ist. Ist die Testphase zufriedenstellend abgelaufen, wird der Change mit einem Review beendet und der erste Schritt der Virtualisierung ist abgeschlossen.
Im zweiten Schritt geht es um die Virtualisierung eines Domänencontrollers, der gleichzeitig als Druckerserver fungiert. Der Ablauf ist wie zuvor (RfC $\rightarrow$ Change Management $\leftrightarrow$ Release Management), nur dass im Change zusätzliche Informationen enthalten sein müssen. Entweder der Druckerserver oder der Domänencontroller erhalten einen neuen Namen, IP Adresse, etc., der dann entsprechend in die CMDB eingetragen werden muss. Hier behält der Druckerserver seinen Namen und es muss nach der erfolgreichen Implementierung des Release Managements, dieser durch das CoM nur soweit verändert werden, dass es sich ab sofort um einen virtuellen Server handelt. Der Domänencontroller wird als neues Serverobjekt eingefügt und auch als virtuelle Maschine entsprechend markiert. Ansonsten geht für die physikalische Maschine auch hier eine Entsorgungsmeldung raus und es müssen andere Datenbanken informiert werden. Die Testphase kann hier möglicherweise länger dauern, da der neue Server in die restliche Umgebung integriert werden muss und die Tests dadurch verlängert werden. Laufen beide virtuellen Server nach der Testphase erfolgreich, wird auch hier der Change mit einem Review beendet. Damit ist der zweite Schritt abgeschlossen.
Der vorletzte Schritt für diesen Use Case ist die Einrichtung eines neuen Servers auf Basis eines Templates. Da diese Maschine bisher noch nicht existiert hat, läuft der Vorgang genauso wie im vorherigen Abschnitt ab (siehe Abbildung 4.6). Dass die Umsetzung mit Hilfe eines Templates vorgenommen wird, ist für die ITIL irrelevant, denn wie in der Praxis die Umsetzung beim Release Management vorgenommen wird, spielt keine Rolle. Es sei nochmal erwähnt, dass die ITIL sich Prozesse vorstellt, die einen strukturellen und qualitativ besseren Ablauf gewährleisten sollen. Daher spielt der Einsatz des Templates hier keine Rolle und der dritte Schritt ist abgeschlossen.
Auch beim vierten und letzten Schritt, der Virtualisierung des primären Domänencontroller (PDC), ist keine große Änderung zum ersten Ablaufschritt vorhanden. Da es sich um den PDC handelt, kann auch hier die Testphase nach der Implementierung im Change Management länger dauern, da diesem Domänencontroller eine höhere Bedeutung zukommt. Darüber hinaus ändert sich am Ablauf nichts und nach entsprechender Zeit kann der Change abgeschlossen werden. Damit ist dieser Ablauf erfolgreich beendet und der Use Case ist mit den ITIL Prozessen abgedeckt. Als Ergänzung sei noch gesagt, dass es auch möglich wäre, für den zweiten Ablaufschritt (ein physikalischer Server zu zwei virtuellen Servern) zwei RfCs einzuführen. Dann erhält jeder Server ein eigenes RfC, um Anfragen nicht zu komplex werden zu lassen. Dies kann je nach Wunsch durchgeführt werden, da dies nicht detailliert in der ITIL geklärt ist.

Im zweiten Use Case geht es um die Bereitstellung von virtuellen Servern auf Basis von Templates. Wie zuvor erwähnt, spielt die genaue Funktionsweise (die Verwendung von Templates) für ITIL keine Rolle. Aber der im vorherigen Abschnitt vorgestellte Prozess wird in diesem Fall um einige Punkte erweitert. Die Anfrage nach Serverkapazitäten kann nicht nur vom Administrator, sondern auch von einem Projektleiter kommen. Dieser benötigt einen Server für sein Projekt und ist mit der IT Infrastruktur und den Abläufen dahinter nicht vertraut. Daher kann nicht erwartet werden, dass von einem Projektleiter die Anfrage direkt an das Change Management gestellt wird. Abgesehen davon ist es meist nicht gewollt, dass Mitarbeiter ihre Anfragen an die entsprechenden Personen stellen. Es gibt eine zentrale Anlaufstelle, an die alle Anfragen gehen und die auch die Informationen publiziert. Dabei handelt es sich um das zuvor genannte Service Desk, dass die Anfragen (beispielsweise durch ein Antragsformular) entgegennimmt. Auf Grund bestimmter Richtlinien leitet das Service Desk den Antrag an die dafür vorgesehene Stelle (z.B. ein Administrator des Rechenzentrums). Dieser prüft im Vorfeld (falls möglich), ob die Anfrage technisch bewerkstelligt werden kann. Ist dies der Fall, gibt er ein RfC an das Change Management. Dies muss nun im Vorfeld eine Leistungsvereinbarung zwischen Projektleiter und der IT festlegen. Diese Service Level Agreements (SLAs) regeln sowohl die Abrechnungs-

modalitäten für die bereitgestellten Kapazitäten, als auch bestimmte Dienstgüteparameter, wie Datendurchsatz oder Verfügbarkeit. Dabei bietet die ITIL eine Vielzahl an Regelungen und Punkte, die in einen SLA Vertrag aufgenommen werden können. Wie zuvor schon erwähnt, kommt es in der Arbeit zu keiner genaueren Definition, wie diese Vereinbarungen aussehen können. Dies ist ein eigenständiges Thema, dass einer genauen Analyse bedarf, um für den Virtualisierungsfall ideale SLAs festzulegen.
Sind die Konditionen geregelt, kann der Vorgang wie in Abbildung 4.6 durchgeführt werden. Nach Abschluss des Changes werden die Informationen dem Administrator übermittelt. Dieser sendet die notwendigen Daten für den Projektleiter an das Service Desk. Dies wiederum informiert den Anwender über die erfolgreiche Einrichtung und teilt ihm die Informationen, wie Servername oder Zugangsdaten, mit. Dadurch ist das Service Desk die einzige Informationsstelle nach Außen und alle zukünftigen Probleme oder Anfragen werden hier gestellt.
Bei Ablauf des Vertrages informiert der Administrator das Service Desk, eine entsprechende Information an den Projektleiter zu geben. In der Praxis läuft dieser Nachrichtenaustausch direkt zwischen Administrator und Projektleiter. Soll der virtuelle Server gesichert werden (weil die Testumgebung komplett gesichert werden muss), ist dies zuvor geregelt. Sonstige Daten müssen sich auf Netzlaufwerken befinden und dürfen nicht auf den virtuellen Platten gelagert werden. Sind diese Punkte geklärt, wird der Server heruntergefahren und gegebenenfalls gesichert. Für den Projektleiter ist alles geklärt und der weitere Ablauf für ihn nicht mehr von Bedeutung. Danach wird das RfC vom Administrator eingereicht und der entsprechende Change Prozess läuft an. Nach Beendigung wird der Administrator über die erfolgreiche Durchführung informiert und die Ressourcen stehen wieder zur Verfügung. Damit ist der komplette Use Case in der ITIL abgebildet worden.

Mit diesem Abschnitt wird nun das Kapitel der Anforderungsanalyse beendet. So wurde zuerst der Anwendungsfall Astrium vorgestellt, der in manchen Punkten firmenspezifische Besonderheiten aufweist. Die Anforderungen werden sowohl für diesen speziellen Fall, als auch für eine allgemeine heterogene Infrastruktur betrachtet. Des Weiteren erfolgt mit der ITIL eine besondere Auflage, um die Virtualisierung strukturiert ablaufen zu lassen. Die Einordnung für die Use Cases ist in diesem Abschnitt geschehen und rundet das Kapitel ab. Im nächsten Schritt erfolgt das eigentliche Konzept, mit dem die Virtualisierung durchgeführt wird. Dazu sind gewisse Vorbedingungen notwendig, die teilweise schon zur Sprache kamen, aber im nächsten Kapitel erneut aufgegriffen und erweitert werden. Diese sind notwendig, um dann die Virtualisierung effizient durchzuführen. Die entscheidenden Schritte erhalten eine detaillierte Vorstellung.

5 Konzept

Ein Konzept zur Umsetzung der Virtualisierung ist notwendig, um am Ende ein funktionierendes, sicheres und zuverlässiges System betreuen zu können. Um dies zu gewährleisten, ist es wichtig, bei der Virtualisierung strategisch vorzugehen (vgl. [Rode 07]). So kann eine optimale Hardwareauslastung dazu verleiten, alle physikalischen Server in virtuelle Systeme umzuwandeln [Rode 07]. Dies ist aber nicht für jeden Server und dessen Anwendung eine ideale Lösung, sondern es müssen noch weitere Überlegungen vorgenommen werden, ob dies auch sinnvoll ist. Die zuvor ermittelten Anforderungen an die Virtualisierung spielen dabei eine wichtige Rolle, denn Punkte, wie die Gewährleistung von Sicherheit, gewinnen an Bedeutung. Aus diesen Gründen werden im Abschnitt 5.1 erneut die Voraussetzungen für eine Virtualisierung zusammengefasst. Zusätzlich gibt es weitere Bedingungen, die es zu erfüllen gilt, bevor der nächste Schritt durchgeführt werden kann. In Abschnitt 5.2 erfolgt die Installation der Virtualisierungsumgebung. Dabei muss nicht nur die eigentliche Umgebung, sondern auch eine Managementkonsole für die zu betreuenden Server und virtuellen Maschinen eingerichtet werden. Des Weiteren erfolgt eine Pilotinstallation, um die Umgebung zu testen. Ist die Installation erfolgreich, kann ein erstellter Use Case umgesetzt werden. Im darauffolgenden Abschnitt 5.3 erfolgt dann der Test des Systems und der darauf laufenden Anwendungen. Dieser erfolgt aber noch nicht als Produktivsystem, sondern befindet sich immer noch in einem Testumfeld, das von den entsprechenden Administratoren überwacht wird. Ist diese Phase erfolgreich, muss ein Sicherungssystem eingeführt werden (siehe 5.4). Hier muss entschieden werden, was gesichert werden soll und ob sich nach dem erfolgreichen Sichern, die Daten auch wiederherstellen lassen. Bevor dann die Virtualisierung eingesetzt werden kann, gilt es, die Sicherheit der virtuellen Umgebung zu prüfen (siehe 5.5). Dabei spielen vor allem die in Abschnitt 3.3.4 genannten Probleme eine Rolle, die soweit wie möglich getestet und überprüft werden müssen. Sind die Sicherheitsüberprüfungen erfolgreich vorgenommen worden, kann im letzten Schritt (siehe 5.6) die Virtualisierungsumgebung produktiv in Betrieb genommen werden. Hierbei geht es um die Funktionalität im ganzen System, entsprechende Schulung von notwendigen Personen und andere Punkte. Wichtig während der ganzen Umsetzung, von den Voraussetzungen bis zur Inbetriebnahme, ist die Dokumentation aller Schritte. Nur anhand dieser können mögliche Fehler oder Entscheidungen ermittelt und nachvollzogen werden. Aus Teilen der Dokumentation entsteht am Ende ein Benutzerhandbuch - von der Installation aller relevanten Vorgänge.
Wie an der bisherigen Beschreibung zu sehen ist, läuft die Virtualisierung in mehreren Phasen ab. Daher ist in Abbildung 5.1 der Ablauf grafisch dargestellt. Dieser zeigt, dass der Ablauf zyklisch aufgebaut ist und in bestimmten Phasen auf die vorherige zurückgegriffen werden kann. Zusätzlich kann in manchen Phasen auf weiter zurückliegende Punkte eingegangen werden. Dadurch können Veränderungen oder Probleme in späteren Phasen in den vorherigen Schritten geändert und überarbeitet werden. So bleibt der Ablauf dynamisch und lässt sich an neue Anforderungen anpassen.

5.1 Voraussetzungen

Zu den Voraussetzungen einer Hostvirtualisierung gehören mehrere Auslöser, die eine Virtualisierung sinnvoll erscheinen lassen. In der Regel sind dies Probleme, die bei der bisherigen Infrastruktur auftreten. Diese wurden bereits in Abschnitt 2.1 beschrieben und die Möglichkeiten der Virtualisierung könnten diese Probleme lösen. Ist die Entscheidung zugunsten der Virtualisierung gefallen, sind einige nicht-technische Punkte zu beachten. Es müssen sowohl die etwaigen Anschaffungskosten der Umgebung, als auch die Zeit für die Einrichtung eingeplant werden. Ist bisher keine Virtualisierung eingesetzt worden, muss möglicherweise auf externe Hilfe zurückgegriffen werden, die unterstützend bei der technischen Vorgehensweise mitarbeitet. Bei bereits existierenden Virtualisierungslösungen muss zuvor überprüft werden, ob das vorhandene Wissen auch ausreichend für den vorliegenden Fall ist. So kann beispielsweise eine bisher unbekannte Umgebung eingesetzt werden, für die zusätzliches Wissen benötigt wird. Des Weiteren spielen die gestellten Anforderungen eine wichtige

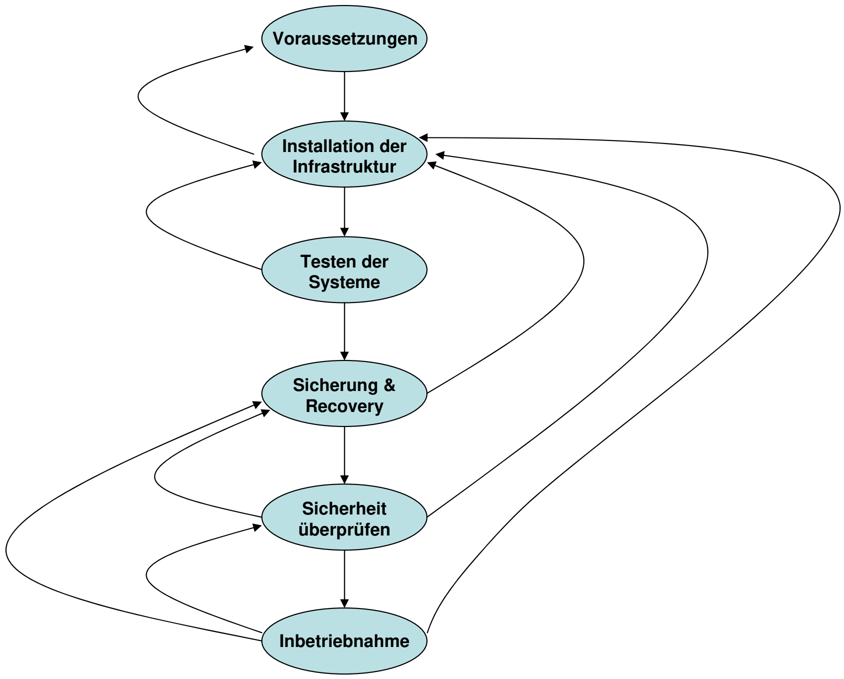

Abbildung 5.1: Die einzelnen Ablaufschritte des Konzeptes und deren Zyklen

Rolle. Anhand derer kann die Wahl der Virtualisierungsumgebung ausschlaggebend sein, wenn eine bestimmte Eigenschaft unbedingt notwendig ist. Neben dem Kostenpunkt und ob das notwendige Wissen vorhanden ist, spielen die vorhanden Server die entscheidende Rolle. Im ersten Schritt muss eine Bestandsaufnahme aller Server vorgenommen werden. Welche Punkte dabei von Bedeutung sind, wird im nächsten Abschnitt geklärt. Anhand des Bestandes müssen nun geeignete Server ausgewählt werden, die sich zur Virtualisierung eignen. Dies wurde bisher noch nicht detailliert besprochen, ist aber die Basis jeder Planung. Auf Grund dieser Analyse und den zuvor ermittelten Punkten fallen die Entscheidungen, welche Virtualisierungsumgebung, in welchem Ausmaß zu verwenden ist.

5.1.1 Bestandsaufnahme

Die Bestandsaufnahme dient zur Ermittlung aller vorhandenen Server, die für eine Virtualisierung in Frage kommen können. Die Auswahl dieser erfolgt im nächsten Abschnitt. Bei der Ermittlung der Server ist es von Vorteil, wenn nach ITIL eine Datenbank (CMDB) existiert, die alle wichtigen Informationen enthält. Diese sind neben den Komponenten des Servers, auch die darauf laufende Anwendung und mögliche zusätzliche Attribute. Unter diese Attribute fällt beispielsweise Zusatzhardware oder bestimmte Treiber, die für spezielle Programme notwendig sind. Auch Zusammenhänge zu anderen Systemen sind von Bedeutung, falls diese Verbindungen später gesondert getestet werden müssen. Existiert solch eine Datenbank nicht, müssen über Inventarlisten oder vor Ort die Daten zusammengetragen werden. Diese allein sind aber nicht ausschlaggebend, wie die Virtualisierungsumgebung dimensioniert wird. Die nächsten bedeutenden Informationen betreffen das Leistungsverhalten der Server. Dabei ist vor allem die Auslastung in Bezug auf CPU, RAM, Netzwerk und Datenspeicher wichtig. Dies sind Daten, die meist nicht so leicht zu ermitteln sind, aber im Auswahlschritt benötigt werden. Um diese zu ermitteln, muss entweder ein Leistungsbenchmark eingesetzt werden, oder es existieren andere Quellen, die diese Daten ermitteln. Beispielsweise bieten die Hersteller für ihre Server in der Regel Managemetprogramme an, die CPU Last, RAM Ausnutzung oder den Netzverkehr angeben. Auch bei manchen Datenspeichersystemen gibt es die Möglichkeit, Leistungsdaten zu ermitteln (vgl. Tool von

[net 07a]). Neben den kurzfristigen Leistungsdaten, sind auch spezielle „Peaks” zu berücksichtigen. So kann ein Server gegen Ende des Jahres die Hardware voll nutzen, in der restlichen Zeit werden die Ressourcen aber kaum beansprucht. Diese Informationen sind von Bedeutung, damit bei einer Virtualisierung die Ressourcen nicht zu knapp bemessen werden und flexibel reagiert werden kann. Als letzten Punkt gilt es noch zukünftige Serveranschaffungen oder Projektanfragen zu berücksichtigen. Möglicherweise eignen sich diese auch zur Virtualisierung und sollten in die Bestandsliste aufgenommen, aber als „noch nicht existierend” vermerkt werden.
All diese Informationen gilt es zu sammeln und strukturiert darzustellen. Anhand dieser Liste kann im nächsten Schritt die Auswahl der Server erfolgen.

5.1.2 Auswahl der geeigneten Server zur Virtualisierung

Für die Auswahl der geeigneten Server gibt es mehrere zu beachtende Punkte. Die Idee der Virtualisierung ist es, die Hardware möglichst optimal aufzuteilen und so die Ressourcen optimal auszunutzen. Bei der dabei verwendeten Hardware handelt es sich um wenige leistungsstarke Server mit mehreren CPU Kernen und viel RAM. Befindet sich in der zuvor erstellen Liste ein Server, der ähnliche Hardwarevoraussetzungen hat und diese auch ausnutzt, ist eine Virtualisierung hier nicht sinnvoll. Dies hätte zur Folge, dass wenig bis keine Ressourcen nach einer Virtualisierung vorhanden wären, die für andere VMs nutzbar sind. Daher können diese Maschinen von der Liste gestrichen werden. Als nächstes werden Maschinen von der Liste genommen, die spezielle Zusatzhardware benötigen, die in einer virtuellen Maschine nicht funktionieren. Dabei kann es sich um hardwarebasierte 3D Beschleunigung handeln, die für bestimmte Anwendungen notwendig sind (vgl. [Rode 07]). Auch Server, die kundenspezifische Treiber für bestimmte Hardwarekomponenten einsetzen, eignen sich nicht zur Virtualisierung, da diese in der virtuellen Umgebung wahrscheinlich nicht mehr laufen werden. Des Weiteren sollten keine Server virtualisiert werden, die schlecht skalierbar sind oder über die unzureichende Informationen vorliegen. Dazu zählen vor allem Datenbankserver, bei denen, durch einen Nutzeranstieg, es zu einer erhöhten E/A (Eingabe/Ausgabe) Belastung kommt. Daher stößt die virtuelle Maschine schnell an ihre Grenzen und es müssen weitere Ressourcen eingeräumt werden. Außerdem entsteht eine erhöhte Belastung des Netzverkehrs, was zur Beeinträchtigung der anderen VMs führen kann. Dies gilt es aber laut Anforderungskatalaog (siehe „Service Qualität in Abschnitt 4.2) unbedingt zu verhindern. Prinzipiell können Datenbankserver virtualisiert werden, wenn mit einer konstanten Nutzeranzahl und Netzlast zu rechnen ist. Als weiteres Kriterium muss die einzusetzende Virtualisierungsumgebung auch das vorhandene Betriebssystem unterstützen. Die meisten Betriebssysteme werden bei den großen Anbietern offiziell unterstützt, doch falls die Umgebung schon feststeht, können in diesem Schritt Maschinen herausfallen, deren Betrieb nicht gewährleistet ist.
Der letzte und sehr wichtige Punkt ist das Thema Sicherheit. Hierbei geht es sowohl um die Ausfallsicherheit der Maschine, als auch die Sicherheitsrichtlinien im Sinne des englischen Begriffs „Security”. Wie bereits beschrieben, ist der Ausfall eines Hosts mit mehreren laufenden VMs wesentlich schlimmer, da nicht nur ein Server, sondern alle laufenden virtuellen Maschinen ausfallen. Daher muss auf diese gesondert geachtet und reagiert werden. Um bestimmte Server dieser erhöhten Gefahr nicht auszusetzen, kann hier festgelegt werden, dass einige Maschinen als physikalische Geräte bestehen bleiben. Diese Entscheidung kann persönliche wie strategische Gründe haben. So mancher Administrator vertraut der Virtualisierungstechnik nicht und lässt daher kritische Anwendungen auf einer dedizierten Hardware laufen. Diese Maschinen werden auch von der Liste entfernt und werden später für die Virtualisierung nicht berücksichtigt. Die Gefahr der Ausfallsicherheit kann aber auch anders vorliegen. Gerade weil die Hardware schon alt und unsicher ist, eignet sich der Server zur Virtualisierung, um die Ausfallsicherheit zu erhöhen. Dadurch können sich bestimmte Maschinen, die bisher nicht beachtet wurden, fhervorheben und später bevorzugt behandelt werden. Wie zuvor beschrieben, müssen hier auch Sicherheitsrichtlinien beachtet werden. Abschnitt 3.3.4 hat gezeigt, dass neue Sicherheitsprobleme mit der Virtualisierung auftauchen und dass bei einem erfolgreichen Eindringen in einen Host auch die virtuellen Maschinen manipuliert werden können. Außerdem entsteht durch die Virtualisierung eine Entkoppelung von einer physikalischen Hardware, die dementsprechend nicht über Zugangssysteme (z.B. Schlüssel für das Rechenzentrum) gesichert werden kann. Daher sollten sicherheitskritische Maschinen weiterhin gesondert behandelt werden. Es gibt zwar auch Sicherheitskonzepte und Lösungen für virtuelle Maschinen, aber gerade durch die aktuelle Problematik mit den Rootkits (siehe 3.3.4 und [Bach 07]) sollten diese sicherheitskritischen Maschinen nicht virtualisiert werden. Dies kann an dieser Stelle aber nur eine Empfehlung sein, deren finale Entscheidung von einem zuständigen Sicherheitsbeauftragten gefällt werden muss. Diesem sind

die aktuellen Probleme und die vorliegenden Sicherheitslösungen bekannt und er kann anhand dieser entscheiden, wie vorzugehen ist. In der Regel fällt aber die Entscheidung gegen die Virtualisierung solcher Maschinen.

Im vorherigen Abschnitt wurden bei der Bestandsaufnahme auch zukünftige Server berücksichtigt, die bisher aber noch nicht angeschafft wurden. Falls möglich, werden alle Kriterien auch auf diese angewandt und diese als mögliche virtuelle Maschinen in Betracht gezogen. Dies ist von Bedeutung, damit in der Planungsphase die zusätzlichen Ressourcen mitberücksichtigt werden. Möglicherweise beeinflussen die zukünftigen Server auch die Wahl der Virtualisierungsumgebung, wenn beispielsweise ein Betriebssystem eingesetzt wird, dass die aktuelle Lösung nicht unterstützt.
Insgesamt entsteht aus diesen Punkten eine Liste von Servern, die folgende Eigenschaften haben:

- Maschinen mit unterstützter Hardware und Software in der Virtualisierungsumgebung
- Systeme mit geringer Auslastung in jeglicher Hinsicht (sowohl E/A, als auch CPU)
- Maschinen, die in Bezug auf Sicherheit keine Sonderstellung einnehmen
- Systeme, die aus weiteren Gründen nicht virtualisiert werden sollen

Der letzte Punkt bezieht sich auf persönliche und subjektive Entscheidungen, warum die Maschine nicht virtualisiert werden sollen. Dies berücksichtigt die Erfahrung von Administratoren und betriebsinterne Entscheidungen, die nicht an den vorliegenden Punkten gemessen werden können.
Mit dieser vorliegenden Liste fallen im nächsten Schritt einige Entscheidungen, die für die Virtualisierungsumgebung wichtig sind. Auch werden die bisher ermittelten Anforderungen in die Entscheidung einfließen.

5.1.3 Entscheidungen aus den Voraussetzungen

Anhand der vorliegenden Liste, den allgemeinen Voraussetzungen aus 5.1 und dem Anforderungskatalog aus Abschnitt 4.2, können nun Entscheidungen für die Virtualisierungsumgebung gefällt werden. Der hier vorliegende Anwendungsfall ist die Virtualisierung einer heterogenen Infrastruktur, wie in Abschnitt 2.1 beschrieben. Aufgrund der entsprechenden Anforderung, muss eine Virtualisierungsumgebung ausgewählt werden, die es erlaubt, verschiedene Betriebssysteme zu berücksichtigen. Dadurch fallen beispielsweise Produkte, deren Virtualisierung auf Betriebssystem Ebene funktioniert, weg. Die beiden verbleibenden Techniken können unter gewissen Voraussetzungen verwendet werden (beispielsweise läuft Windows unter paravirtualisierten Systemen nur, wenn hardwareunterstützte Prozessoren (AMD-V oder Intel VT-x) eingesetzt werden). Der Umfang der Virtualisierungsumgebung hängt von der ermittelten Anzahl der Server aus dem vorherigen Abschnitt ab. Ergibt die Liste nur eine geringe Anzahl an Rechnern, kann ein anderes Produkt eingesetzt werden, als bei einer größeren Serveranzahl. Neben der Virtualisierungsumgebung entscheidet die zu virtualisierende Serveranzahl auch, wie viele physikalische Hosts eingesetzt werden müssen. Zuerst muss der eingesetzte Host zu der Virtualisierungslösung kompatibel sein. Des Weiteren kann davon ausgegangen werden, dass Anwendungen in virtuellen Maschinen ungefähr dieselben Ressourcen erfordern, wie auf physikalischen Maschinen. Das Leistungsvermögen eines physikalischen Servers mit 512 MB RAM wird auch von einer virtuellen Maschine benötigt, um die gleiche Arbeitslast zu bewältigen [Rode 07]. Auch das eingesetzte Produkt benötigt zusätzliche Ressourcen, die ebenfalls eingeplant werden müssen. Auch Pufferzonen fließen in die Berechnung ein, was am Ende eine bestimmte Anzahl an Hosts ergibt. Als letztes gilt es, die Ausfallsicherheit hier zu berücksichtigen, was zu einer Einplanung von mehreren redundanten Maschinen führt. Ob die Ausfallsicherheit durch die Virtualisierungssoftware vorgenommen wird, oder ob hier eigene Systeme eingreifen müssen, ist ein weiteres Kriterium, auf welches Produkt die Wahl fällt. Insgesamt ergibt sich aus den genannten Punkten die Anzahl der benötigten Hosts, für die dann die ausgewählte Virtualisierungsumgebung gegebenenfalls lizensiert werden muss.
Des Weiteren muss zu Beginn geklärt werden, welche Backup Software eingesetzt werden soll. So gibt es auch hier die Möglichkeit, dass die Virtualisierunglösung eine entsprechende Funktion anbietet, oder es muss auf Drittherstellerprodukte zurückgegriffen werden. Als letzten und wichtigsten Punkt für die Entscheidung der Virtualisierungsumgebung ist das Management der virtuellen Maschinen. Da eine essenzielle Anforderung, die „Zeiteinsparung durch einfachere und komfortablere Handhabung der VMs über eine zentrale Konsole" ist, gilt es, das Produkt zu wählen, das dies dem Fachmann auch garantiert. So kommen Administratoren, die in Linuxumgebungen arbeiten, möglicherweise mit einer Konsole auf Kommandozeile besser zurecht, als

Administratoren von Windowssystemen. Auch spielen die zusätzlichen Merkmale der Konsole zur Erleichterung der Verwaltung eine Rolle, die bei jedem Produkt anders ausfallen. Ob diese Merkmale von Bedeutung sind, liegt auch hier wieder an den Anforderungen, die an das System gestellt werden. Beispielsweise ist die Migration von physikalischen zu virtuellen Servern ein wichtiger Punkt, der durch die Umgebung oder durch Zusatzprogramme gelöst werden muss.

Sind all diese Punkte geklärt, hat sich für die entsprechend vorliegende Situation eine Virtualisierungsumgebung hervorgetan. Alle Anforderungen, die ermittelte Serverliste, die äußeren Rahmenbedingungen (finanzieller Spielraum, vorhandenes Wissen der Umgebung, etc.), die einzusetzenden Hosts und die individuellen Entscheidungen des Administrators, haben auf die zu verwendende Lösung Einfluss genommen. Das Produkt ist jetzt vorhanden und entsprechend lizensiert, um es im nächsten Schritt einzusetzen. Des Weiteren stehen die notwendigen Hosts zur Verfügung und können installiert werden. Vorbedingungen, bezüglich Sicherung der Daten und Sicherheit der Umgebung, hat es gegeben und werden im späteren Verlauf umgesetzt. Mit all diesen Voraussetzungen kann im nächsten Abschnitt mit der Installation der Infrastruktur begonnen werden.

5.2 Installation der Infrastruktur

Die Installation der Virtualisierungsumgebung muss auf allen Hosts erfolgen, die später zur Virtualisierung eingesetzt werden sollen. Je nach eingesetztem Produkt, muss zuerst ein entsprechendes Betriebssystem installiert werden, der sogenannte Wirt. Dabei handelt es sich in der Regel um eine Windows- oder Linuxinstallation. Ausnahme ist beispielsweise der ESX Server, der ein eigenes Betriebssystem mitbringt. Ist der Wirt installiert und konfiguriert (Netzverbindung, Zugriffsrechte, etc.) kann die Virtualisierungsumgebung installiert werden. Im Detail bedeutet das, es installiert sich ein Virtual Maschine Monitor, auch Hypervisor genannt, auf dem vorliegenden Wirtssystem. Dabei ist der entsprechenden Anleitung zu folgen, um die Umgebung korrekt zu installieren und einzurichten. Ist die Installation abgeschlossen, sind die Grundvoraussetzungen für einen arbeitenden VMM gegeben. Damit kann meist auf Kommandozeilenebene gearbeitet werden. Eine übergreifende Konsole für alle Hosts und dessen zukünftige VMs ist aber noch nicht vorhanden. Daher wird im nächsten Schritt der Managementserver installiert, der die eigentlichen Aufgaben der Virtualisierung übernimmt. Es sei noch angemerkt, dass bei manchen Produkten automatisch eine Verwaltungsoberfläche mitinstalliert wird. Dies ist vor allem bei den kostenlosen Programmen für den Privat- und Kleineinsatz der Fall. Im Folgenden wird aber von größeren Umgebungen ausgegangen und bei der Verwendung dieser Produkte ist meist ein eigenständiger Managementserver vorhanden, der installiert und eingerichtet werden muss.

5.2.1 Installation und Konfiguration des Managementservers

Bei der Installation des Managementservers steht zu Beginn die Entscheidung an, ob dieser auf einer eigenen physikalischen Maschine oder auch als virtuelle Maschine installiert wird. So wird dies von manchen Herstellern nicht untersagt und dadurch kann ein eigenständiger Server eingespart werden. Außerdem befindet sich die VM direkt in dem notwendigen Netz und kann auf die Hosts zugreifen. Die entsprechenden Ressourcen müssen vorab auf den Hosts vorhanden sein und in die vorherigen Überlegungen eingeplant werden. Unabhängig wie die Wahl ausfällt, der Managementserver benötigt ein Betriebssystem, welches entweder schon vorhanden ist oder bei einer VM erst installiert werden muss. Liegt nun die Maschine vor, muss geregelt sein, dass die Maschine Netzzugriff auf alle zu verwaltenden Hosts hat. Ansonsten kann nicht von einem zentral agierenden Server ausgegangen werden. Ist dies der Fall, erfolgt die Installation des Managementservers. Meist sind dabei mehrere Punkte zu beachten, da der spätere Server die komplette Verwaltung übernimmt. Dies gestaltet sich, je nach eingesetztem Produkt anders, muss aber bei der Installation entsprechend berücksichtigt werden. Ist die Installation abgeschlossen, muss gegebenenfalls auf allen Hosts ein sogenannter Agent eingerichtet werden. Bei der Installation des VMM wird dieser automatisch mitinstalliert, oder es erfolgt eine separate Installation. Über diesen Agenten tauscht der Managementserver die Informationen aus und steuert die einzelnen Hosts. Sind diese eingerichtet, ist eine fertige Managementumgebung vorhanden. Um diese aufzurufen, gibt es mehrere Möglichkeiten. Die einfachste Art ist eine Konsoleneingabe, in der über entsprechende Befehle alles gesteuert wird. Eine etwas komfortablere Art ist ein webbasierter Zugriff, der alle wichtigen Einstellungen anzeigen und ändern lässt. Als dritte Möglichkeit existiert ein eigenes Programm, das sich mit

dem Managementserver verbindet und die Daten grafisch darstellt. Hier können dann alle Hosts und deren virtuelle Maschinen angezeigt werden. Des Weiteren können alle notwendigen Einstellungen vorgenommen werden. Idealerweise ist dies in allen Zugriffsarten gleich, nur die Präsentation der Informationen gestaltet sich anders.
Der Zugriff erfolgt ab sofort über den Managementserver und alle wichtigen Einstellungen werden daüber vorgenommen. So muss bei der Ersteinrichtung festgelegt werden, welche Hosts zu betreuen sind. Hinzu kommen einige Konfigurationseinstellungen, die für jede Virtualisierungsumgebung anders ausfallen. Beispielsweise kann ein externer Datenspeicher angebunden werden, in dem die virtuellen Maschinen gespeichert sind. Wichtig ist vor allem, die Netzwerkkarten zu konfigurieren. Hier gibt es verschiedene Möglichkeiten, wie die Netzlast verteilt wird. Je nachdem, wie viele Netzschnittstellen vorhanden sind und ob diese gesondert behandelt werden, muss dies eingerichtet werden. Falls gewünscht, könnte der Managementserver einen Netzwerkport nur für sich nutzen, um immer Zugriff auf die Maschinen zu erhalten. Bei Ausfall dieses Ports muss, falls möglich, ein Ersatzport eingerichtet werden. Bietet die Konsole zusätzlich bestimmte Eigenschaften an, die für das Anlegen und Verwalten von VMs notwendig sind, müssen diese entsprechend beachtet und installiert werden. Ist dies erfolgreich vorgenommen worden und ein Datenspeicher (intern oder extern) ausgewählt, steht die Umgebung bereit, eine erste VM zu installieren.

5.2.2 Durchführung einer Pilotinstallation

Die Umgebung ist mittlerweile so weit eingerichtet, dass für eine Installation alles vorhanden ist. Daher gilt nun im ersten Schritt die Pilotinstallation einer VM. Über die entsprechende Funktion in der Konsole wird eine VM erzeugt. Dabei sind einige Parameter wichtig, die die VM definieren. Darunter fallen Punkte, wie die Wahl des Hosts und des Betriebssystems, Zuteilung des Hauptspeichers, Anlegen von einer oder mehreren virtuellen Platte(n), Angabe wie viele CPU Kerne durchgereicht werden und ob eine Netzverbindung vorhanden sein soll. Für einen ersten Test, muss die VM nicht unbedingt am Netzwerk angeschlossen sein. Sind die Tests erfolgreich, kann dies in einem weiteren Schritt aktiviert werden, um auch die Kommunikation zu anderen physikalischen Maschinen zu testen. Mit Hilfe aller Daten kann die virtuelle Maschine erstellt werden. Nach erfolgreicher Erstellung, kann die VM über die Managementkonsole gestartet werden. Bisher ist aber noch kein Betriebssystem installiert, sondern es wurde nur ausgewählt, welches System installiert werden soll. Dies ist für die Virtualisierungsumgebung wichtig, damit entsprechende Systembefehle besser behandelt werden können. Dadurch kann eine höhere Performanz erreicht werden, wenn beispielsweise von Beginn an mit Kernelbefehlen von Linux gerechnet werden kann. Daher muss jetzt das ausgewählte Betriebssystem installiert werden, dass über mehrere Möglichkeiten funktioniert, je nach Virtualisierungsumgebung. So kann das CD Laufwerk des Hosts an die virtuelle Maschine durchgereicht werden, von dem aus dann die Installation erfolgt. Des Weiteren kann eine zuvor erstellte CD-Image Datei, als virtuelles Laufwerk eingebunden werden. Dies erscheint wie ein echtes Laufwerk, von dem aus gebootet werden kann. Als letzte Möglichkeit bieten manche Umgebungen das Booten über Netzwerk an. Dadurch kann entweder ein Betriebssystem von einer anderen Platte gebootet werden oder die Installation erfolgt über einen Installationsserver aus dem Netzwerk. Dieser übernimmt automatisch die Installation des Betriebssystems. Bei allen drei Möglichkeiten liegen nun die Installationsdateien vor und können manuell oder automatisch installiert werden. Bei manchen Betriebssystemen müssen bestimmte Treiber installiert werden, damit diese auch in der Virtualisierungsumgebung arbeiten. Dies hängt aber vom eingesetzten Produkt ab und ist daher entsprechend in der Anleitung dokumentiert. Ansonsten läuft die Installation wie bei einer physikalischen Maschine ab und kann vom Administrator vorgenommen werden. Ist dies abgeschlossen, steht die VM mit dem gewünschten Betriebssystem zur Verfügung. Hier können nun entsprechende Tests und Erfahrungen gesammelt werden. Installationen erfolgen über das virtuelle CD Laufwerk, das wie zuvor entweder vom Host durchgereicht oder per CD-Image Datei angebunden wird. Sind alle Tests positiv, kann im letzten Schritt das Netzwerk aktiviert werden. Das funktioniert meist „on-the-fly" und steht sofort zur Verfügung. Wurden alle Einstellungen in der Managementkonsole bezüglich des Netzwerks korrekt vorgenommen, steht dies auch für die VM zur Verfügung und kann entsprechend verwendet werden. Hier können Zugriffe auf andere freigegebene Maschinen erfolgen, wie der Proxyserver für das Internet oder ein Mailserver. Nach erfolgreichem Testen, kann nun im nächsten Schritt die eigentliche Umsetzung der Anwendungsfälle vorgenommen werden. Sollte es in einer der bisherigen Phasen zu Problemen gekommen sein, müssen entweder die Einstellungen in der Managementkonsole oder die komplette Umgebung überprüft werden. Dies kann anhand der dokumentierten Schritte nachvollzogen werden, wie die bisherige Umsetzung durchgeführt wurde. Sollte es zu keiner Lösung der auftretenden Probleme kommen, muss eine grundsätzliche Überarbeitung bei den Voraussetzungen erfolgen (siehe Zyklus in Abbildung 5.1).

5.2.3 Schrittweise Virtualisierung der ermittelten Server

Nach dem erfolgreichen Testen im vorherigen Schritt, kann nun hier die Umsetzung des Use Cases erfolgen. Deren Ablauf sind in der Regel grob skizziert und dieser muss an die entsprechende Virtualisierungsumgebung angepasst werden. Wenn es keine bestimmten Zusammenhänge der Server gibt, sondern nur eine Liste, wie sie in Abschnitt 5.1 erstellt wurde, zu virtualisieren gilt, sollte mit Maschinen angefangen werden, die auf unsicherer Hardware laufen und daher eine erhöhte Ausfallgefahr vorliegt. Anhand der Anforderungen ist hier eine Entscheidung gefallen, ob die vorhandenen Maschinen migriert oder neu angelegt werden. Die Migration hat die Vorteile, dass keine Neuinstallation und Einrichtung vorgenommen werden muss, was erheblich Zeit und Geld spart. Manchmal ist es aber sinnvoll, die Maschine, wenn sich die Gelegenheit bietet, neu anzulegen, um manche Einstellungen anders vorzunehmen, was bisher nicht möglich war. Dies muss je nach Anwendungsfall entschieden werden. Für eine Migration wird ein eigenes Programm benötigt, dass entweder mitgeliefert oder zusätzlich installiert werden muss. Idealerweise bindet sich das Migrationsprogramm in den Managementserver ein und lässt sich per Konsole verwenden. Dadurch ist gewährleistet, dass alle Hosts und Datenspeicher zu sehen sind und auch verwendet werden können. Sind diese Vorbereitungen abgeschlossen, kann die Migration des Servers vorgenommen werden. Je nach eingesetztem Programm, kann die Maschine während des Migrationsvorgangs nicht verwendet werden. Ist dies der Fall, muss die Durchführung in einem Wartungsfenster vorgenommen werden. Bevor die eigentliche Migration startet, können in der Regel noch einige Daten über die neu erstellte virtuelle Maschine eingerichtet werden. Für ein schnelles Umschalten in den Produktivbereich sollten dabei so wenig Daten wie möglich geändert werden. Oft ist es sinnvoll, die Platten anzupassen, da in der physikalischen Maschine Platten mit größerer Kapazität vorhanden sind, als benötigt wird. Des Weiteren kann auch hier eingestellt werden, ob beim Starten das Netz aktiviert werden soll. Dies sollte in der Regel deaktiviert werden, denn die virtuelle Maschine wird zuerst einigen Tests (siehe Abschnitt 5.3) unterzogen, bevor sie ans Netz geht. Außerdem würden zwei Maschinen mit identischen Netzwerkkonfigurationen (IP Adresse, Maschinenname, etc.) existieren, wenn nicht die physikalische Maschine heruntergefahren wird. Um hier Probleme im Netzwerk zu verhindern, sollte das Netzwerk der VM erst aktiviert und getestet werden, wenn die ursprüngliche Maschine ausgeschaltet ist.
Ist die Migration erfolgreich abgeschlossen, erscheint die neue virtuelle Maschine in der Konsole. Diese kann nun gestartet werden, um zu sehen, ob die Migration erfolgreich war. Scheint auf den ersten Blick alles in Ordnung, können weitere Server migriert werden. Sinnvoll ist es hier, die Server eines Use Cases umzusetzen und nicht alle Server aller Anwendungsfälle. Meist hängen bestimmte Maschinen zusammen und es gilt auch diese untereinander zu testen. Daher sei hier nochmals auf den Zyklus in Abbildung 5.1 hingewiesen, dass nach dem Umsetzen eines Use Cases die Testphase anläuft. Danach werden alle Schritte durchlaufen und es kann nach der Inbetriebnahme erneut in diesen Schritt zurückgekehrt werden. Daraufhin kann die Umsetzung des nächsten Anwendungsfalls beginnen.
Liegen alle gewünschten Server als virtuelle Maschine vor, kommt der nächste Schritt: die ausführliche Testphase. Welche Punkte hierbei zu beachten sind, wird im nächsten Abschnitt genauer erklärt.

5.3 Test der Systeme und Anwendungen

In dieser Phase liegt bereits die Umsetzung eines Use Cases vor, dessen Funktionalität aber bisher noch nicht ausreichend getestet wurde. Dies ist aber notwendig, um die Anforderung „Gleiche Funktionalität der virtuellen Maschinen zu den bisherigen Maschinen" aus Abschnitt 4.2 zu erfüllen. Daher muss in diesem Schritt jede virtuelle Maschine für sich und im Zusammenhang mit der Umgebung getestet werden. Dazu ist es sinnvoll, einen Testplan (auch „Test Suite" genannt) aufzustellen, der alle Eigenschaften anhand einer Checkliste beinhaltet und aufgrund des Use Cases die vorliegenden Abhängigkeiten. Dieser Testplan legt alle wichtigen Punkte, wie Dauer des Tests oder die Testpersonen, fest. Die Abwicklung einer Test Suite läuft in mehreren Schritten ab, damit am Ende alle wichtigen Punkte behandelt worden sind.
Zuerst findet eine Testphase für die jeweilige Maschine statt. Bisher ist diese noch nicht mit dem Netz verbunden (siehe Einstellungen bei der Migration in Abschnitt 5.2.3) und es muss hier entschieden werden, ob dies nun benötigt wird. Falls es sich um eine Test- oder Entwicklungsumgebung handelt, kann der Zugriff auch

über den Managementserver erfolgen. Sollen Personen Zugriff auf die VM haben, die keine Administratoren sind, ist ein Netzzugriff sinnvoll, um die VM entsprechend nutzen zu können und nicht den Weg über den Managementserver zu gehen. Je nachdem wie hier entschieden wird, muss die Testphase entsprechend geplant werden. Ist ein Netzzugang notwendig, gibt es zwei Möglichkeiten für das Testen: Entweder wird die VM umkonfiguriert (da das produktive System mit identischen Einstellungen parallel läuft), so dass es keine Konflikte gibt, oder es wird ein Testzeitraum festgelegt, in dem die ursprüngliche Maschine abgeschaltet wird. Danach kann diese durch die VM ersetzt und von den Administratoren getestet werden. Wichtig in diesem Schritt ist, dass ein Test durch ausgewählte Personen vorgenommen wird und diese noch nicht ins Produktivsystem aufgenommen wird. Für welche Methode sich entschieden wird, hängt von der jeweiligen Situation ab. Handelt es sich um einen länger angelegten Test, der über Tage oder Wochen durchgeführt wird, ist es ratsam, die VM soweit zu konfigurieren, dass sie zwar alle Funktionen und Anwendungen anbietet, aber parallel zur physikalischen Maschine laufen kann. Beispielsweise könnte ein virtualisierter Mailserver so konfiguriert werden, dass er in die bestehende Struktur integriert wird, aber die Maschine nur für die Testpersonen zur Verfügung steht. Ist absehbar, dass der Test in kurzer Zeit erledigt werden kann, ist ein Abschalten der physikalischen Maschine in der Testphase ratsam, da keine Veränderungen an der VM vorgenommen werden müssen.
Neben der Dauer des Tests, spielen in der Test Suite die Abhängigkeiten eine wichtige Rolle. Oft muss eine Maschine von mehreren Stellen erreicht werden können, da diese miteinander arbeiten oder benötigte Dienste im Produktivsystem angeboten werden. Diese Punkte sind im zuvor erstelltem Use Case bedacht worden, falls es entsprechende Abhängigkeiten gibt. In der Testphase gilt es, diese zu überprüfen, wie sie zu Beginn im Testplan festgehalten wurden. Sowohl die Beziehungen zu virtuellen, wie auch physikalischen Maschinen (falls vorhanden) müssen getestet werden. Sollte es hier zu Problemen oder Fehlern kommen, muss beim Aufbau der Infrastruktur überprüft werden, ob auch alle Netzeinstellungen korrekt vorgenommen worden sind. Treten größere Probleme auf, müssen die anhand der geführten Dokumentation überprüft und behoben werden. Ansonsten sei nochmal erwähnt, dass diese Tests entsprechend geplant und durchgeführt werden müssen. Möglicherweise müssen bei größeren Abhängigkeiten die Tests auf betriebsarme Zeiten (Wochenende, Abend-/Nachtstunden) festgelegt werden.
Sind alle Punkte der Test Suite erfolgreich gewesen, ist die Testphase abgeschlossen, ansonsten geht es wieder in die vorherige Phase (siehe Abbildung 5.1). Im nächsten Schritt wird nun die Sicherung für diesen Use Case eingeführt. Welche Punkte dabei beachtet werden müssen, wird im nächsten Abschnitt besprochen.

5.4 Sicherung und Disaster Recovery einführen

Nachdem die Umsetzung des Use Cases erfolgt ist und dessen Tests erfolgreich war, gilt es nun im nächsten Schritt ein Sicherungssystem einzuführen. Überlegungen zu einem entsprechenden Konzept müssen bereits in der Vorbereitungsplanung entstanden sein, weil sich hier die Frage entscheidet, wie weit eine Sicherung (Backup) vorgenommen werden soll. Welche Arten der Sicherungen es gibt, werden hier nochmal kurz vorgestellt, um, je nach Wunsch, die vorhandene Technik auszuwählen. Die einfachste Möglichkeit ist die Verwendung der bereits eingesetzten Lösung im Rechenzentrum, auch für die virtuellen Maschinen zu übernehmen. Dabei handelt es sich in der Regel um eine der drei Möglichkeiten: Ein Vollbackup (komplette Datensicherung), einem inkrementellen Backup (Sicherung der Daten, welche sich seit dem letzten inkrementellen Backup verändert haben) sowie ein differentielles Backup (Sicherung der Daten, welche sich seit dem letzten Vollbackup verändert haben). Für die Datensicherung wird ein Backupserver benötigt, der mit den einzelnen Maschinen kommuniziert (meist mittels installiertem Agent). Je nach eingesetzter Software können mehrere Einstellungen vorgenommen werden, die festlegen, welche Daten, wann und wie gesichert werden. Diese Sicherungsmöglichkeiten stehen auch in der virtuellen Maschine zur Verfügung und können daher entsprechend verwendet werden. Bei migrierten Maschinen ist meist eine Backupsoftware oder ein Agent installiert, der ab sofort weiterverwendet werden kann. Bei neu angelegten Maschinen, muss die gewünschte Sicherungssoftware installiert und eingerichtet werden. Danach erfolgt eine Einbindung in das bestehende System und die Sicherung unterscheidet sich nicht von physikalischen Hosts.
Virtuelle Maschinen bieten die Möglichkeit, eine Vollsicherung wesentlich einfacher zu gestalten, als dies bei physikalischen Geräten der Fall ist. In der Regel besteht eine VM aus wenigen Dateien, wie virtuelle Platte(n), Konfigurationsdaten und möglichen Snapshotdaten. Des Weiteren befinden sich die VMs auf einem Datenspeicher, der meist in einem SAN integriert ist. Dies gewährleistet, beispielsweise bei Fibre Channel, eine schnelle Datenanbindung, was auch für eine Sicherung von Vorteil ist. Wird jetzt eine Vollsicherung

durchgeführt, muss nicht für das jeweilige Betriebssystem eine Datensicherung installiert und durchgeführt werden, sondern es können die wenigen Dateien der VM gesichert werden. Meist befindet sich im SAN auch ein entsprechendes Gerät (z.B. ein Bandlaufwerk), das Zugriff auf den Datenspeicher der VMs hat. Über das Netzwerk können, je nach Einstellung, die virtuellen Maschinen dann komplett gesichert werden. Dabei muss beachtet werden, dass bei dieser Lösung die VM ausgeschaltet sein muss, da sonst die Datenintegrität nicht gewährleistet werden kann. Bei hochverfügbaren Maschinen ist dies teilweise nicht möglich und es muss die Sicherung auf Dateiebene innerhalb der VM durchgeführt werden. Bevor die VM aktiviert wird, kann solch eine Sicherung durchgeführt werden. Dann ist im Fehlerfall gewährleistet, dass durch das Zurücksichern, die VM schnell wieder bereit steht.
Die bisherigen Lösungen basieren auf Drittherstellerprodukte, die unabhängig von Virtualisierung funktionieren. Bei der Sicherung auf Dateiebene oder dem Vollbackup einer ausgeschalteten VM spielt es keine Rolle für das Backupsystem, ob es sich um eine virtuelle oder physikalische Maschine handelt. Die Nachteile der Sicherung auf Dateiebene ist die Gewährleistung des Backupsoftware, dass dies für jedes verwendete Betriebssystem funktioniert. Des Weiteren ist in der Regel für jeden installierten Agenten eine Lizenzgebühr notwendig, was bei Testumgebungen (die aber trotzdem gesichert werden sollen) hohe Kosten verursachen kann. Bei der Vollsicherung muss die VM ausgeschaltet sein. Dies gilt es zu vermeiden, wenn Hochverfügbarkeit gewährleistet werden soll. Aus diesem Grund bieten einige Anbieter als auch manche Virtualisierungsprodukte speziell angepasste Backuplösungen an, die für virtuelle Maschinen besser geeignet sind. Diese basieren teilweise auf der Snapshot Technologie, die eine Sicherung im laufenden Betrieb zulässt. Die Funktionsweise eines Snapshots wurde in Abschnitt 3.2.2 bei *VMwares Consolidated Backup* erklärt, funktioniert aber auch bei anderen Lösungen nach ähnlicher Weise.
Nachdem die gängigsten Möglichkeiten der Sicherung vorgestellt wurden, wird nun die gewünschte Lösung eingesetzt. Eine Vollsicherung aller virtuellen Maschinen, bevor diese produktiv ans Netz gehen, ist einfach und unerlässlich. Dies kann mit jeder Backupsoftware bewerkstelligt werden. Damit ist die Ausgangsposition aller VMs gesichert. Werden weiterführende Sicherungen vorgenommen, muss dies an einer VM getestet werden. Daher gilt es, die verwendete Sicherungstechnik zu installieren und einzurichten. Danach erfolgt eine Sicherung der Testmaschine auf den Sicherungsspeicher (z.B. das Bandlaufwerk). Als letztes muss die Rücksicherung (Restore) getestet werden, denn erst dann gilt das System als erfolgreich. Handelt es sich um eine Datensicherung, werden bestimmte Dateien auf der Testmaschine gelöscht und es wird überprüft, ob diese wieder hergestellt werden. Bei einer Vollsicherung oder die Sicherung per Snapshots muss auch dies getestet werden, ob eine Rücksicherung erfolgreich war. Möglicherweise muss eine erneute Testphase eingeführt werden, die wieder alle Funktionen überprüft. Waren alle Tests erfolgreich, muss die Einrichtung auf allen notwendigen VMs durchgeführt werden. Hier können für jede VMs gegebenenfalls noch kleinere Testfälle durchprobiert werden, ob die Einrichtung überall korrekt war.
Als letzte Überlegung für diesen Schritt ist die Frage, ob die Virtualisierungsumgebung gesichert werden soll. Auch hier kann die Sicherung mit den bisherigen Backupprogrammen erfolgen. Meist wird ein Vollbackup der kompletten Platten vorgenommen und im Notfall zurückgesichert. Wie für virtuelle Maschinen, gibt es hier Hersteller, die für eine bestimmte Virtualisierungsumgebung Implementierungen anbieten, um diese schneller und öfter zu sichern. Je nach Budget, Handhabung und Nutzen, muss hier die Sicherung wie gewünscht vorgenommen werden. Meist reicht eine Komplettsicherung der Umgebung mit den herkömmlichen Programmen. Auf Grund von Updates oder die Einführung neuerer Versionen sollte in größeren Abständen, immer wieder eine Sicherung durchgeführt werden. Dazu muss sich die Maschine in einem „Wartungsmodus” befinden und steht in der Zeit nicht zur Verfügung. Nach Abschluss des Backups wird der Host in den Ressourenpool aufgenommen und kann wieder verwendet werden.

Nach Einführung und ausführlichen Testen des Sicherungssystems, stehen nun die virtuellen Maschinen für einen Produktiveinsatz bereit. Bevor diese aber endgültig in Betrieb genommen werden, wird noch die Sicherheit der Umgebung geprüft und gegebenenfalls angepasst. Die dafür notwendigen Punkte werden im nächsten Abschnitt beschrieben.

5.5 Sicherheit der virtuellen Umgebung gewährleisten

In Abschnitt 3.3.4 wurde bereits detailiert auf die auftretenden Probleme bei virtuellen Umgebungen eingegangen. Gerade der Befall von „Virtual Maschine Based Rootkits” (VMBRs) können erheblichen Schaden verursachen. Diese Rootkits sind schwer zu entdecken und es existieren zur Zeit noch keine allumfassende Abwehrlösungen (siehe Abschnitt 3.3.4). Wie in dem oben benannten Abschnitt beschrieben, können diese nur auf Grund von Indizien und bestimmten Unregelmäßigkeiten entdeckt werden. Ein möglicher Test könnte beispielsweise mit dem Rootkit „Subvirt” durchgeführt werden, dessen Implementierung für Windows mit *Virtual PC* und Linux mit VMware vorhanden ist (vgl. [KiCh 06]). Dies zeigt die Gefahren eines Rootkits und kann die Administratoren schulen, auf welche Punkte zu achten sind, um solche VMBRs zu bemerken. Idealerweise wird das Eindringen selbst schon bemerkt und verhindert. Bei virtuellen Maschinen muss daher genauso der Schutz gegen Bedrohungen von Außen vorgenommen werden. Hier gilt es, diese in die bestehende Sicherheitsumgebung einzubinden, so dass keine VM als Angriffspunkt von Außen dient. Die Einführung des Sicherheitskonzeptes muss in Absprache mit dem zuständigen Administrator erfolgen. Meist erfolgen auch hier Sicherheitstests, um zu überprüfen, ob alle Einstellungen korrekt vorgenommen worden sind. Dies kann von sicheren Passwörtern, über die Installation der neuesten Patches, bis zu Angriffen auf Sicherheitslücken alles enthalten, was für notwendig erachtet wird. Dies sollte auch für jede virtuelle Maschine durchgeführt werden, denn falls eine befallen ist, kann das wesentlich größere Auswirkungen haben, als der Befall eines physikalischen Servers. Dies liegt daran, dass die Grenzen, die eine VM von einer anderen trennt, einfacher überwunden werden können. Aus diesem Grund sind die anderen laufenden VMs auf einem Host auch in Gefahr.

Auch hier gibt es neben dem vorhandenen Sicherheitskonzept speziell angepasste Lösungen, die Erweiterungen für die Virtualisierungsumgebung mitbringen. Dazu werden eigene sichere virtuelle Infrastrukturen auf dem Host erzeugt, der dann alle darauf laufenden VMs überwacht und entsprechend bei Gefahr reagiert. Fällt die Entscheidung für dieses oder ein ähnliches Produkt, sollte auch dies eingerichtet und ausführlich getestet werden. Dazu sind auch hier Testfälle durchzuführen, um bestimmte Angriffe zu simulieren. Mit Hilfe von sogenannten „Honeypots[1]” kann dies getestet und realisiert werden. Erfolgt ein Zugriff auf solch einen Honigtopf, existiert eine Schwachstelle im Netz, die ermittelt werden muss.

Sind alle Sicherheitslösungen implementiert und getestet worden, steht das System für den Produktiveinsatz bereit. Idealerweise erfolgt an dieser Stelle nochmal eine Vollsicherung der bestehenden Maschinen, wenn alle Sicherheitskriterien integriert sind (siehe Pfeil in Abbildung 5.1). Die Inbetriebnahme wird dann im nächsten Abschnitt beschrieben.

5.6 Produktive Inbetriebnahme

Die bisherigen Schritte dienen als Voraussetzung, um die virtuellen Maschinen in Betrieb nehmen zu können. Erst wenn alle vorangegangenen Schritte erfolgreich sind, ist gewährleistet, dass die VMs arbeiten, gesichert werden und über die notwendige Sicherheit verfügen. Beim „Umschalten” auf die virtuellen Maschinen ist nun wichtig, wie im Schritt 5.2.3 vorgegangen wurde. Sind die Maschinen nach der Migration nicht verändert worden, können sie direkt eingesetzt werden. Dies kann beispielsweise über ein Wochenende vorgenommen werden, bei dem die physikalische Maschine abgeschaltet und die virtuelle Maschine hochgefahren wird. Wurde die Maschine für die Testphase geändert, müssen entweder wieder die ursprünglichen Daten eingetragen werden (Maschinenname, IP Adresse, etc.) oder die VM wird mit dem neuen Namen in die Architektur integriert. Dazu muss gewährleistet sein, dass alle notwendigen Stellen informiert werden. Möglich wäre eine Weiterleitung bei der Namensauflösung des Servers. So erfolgt beim Aufruf des alten Servernamens, mittels Eintrag im DNS Server, ein Verweis auf den neuen virtuellen Server. Dadurch ist zumindest im Netzwerk die Erreichbarkeit des Servers gewährleistet. Wird von anderen Personen der Name des Servers benötigt, muss dieser entsprechend mitgeteilt werden. All diese Einstellungen müssen im Vorfeld vorgenommen werden, bevor entgültig die VMs ans Netz genommen werden.

[1] Als “Honeypot” (Honigtopf) wird ein Dienst bezeichnet, der die Aufgabe hat, Angriffe auf ein Netzwerk zu protokollieren. Dieser Dienst kann ein Programm sein, das einen oder mehrere Dienste zur Verfügung stellt, oder ein Server. So ein Hongigtopf dient sowohl zur Überwachung als auch als Sicherheitseinstufung des Netzwerkes. Dieser unterscheidet sich nicht von einem herkömmlichen Dienst oder Server, aber bei dessen Benutzung wird der Administrator informiert.

Befinden sich die Maschinen in der Produktivumgebung, ist in der ersten Laufzeit ein erhöhte Beobachtung (Monitoring) sinnvoll, um auf plötzliche Probleme reagieren zu können. Dies kann beispielsweise daran liegen, dass es eine etwas andere Nutzung der Server gibt, als dies in einer Testumgebung oder mit Test Suites nachgebildet werden kann. In einer Produktivumgebung können daher durch die Nutzer Probleme auftreten, die erst jetzt festgestellt werden können. Solche Vorkommnisse treten nur in seltenen Fällen auf, denn im Vorfeld (siehe Abschnitt 5.1) sind Nutzungsprofile berücksichtigt und in die Folgeschritte eingeplant worden.
Neben des erhöhten Monitoring der virtuellen Umgebung, wird zeitgleich ein Benutzerhandbuch erstellt. Diese Dokumentation dient für zukünftige Umsetzungen und wie der Aufbau einer virtuellen Infrastruktur (für das hier vorliegende Produkt) durchgeführt wird. So liegt die Information in strukturierter Form für die Administratoren vor und es erleichtert die Einarbeitung in die Technologie. Zusätzlich muss möglicherweise ein Teil der Personen für die neue Technologie geschult werden. Ist die Umsetzung von einer bestimmten Person oder einem externen Dienstleister durchgeführt worden, ist es sinnvoll, alle dafür zuständigen Personen zu schulen und einzuarbeiten. Nur wenn sich die Personen genau mit der Infrastruktur auskennen und die Technik verstehen, wissen sie, wie im Anforderungs- und/oder Fehlerfall zu reagieren ist. Mit dieser Maßnahme ist der Schritt abgeschlossen, sowie die komplette Vorgehensweise.
Als finale Überprüfung des Konzeptes kann von unabhängiger Stelle die Virtualisierungsumgebung dem Anforderungskatalog gegenübergestellt werden. Bei dem Katalog müssen für praxistaugliche Umsetzung alle Anforderungen der Gruppe I und II erfüllt sein. Nur in Ausnahmefällen dürfen Punkte der zweiten Gruppe nicht erfüllt sein. Anforderungen der dritten Gruppe ermöglichen eine weitere Verbesserung des Arbeitens, sind aber nicht unbedingt nötig. Fällt diese Prüfung positiv aus, ist das Konzept erfolgreich abgeschlossen.

Mit diesem Abschnitt endet das Kapitel, in dem alle wichtigen Schritte für eine erfolgreiche Hostvirtualisierung genannt worden sind. Dazu gehört das schrittweise Vorgehen aus der Abbildung 5.1 auf Seite 60, mit der Möglichkeit bestimmte Schritte erneut durchlaufen zu können. In der Praxis erhalten bestimmte Punkte eine größere oder geringere Wichtigkeit, als vielleicht hier vorgestellt wurde. Das hier vorgestellte Vorgehen orientiert sich an einem allgemeinen Anwendungsfall. Eine Anpassung an die vorliegende Situation ist ohne großen Aufwand möglich, indem die für den Use Case wichtigen Punkte herausgenommen werden. Um das vorliegende Konzept an einem praktischen Beispiel zu verdeutlichen, wird im nächsten Kapitel eine mögliche Realisierung vorgestellt. Dies erfolgt am Beispiel der Astrium GmbH, die mit ihrer vorliegenden Infrastruktur (siehe Abschnitt 4.1.2) ideale Voraussetzungen liefert, um mit Hilfe der Virtualisierung diese zu verbessern.

6 Realisierung

In diesem Kapitel erfolgt eine Umsetzung des vorangegangenen Konzeptes bei der Firma Astrium GmbH. Bereits in der Anforderungsanalyse wurden die Voraussetzungen und Probleme vorgestellt, die sich mit der aktuellen Infrastruktur ergeben. Zusammenfassend ist hier nochmal erwähnt, dass eine Vielzahl alter Server vorhanden sind, mit nur minimaler Auslastung der zugrundeliegenden Hardware. Die Verwaltung dieser Maschinen gestaltet sich komplex, da diese an unterschiedlichen Managementkonsolen angeschlossen sind und durch das Alter der Hardware ein erhöhtes Ausfallrisiko darstellen. Zusätzlich bietet die aktuelle Infrastruktur kaum Flexibilität, um auf Kapazitätsanfragen reagieren zu können. So steht nur ein begrenztes Platzangebot an Servern zur Verfügung, die des Weiteren durch Aufbau, Einrichtung und Konfiguration viel Zeit und deshalb Kosten produzieren, die nicht immer vom Budget abgefangen werden können. Aufgrund dessen, fiel die Entscheidung eine Virtualisierungsumgebung einzusetzen, die diese Probleme lösen kann. Da bisher noch keine Virtualisierung verwendet wurde, galt es diese, zu planen, einzurichten, aufzubauen, dokumentieren und in den produktiven Betrieb zu überführen.
Aus diesem Grund werden im ersten Schritt (Abschnitt 6.1) die spezifischen Vorgaben genannt, die für diesen Anwendungsfall von Bedeutung sind. Dazu zählt die Wahl der Virtualisierungsumgebung, auf die keinen Einfluss genommen werden konnte. Des Weiteren werden in diesem Abschnitt die Ziele genannt, die mit der Virtualisierung erreicht werden sollen. Dabei werden die zuvor genannten Use Cases (aus 4.1.3) noch einmal zusammenfassend dargestellt. Im darauffolgenden Abschnitt 6.2 erfolgt die Umsetzung des Konzeptes. Diese entspricht dem Ablaufdiagramm, an dem sich das Konzept orientiert. Welche Besonderheiten oder Anpassungen hier zu beachten sind, werden dabei vorgestellt. Dabei wird jeder Punkt des Konzeptes betrachtet und für den Anwendungsfall entsprechend eingeordnet. Auf die Umsetzung wird detailliert eingegangen, um die Implementiertung exemplarisch für diese Virtualisierungsumgebung vorzustellen.
Im letzten Abschnitt (siehe 6.3) dieses Kapitels wird auf auftauchende Probleme und Schwierigkeiten eingegangen, die es zu lösen gilt. Diese werden bewertet und führen zu Überlegungen, wie eine Optimierung des Konzeptes vorgenommen werden könnte. Ob diese auch sinnvoll sind oder es sich nur um spezifisch auftretende Probleme handelt, muss hier berücksichtigt werden. Mit diesen Überlegungen endet das Kapitel und die Realisierung ist abgeschlossen.

6.1 Gestellte Vorgaben und Ziele

Als obersten Rahmen für eine Umsetzung der vorangegangenen Use Cases mittels Virtualisierung, ist die Festlegung auf die Produkte von VMware. Insbesondere wird hier die *VMware Enterprise Infrastructure 3* (Enterprise Edition) eingesetzt. Diese beinhaltet neben den *ESX Server*, das *Virtual Center*, den *VMware Converter* und eine Backuplösung, das so genannte *Consolidated Backup for ESX Server*. Die einzelnen Komponenten wurden bereits in Abschnitt 3.2 beschrieben, dessen Anwendung hier erfolgt. Im Vorfeld wurde dieses Produktpaket ausgewählt, da sich dies gut in die bisherige Firmenstruktur eingliedert. Auf diesen Entscheidungsprozess konnte kein Einfluss genommen werden, womit ein Vergleich oder die Wahl eines anderes Produktes (auf Grund zusätzlicher Vorteile) nicht möglich ist.
Neben der Vorgabe Produkte von VMware einzusetzen, gilt als oberste Prämisse die Kostensenkung. Dies soll durch Einsparung von Materialkosten (für neue Server), Verringerung des Zeitaufwands und durch vereinfachte Administration im Konfigurations- und Fehlerfall gelöst werden. Ist die Verwaltung bisher umständlich zu handhaben (siehe Abschnitt 4.1.2), soll nun durch eine einheitliche Managementkonsole, alle virtuellen Maschinen administrierbar sein. Diese Erleichterung kann so genannte „Manpower” einsparen, wodurch die Administratoren wieder Zeit für andere Aufgaben haben.
Eine weitere wichtige Vorgabe ist, dass neben der Funktionalität auch ein Ausfallkonzept mit einfließen soll. Daher muss einerseits entsprechende redundante Hardware eingeplant werden, wie einen weiteren ESX Server und andererseits muss der Datenspeicher mit den enthaltenen VMs gesichert werden, so dass im Fehlerfall die

gespeicherten VMs auf einen anderen Speicher zurückgesichert werden können. Diese Punkte sind auch im Konzept vorhanden und werden an gegebener Stelle behandelt. Zusätzlich werden durch die Einbindung in die bestehende IT Infrastruktur die Server im vorhandenen Sicherheitskonzept bezüglich Integrität und Zugriffsschutz der Daten eingeordnet.
Grundlegend basiert die Virtualisierungsumgebung auf mehreren Servern von HP[1], genauer dem Modell DL385 G2. Ausgestattet ist jeder Server mit zwei Dual-Core Prozessoren von AMD der Opteron Serie (2,4 GHz, 68 Watt), 16 GB DDR2 Arbeitsspeicher (2 GB Speicherbausteine pro Steckplatz) und vier 36 GB SATA Festplatte im Raid 0+1 Verbund. Diese Serverkonfiguration eignet sich, laut Spezifikation (vgl. [vmh 07]), für die verwendete Software von VMware.

Aus den vorangegangen Aufgaben ergeben sich die folgenden drei Ziele:

1. Aufbau, Einrichtung und Konfiguration der *VMware Infrastructure 3* Umgebung, so dass die Infrastruktur für virtuelle Umgebungen zur Verfügung steht. Dies beinhaltet Installation zweier ESX Server, Konfiguration an die zugrundeliegende Netzarchitektur, Anbindung des gemeinsamen Speichers mittels SAN (Fibre Channel) an die Server. Konfiguration der Managementkonsole, genannt *VMware VirtualCenter*, um alle weiteren Einstellungen darüber vornehmen zu können. Zusätzlich ist im *Infrastructure 3 Enterprise* Paket noch der *VMware Converter* dabei, der zur Migration von physikalischen zu virtuellen (P2V) Maschinen dient. Diesen gilt es, für das folgende Ziel zu verwenden.

2. Virtualisierung aller vorhandenen NT4 Server: Auf diesen Servern läuft noch eine alte Domäne auf Basis von *Windows NT4 Server*, deren Auslastung der zugrundeliegenden Hardware minimal ist. Des Weiteren ist noch ein Druckerserver im Einsatz, der gleichzeitig als Domänencontroller fungiert. Diese beiden Funktionen gilt es zu trennen und jeweils auf einer virtuellen Maschine laufen zu lassen. Für Testumgebungen und Simulationen wird ein Template auf Basis von NT4 benötigt, da alte Entwicklungsumgebungen dieses Betriebssystem zwingend voraussetzen. Mit dem erstellten Template soll ein Druckerserver als Backup (aus firmenspezifischen Gründen) erstellt werden.

3. Bereitstellung von virtuellen Servern bei Projektanfragen. Mit Hilfe der Template Funktion, die im vorherigen Punkt schon erwähnt wurde, wird ein *Windows 2003 Server* erstellt und falls für Testumgebungen oder Projekte ein Server benötigt wird, kann unter bestimmten Umständen ein virtueller Server verwendet werden. So ist eine schnellere Reaktion auf solche Anfragen möglich, wenn die Rahmenbedingungen stimmen. So muss zum Beispiel vorher geklärt werden, ob die Anforderungen mit der aktuellen Auslastung vereinbar ist. Außerdem gilt zu beachten, dass nicht jeder Server als VM betrieben werden kann. Gerade wenn es sich um einen Datenbankserver mit hohen E/A Operationen handelt, sollte ein eigenständiger physikalischer Server verwendet werden. Ob ein virtueller oder physikalischer Server zum Einsatz kommt, kann nur der Administrator aufgrund seiner Erfahrung, eines Aufgabenszenarios vom Projektleiter und statistischen Werten entscheiden und dementsprechend handeln.

Diese drei Ziele werden im nächsten Abschnitt aufgespaltet, da die Einrichtung der Infrastruktur als Voraussetzung für die anderen beiden Punkte dient. Anhand des Konzeptes erfolgt die Umsetzung der Ziele und deren Randbedingungen, wie Backuplösung und Sicherheit.

6.2 Umsetzung des Konzeptes

Dieser Abschnitt befasst sich mit der Umsetzung des Konzeptes, wie es zuvor in Kapitel 5 erarbeitet wurde. Darin bietet jeder der genannten Schritte einen Unterpunkt, wobei es zwei Ausnahmen gibt. Die Voraussetzungen sind bereits ausreichend geklärt worden, so dass eine Virtualisierung hier sinnvoll ist. Es ist eine Analyse der möglichen Server erfolgt und findet in den vorgestellten Anwendungsfällen die entsprechende Anwendung. Zusätzlich wurden die Entscheidungen für eine Virtualisierungsumgebung, der Backuplösung und anderer Punkte vorab getroffen, so dass mit einer Umsetzung beginnen kann. Des Weiteren erhält die Umsetzung der Use Cases einen gesonderten Punkt und fällt nicht unter die „Installation der Infrastruktur” wie im

[1] Die Hewlett-Packard Company; eine US-Technologiefirma mit großen Geschäftsanteilen unter anderem im Serverbereich.

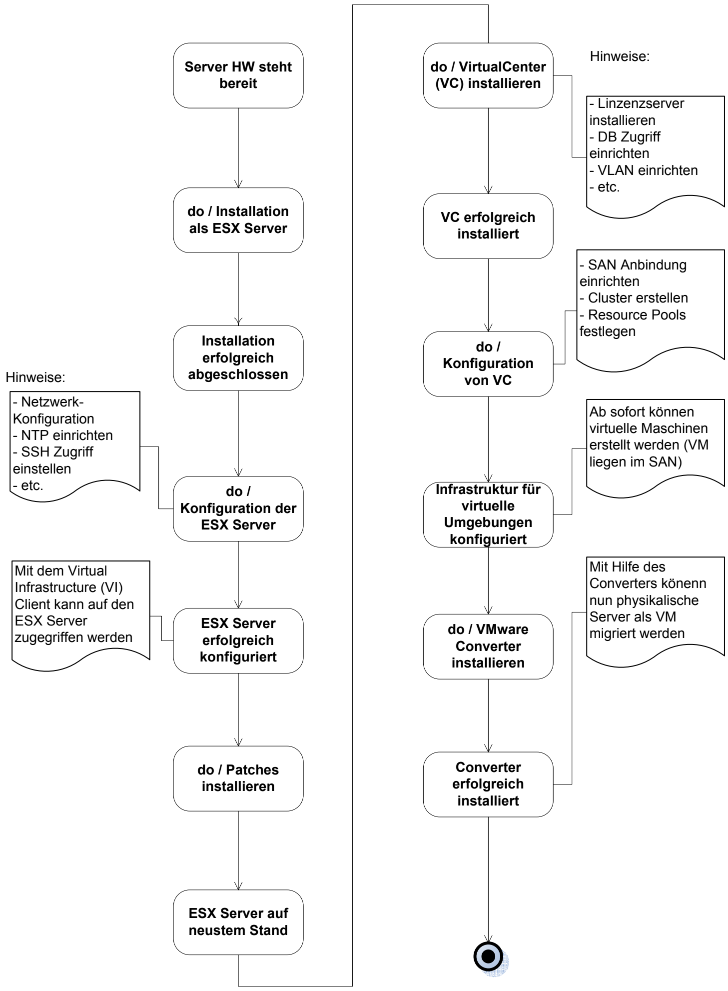

Abbildung 6.1: Aktivititätsdiagramm über die Einrichtung einer Infrastruktur zur Nutzung der virtuellen Umgebung

Konzept beschrieben. Daher wird im nächsten Abschnitt mit der Einrichtung der Virtualisierungsumgebung begonnen, bevor auf die Use Cases eingegangen wird.

6.2.1 Aufsetzen und Konfigurieren der ESX Server

Der Ablauf der Umsetzung ist als Zustandsdiagramm (in Anlehnung an UML[2]) in Abbildung 6.1 dargestellt. Dieser zeigt das schrittweise Vorgehen bei der Umsetzung, auf das jetzt genauer eingegangen wird.
Für die Installation der ESX Server müssen die entsprechenden Server (von HP) aufgebaut und angeschlossen sein. Über einen Monitorswitch kann die Installation der Server gesteuert und überwacht werden. VMware bietet immer die neueste Version des ESX Servers als ISO Image auf ihrer Homepage an, das nach erfolgreicher Registrierung heruntergeladen werden kann. Mittels dieser CD erfolgt die Installation, die anhand der entsprechenden Anleitung vorgenommen werden muss. Einzige Besonderheit ist die Partionierung der internen Festplatte. Da es sich um ein eigenes Betriebssystem, in Anlehnung an Red Hat Linux, handelt, werden hier mehrere Partitionen angelegt, je nach Wunsch und Notwendigkeit. In Tabelle 6.1 ist eine Konfiguration zu sehen, wie diese ausfallen könnte. Dabei werden für alle wichtigen Bereiche eigene Partitionen angelegt. Die ersten drei Partitionen werden für den Bootvorgang benötigt, es handelt sich dabei um eine typische Einrichtung. Auffällig sind die beiden Partitionen mit dem Dateisystem „Vmkcore” und „Vmfs3”. Diese Partitionen

[2] hier: Unified Modeling Language

Name der Platte	Filesystem	Größe der Platte	Primary ja/nein
/boot	Ext3	100MB	Ja
/ = root	Ext3	5.000MB	Ja
leer	Swap	1.000MB	Ja
/home	Ext3	1.000MB	Nein
/tmp	Ext3	3.000MB	Nein
/var	Ext3	3.000MB	Nein
leer	Vmkcore	100MB	Nein
leer	Vmfs3	10.000MB	Nein
vmimages	Ext3	fill to max	Nein

Tabelle 6.1: Mögliche Festplattenkonfiguration der ESX Server

sind notwendig, wenn der Host nicht über einen externen Datenspeicher verfügt (vgl. [vmh 07]). Mit Hilfe dieser Partitionen können lokal virtuelle Maschinen gespeichert und verwendet werden. Dies ist sinnvoll, wenn im Notfall (Wegfall des Datenspeichers) wichtige Maschinen lokal auf dem Server gespeichert werden sollen. Mit der hier vorliegenden Konfiguration (ca. 10 GB) lässt das in der Regel eine VM zu und war gewünscht. Die letzte Partition dient für Daten aller Art, beispielsweise die Lagerung von ausgeschalteten VMs. Die Größe dieser Partition orientiert sich an der noch zur Verfügung stehenden Restkapazität und hängt von der verwendeten Platte des Hosts ab. Nach Abschluss der Plattenkonfiguration erfolgen noch einige wenige Einstellungen, wie Netzwerkeinstellungen, Zeitzone oder Root Passwort. Die Installation ist nach kurzer Zeit abgeschlossen und der ESX Server kann per eingerichteter IP Adresse angesprochen werden. Falls über einen Servernamen kommuniziert werden soll, muss dieser entsprechend in einen DNS Server eingetragen werden.
Nach der Installation, erfolgt die Einrichtung des ESX Servers. Dazu wird im ersten Schritt der SSH (Secure Shell) Zugriff aktiviert, um ab sofort mittels SSH Programm und nicht über den Monitorswitch auf den Server zuzugreifen. So kann die jeweilige Konsole der Server von einem internen Firmenrechner mittels SSH angesprochen und konfiguriert werden. Daher erfolgen die künftigen Zugriffe auf einen ESX Server mittels SSH Programm. Mit diesem wird im nächsten Schritt die NTP (Network Time Protocol) Konfiguration vorgenommen. Eine synchronisierte Zeit ist für die Kommunikation mehrerer ESX Server notwendig, denn sonst arbeiten bestimmte Funktionen wie *VMwares High Availability* nicht korrekt. Die verwendeten HP Server erhalten eine Besonderheit: Die *HP Management Agents for ESX Servers*. Mit diesen Agenten können über das zentrale Managmentprogramm von HP eine Vielzahl an Informationen ausgelesen werden. Dadurch ist eine Überwachung der integrierten Komponenten möglich und der Administrator wird über Komponentenausfälle informiert. Mit dieser Installation ist die Konfiguration soweit abgeschlossen.
Im nächsten Schritt erfolgt das etwas umständliche Patchen der ESX Server. Es gibt keine automatische Routine, die überprüft, ob neue Patches erhältlich sind. Deshalb erfolgt weder das Herunterladen, noch die Installation automatisch. All diese Schritte müssen per Hand vorgenommen werden. So muss auf der Homepage von VMware (`http://www.vmware.com/download/vi`) von Zeit zu Zeit überprüft werden, ob neue Patches verfügbar sind. Ist dies der Fall, müssen diese heruntergeladen und auf die Server kopiert werden. Danach muss jeder Patch entpackt und mittels speziellen ESX Befehls installiert werden. Auf der Homepage ist angegeben, ob der Patch einen Neustart benötigt oder nicht. Dies ist in dieser Phase der Installation noch unerheblich, da noch keine VMs laufen, aber für den späteren Betrieb ist dies von Bedeutung. Sicherheitshalber sollte der ESX Server bei Wartungsarbeiten durch Patches in den sogenannten „Maintenance Modus" gefahren werden, der gewährleistet, dass in diesem Modus keine VMs beeinflusst werden. Ist die Prozedur für einen Patch abgeschlossen, muss das Verfahren für jeden weiteren Patch wiederholt werden. Dies kann bei mehreren ESX Servern und Patches einige Zeit in Anspruch nehmen, die auch später eingeplant werden muss. Momentan gibt es keine Verbesserung dieser Situation.
Nachdem nun alle ESX Server auf dem neuesten Stand sind, wird im nächsten Schritt zuerst der *Virtual Infrastructure Client* (VI Client) installiert, um sowohl die ESX Server, als auch später den *Virtual Center Server* (VC Server) mit einer grafischen Oberfläche zu verwalten. Dies vereinfacht die Konfiguration des Netzwerks, die zuerst erfolgen muss. Dazu werden die freien Netzwerkports (hier: vier) zugeordnet, um den Netzverkehr zuzuteilen. Der Host hat dazu zwei interne Netzwerkports auf dem Mainboard und eine zusätzliche Steckkarte mit zwei weiteren (externen) Ports. Diese müssen nun so aufgeteilt werden, dass bei Ausfall des internen oder externen Netzwerks, dennoch die virtuellen Maschinen, die Service Konsole und der *VMkernel*, der für spätere Dienste, wie *VMotion* benötigt wird, noch arbeiten können. Aus diesem Grund bekommen die virtu-

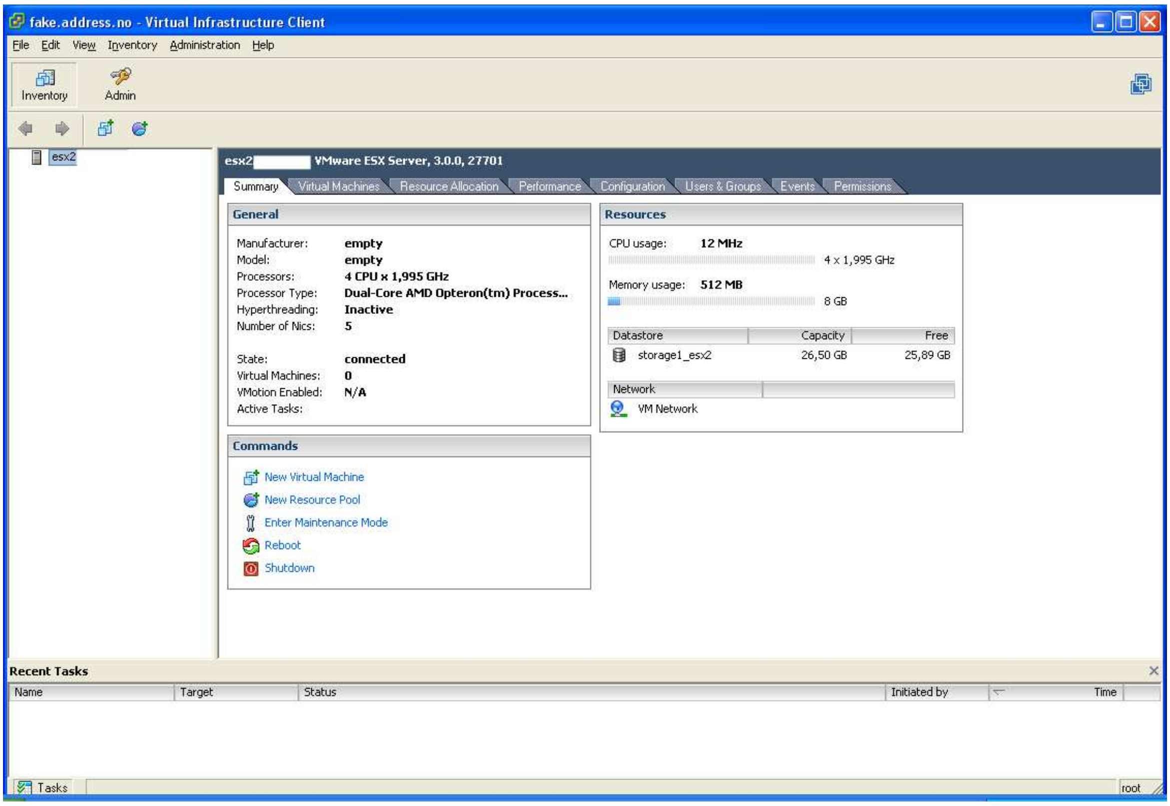

Abbildung 6.2: Grafische Oberfläche des VI Clients für einen ESX Server

ellen Maschinen exklusiv einen internen und einen externen Port zugewiesen. Die Service Konsole erhält den zweiten internen Port und als Ausfallsicherheit den zweiten externen Port. Über den wird nur kommuniziert, wenn der erste nach einem gewissen Timeout nicht mehr reagiert. Diese Funktion bietet VMware in ihrem Konfigurationsmenü an. Als letztes bekommt der *VMkernel* den zweiten externen Port als primäre Schnittstelle und den zweiten internen als Ausfallschutz. Damit sind alle Funktionen eingerichtet und abgesichert. Bei Ausfall von einem Port können weiterhin alle Funktionen (mit Einschränkungen) genutzt werden. Diese Konfiguration muss für alle ESX Server erfolgen, bevor die Installation des VC Servers vorgenommen werden kann. Für diesen wird ein Rechner mit Windows 2003 Server (Win2003) Betriebssystem benötigt, um den VC Server installieren zu können. Außerdem muss er alle zu verwaltenden ESX Server (hier: zwei) erreichen können. Daher bietet es sich an, diesen auch als virtuelle Maschine zu betreiben. Aus diesem Grund wird mittels VI Client auf einen der ESX Server verbunden (siehe Abbildung 6.2) und dort eine virtuelle Maschine eingerichtet. Da bisher noch keine Konfiguration des Datenspeichers erfolgt ist, wird diese nun lokal auf dem verbundenen ESX Server aufgesetzt und gestartet. Später erfolgt eine Verschiebung in den externen Datenspeicher. Alle Konfigurationen werden dann später mit dem Virtual Center erledigt und erfolgen im nächsten Schritt. Nach dem Anlegen der VM, geschieht die Installation des notwendigen Betriebssystem, nach einer firmenspezifischen Anleitung. Nach Abschluss der Installation, steht die VM bereit und es kann der Virtual Center Server eingerichtet werden. Auch dieser ist über die Homepage oder mitgelieferter CD zu beziehen und wird mittels Installationsroutine konfiguriert. Dabei übernimmt dieser mehre Aufgaben: So fungiert der VC Server als Lizenzserver für alle kostenpflichtigen Optionen und Produkte. Diese Lizenzen müssen zuvor auf der VMware Homepage registriert werden, um eine Lizenzdatei zu erhalten, die der Server benötigt. Dieser überwacht und verteilt die Lizenzen, für die Server, die er später verwaltet. Diese Zuteilung erfolgt dynamisch, so dass gerade nicht eingesetzte Funktionen bei einem Server bei einem weiteren verwendet werden können. Neben dem Lizenzserver erfolgt die eigentliche Installation des VC Servers. Dazu wird eine Datenbank benötigt, die hier mit einem Microsoft SQL Server bereit steht. Nach Anbindung der Datenbank kann die Installation abgeschlossen werden und der VC Server steht als Windows Systemdienst zur Verfügung. Ab sofort erfolgt die Anmeldung nicht mehr direkt auf einen ESX Server, sondern an den Virtual Center Server. Als Programm dient dafür weiterhin der VI Client, dessen Oberfläche sich nicht geändert hat, aber es stehen

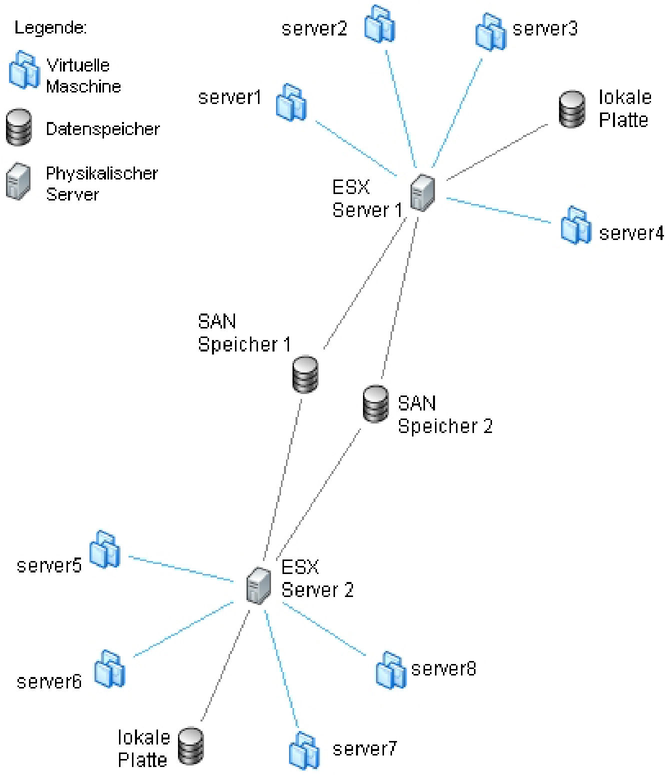

Abbildung 6.3: Abbildung der Zusammenhänge von VMs, Hosts und dem Datenspeicher mittels der Funktion „Maps" im Virtual Center. Anmerkung: Alle Namen wurden aus Sicherheitsgründen ersetzt.

nun neue Optionen zur Verfügung.
Mit dem Virtual Center kann nun die Einrichtung der Infrastruktur erledigt werden. Dazu wird ein so genanntes „Datacenter" erstellt, in dem alle ESX Server eingebunden werden. Des Weiteren erfolgt ein neues Cluster im Datacenter, indem Ressourcen Pools angelegt werden können. Ressource Pools dienen zur Einordnung von VMs, für die unterschiedliche Bedingungen gewährleistet werden sollen (genaueres dazu siehe in Abschnitt 3.2.2 in Abbildung 3.10 auf Seite 25). Ist diese Einrichtung erfolgt, muss jetzt der Datenspeicher eingerichtet werden. Dazu wurden im Vorfeld die ESX Server ans SAN mittels Fibre Channel angeschlossen, um Zugriff auf den Datenspeicher zu haben. Auf diesem wurden zwei LUNs angelegt, die für virtuelle Maschinen zur Verfügung stehen. Diese gilt es, mittels VC entsprechend einzurichten, damit der Datenspeicher für alle ESX Server bereit steht. Ist die Anbindung erfolgreich, ist die Grundkonfiguration fertig gestellt und es könnte mit der Einrichtung von VMs begonnen werden. Bevor dies aber im nächsten Schritt erfolgt, werden als letztes im angelegten Cluster noch „High Availability" (HA) und das „Distributed Ressource Scheduling" (DRS) eingerichtet. Daraufhin steht die Infrastruktur bereit und kann genutzt werden.
Für die Umsetzung des erstem Anwendungsfalls wird noch ein Programm benötigt, dass die Migration der physikalischen Maschinen vornimmt. Dabei wird der *VMware Converter* eingesetzt, der alle gewünschten Funktionen mitliefert. Dieser Konverter funktioniert auch nur unter einem Windows Betriebssystem und wird hier auf einer eigenen VM installiert, die nebenbei auch als Testmaschine dient. Da der Konverter nicht dauerhaft verfügbar sein muss, sondern nur wenn er benötigt wird, kann er auf einer beliebigen Maschine installiert werden, die eine Verbindung zum Virtual Center hat. Für die Installation sind keine besonderen Einstellungen notwendig und der Konverter steht nach kurzer Zeit zur Verfügung. Mit dieser Installation ist nun die komplette Voraussetzung gegeben, um die Use Cases umzusetzen. Zuvor wird in den folgenden Unterpunkten nochmal detailliert auf das Einrichten von virtuellen Maschinen und auf verwendete Programme, die nicht von VMware bereitgestellt werden, eingegangen.

Einrichten virtueller Maschinen

Wie die zuvor vorgenommenen Einstellungen, funktioniert auch das Einrichten einer virtuellen Maschine über den Virtual Center Server. Ein entsprechender Menüpunkt ist für die Erstellung vorhanden und wird im ersten Schritt ausgewählt. Danach erscheint ein Konfigurationsmenü, in dem alle notwendigen Daten angegeben werden. Zuerst wird festgelegt, wie der Name der VM lautet und wo sie eingeordnet wird. Dies kann entweder in einen Ressource Pool oder auf einem bestimmten Host sein. Der Vorteil der ersten Möglichkeit, ist die Abkoppelung von einem bestimmten Server. Die Verteilung und die Garantie für bestimmte Ressourcen übernimmt das Virtual Center in Kombination mit DRS. Das VC verschiebt die Maschinen im laufenden Prozess und versucht, je nach Einstellungen der Pools, die bestmöglichen Voraussetzungen für diese zu bieten. Auch bei der Erstellung einer VM, wählt das VC den Host aus, auf dem sich die zukünftige VM befinden soll. Bei der zweiten Möglichkeit, kann explizit ein Host angegeben werden, falls dies aus bestimmten Gründen notwendig ist. Im vorliegenden Fall, wurden die Maschinen immer Ressource Pools zugeordnet.
Nach Namen und Pool, muss angegeben werden, wo die virtuelle Platte gespeichert werden soll. Hier steht entweder die lokale Platte oder der externe Datenspeicher, in Form der LUNs zur Verfügung. Im Normalfall werden alle VMs in den LUNs gespeichert. Im nächsten Schritt erfolgt die Auswahl des Betriebssystems, welches später installiert werden soll. Dies ist für das VC wichtig, um auf spezifische Befehle des Gastes besser reagieren und dadurch performanter arbeiten zu können. Des Weiteren erfolgt die Auswahl der virtuellen Prozessoren (1, 2 oder 4), die durchgereicht werden sollen. Unabhängig wie viele Prozessorkerne zur Verfügung stehen, der VM können nicht mehr als vier Kerne übergeben werden. Die letzten Einstellungen beschäftigen sich mit der Wahl des Hauptspeichers, die Anzahl der Netzwerkports (ein oder zwei) und zuletzt die Größe der virtuellen Platte. Diese kann entweder neu angelegt werden oder es existiert bereits eine, die hier eingebunden werden soll. Zusätzlich können weitere Platten erstellt und ausgewählt werden. Bevor die Konfiguration komplett ist, muss als letztes noch die Bootplatte ausgewählt werden. In einem Übersichtsfenster sind alle Einstellungen nochmal dargestellt, bevor das Anlegen beginnen kann. Nach der Erstellung steht die VM im Virtual Center bereit und kann mit dem Gastsystem installiert werden. Dies kann mit den drei beschriebenen Möglichkeiten aus Abschnitt 5.2.2 geschehen: Durchgereichtes Hostlaufwerk, per ISO Image oder mittels Netzboot. Bei Astrium existieren alle benötigten Betriebssysteme als ISO Image und wurden auf einen eigenen Datenspeicher abgelegt. Ist das Image über das Konfigurationssmenü eingebunden, kann die VM in der Konsole gestartet werden. Daraufhin bootet es von dem virtuellen CD Laufwerk und die Installation erfolgt wie bei einem physikalischem Host.
Nachdem mehrere VMs angelegt worden sind, gibt es mittels der Funktion „Maps" die Möglichkeit, eine Übersicht der Infrastruktur anzuzeigen (siehe Abbildung 6.3). Dies zeigt die Verbindungen, auf welchem Host die einzelnen VMs laufen und über welchen Datenspeicher die Hosts verbunden sind. Aus Sicherheitsgründen wurden in der Grafik alle vorkommenden Namen durch generische ersetzt, ansonsten sah die Virtualisierungsumgebung so aus, wie in der Abbildung dargestellt.

Neben den Programmen von VMware wurden zusätzlich noch einige weitere Tools verwendet, die für das produktive Arbeiten sinnvoll sind. Um welche es sich dabei handelt, wird im nächsten Punkt erklärt.

Zusätzliche Programme

Für die Umsetzung der Anwendungsfälle und zur Erleichterung mancher Aufgaben, sind noch einige Programme notwendig. Bevor es zur Realisierung der Use Cases kommt und als Überblick der verwendeten Tools, folgt nun eine Aufzählung dieser, mit einer kurzen Erklärung:

- Das SSH Programm *PuTTY* [put 07]; ein kostenfreies Programm, mit dem die SSH Verbindung zu den ESX Servern hergestellt wird. Dies wird benötigt, um sich per SSH auf die Konsole einzuwählen und beispielsweise das Patchen durchzuführen.
- Das Secure FTP Programm *WinSCP* [win 07b]; WinSCP ist ein grafischer Open Source SFTP Client für Windows, der SSH benutzt. Mit diesem können Dateien auf die ESX Server kopiert werden. Auch dies ist für das Patchen notwendig, denn die zuvor heruntergeladenen Patches, müssen auf die Hosts gelangen. Des Weiteren können Log- oder Konfigurationsdateien von den Maschinen kopiert und ausgewertet werden.

- Backupprogramm *Norton Ghost 12.0* [gho 07]; Dieses Programm dient später einerseits zur Sicherung der ESX Server (siehe Abschnitt 6.2.4) und kann andererseits als zusätzliches Migrationsprogramm eingesetzt werden. So ist es möglich, dass in der neuesten Version ein erstelltes Backup mit *Norton Ghost* in eine virtuelle Platte umgewandelt wird. Diese kann im nächsten Schritt in eine virtuelle Maschine eingebunden werden.
- Die Backupsoftware *Veritas NetBackup 6.0* [net 07b]; Diese Programm ist die eingesetzte Backuplösung im Unternehmen für die anfallenden Daten auf den Netzlaufwerken. Des Weiteren können mit *Netbackup* ausgeschaltete VMs auf ein Bandlaufwerk gesichert werden.
- *Microsoft Printer Migrator 3.1* [pri 07]; Mit diesem freien Programm von Microsoft können alle angelegten Drucker inklusive deren Treiber und Einstellungen exportiert und auf einem anderen Server exportiert werden. Das Programm unterstützt alle gängigen Windows Versionen und wird auch für den ersten Anwendungsfall benötigt.

Damit wurden alle verwendeten Programme vorgestellt, die hier zum Einsatz gekommen sind. Diese finden in den nächsten Abschnitt ihre Verwendung.

Insgesamt ist nun die Einrichtung der Infrastruktur abgeschlossen und steht für die Umsetzung der Use Cases bereit. Wie diese umgesetzt wurden, wird im nächsten Schritt genau vorgestellt.

6.2.2 Umsetzung der Use Cases

Bevor die Umsetzung der Use Cases durchgeführt wird, erfolgt eine Migration von zwei Testmaschinen. Dabei handelt es sich um zwei alte Softwareverteilungsserver, die immer noch in Verwendung sind, aber nur selten genutzt werden. Diese sollten als ersten Test der Umgebung dienen, da die Server bereits als virtuelle Maschinen unter *VMware Server* liefen. Mittels Konverter wurden sie in die neue Umgebung migriert und wurden zwei Wochen lang getestet. Dieser Test lief erfolgreich und somit stand einer Umsetzung des ersten Use Cases nichts mehr im Wege. Der genaue Ablauf beider Use Cases wird in den nächsten beiden Unterpunkten genau vorgestellt.

Virtualisierung der NT4 Domäne

Zuerst seien nochmal die Ziele der Umsetzung genannt, die mit diesem Anwendungsfall erreicht werden sollen:

- Virtualisierung der NT4 Domäne
- Virtualisierung des alten Druckerservers, der noch auf NT4 läuft
- Aufspaltung eines Druckerservers, der gleichzeitig als Domänencontroller (BDC) fungiert, in zwei eigenständige virtuelle Server
- Erstellen eines NT4 Templates für Simulationen und im Fehlerfall (falls eine virtuelle Maschine ausfällt und diese durch eine andere ersetzt werden muss; z.B. das SAN, in dem sich die virtuelle Maschine befindet ist, nicht mehr erreichbar)
- Einrichten eines Backup Druckerserver auf Basis von NT4

Um die Ziele zu erreichen, muss eine bestimmter Ablauf vorgenommen werden. Dieser ist im Folgenden kurz beschrieben und enthält jeweils einen Verweis auf das Ablaufdiagramm. Im Ablaufdiagramm sind alle Schritte genau vorgestellt, wie in jeder Situation zu reagieren ist.

Vorgehensweise: Alle Migrationen werden mit dem *VMware Converter* durchgeführt. Hinweise und Anmerkungen zu bestimmten Programmen, befinden sich auf den Ablaufdiagrammen. Als gesonderter Punkt sei hier genannt: Das Tool *UPromote* ist zwar in den Abläufen genannt, ist aber hier bei Astrium nicht zum Einsatz gekommen. Dennoch ist dies ein nützliches Programm, weshalb es trotzdem genannt wird. Es gibt aber auch immer die Möglichkeit, den Ablauf ohne *UPromote* zu bewerkstelligen. Dieser erfolgt in fünf Schritten und erhält nun eine kurze Beschreibung:

1. Virtualisierung eines BDCs, um im Vorfeld zu testen, ob in der gegebenen Umgebung eine Virtualisierung einer NT4 Maschine möglich ist. Dabei wird die physikalische Maschine mittels dem Converter migriert. Danach erfolgt ein kurzer Test, ohne Netzverbindung, ob die Migration erfolgreich war. Danach erfolgt die Testphase die im nächsten Abschnitt 6.2.3 besprochen wird. Läuft diese erfolgreich, können weitere Server virtualisiert werden (Ablauf siehe Abbildung 6.4 auf Seite 86).

2. Im zweiten Schritt wird ein weiterer BDC virtualisiert, der gleichzeitig als Druckerserver arbeitet. Dazu wird zuerst die Virtualisierung des Servers vorgenommen. Danach kommt ein kurzer Funktionstest der neuen VM. War dieser erfolgreich, wird die VM geklont und es existieren zwei identische Maschinen. Auf die erste VM (server2_1) wird das Tool *Upromote* installiert, dass die Trennung vornehmen soll. Falls dafür keine Lizenz vorhanden ist, sind die Alternativschritte angegeben. Dazu wird dann der *Printer Migrator* von Microsoft benötigt. Alle Möglichkeiten sind detailliert in Abbildung 6.5 auf Seite 87 vorgestellt.

3. Bei VMware können Templates erstellt werden, die im Bedarfsfall schnell zur Verfügung stehen. Dies ist hier notwendig, falls für Testzwecke ein NT4 Server benötigt wird oder bei einem irreparablen Ausfall dieser schnell ersetzt werden muss. Dies funktioniert über das Virtual Center, bei dem auch Templates eingerichtet werden können. Hier wird das NT4 Server Betriebssystem und alle bisherigen Service Packs installiert. Zu beachten ist, dass bei der Konfiguration die VM als Memberserver eingerichtet wird. Nach der Installation erfolgt die Netzwerkkonfiguration, damit die VM sofort verwendet werden kann. Zuletzt kann das Tool *UPromote* (bei vorliegender Lizenz) installiert werden, um im Notfall die VM als Domänencontroller einzurichten (Ablauf siehe Abbildung 6.6 auf Seite 88).

4. Aus dem zuvor erstellten Template wird im jetzigen Schritt ein zweiter Druckerserver als Backup erstellt. Dies hat Astrium-interne Hintergründe und ist für bestimmte Abläufe von Bedeutung. Dazu wird das Template in eine VM umgewandelt und konfiguriert. Auf der VM werden die gewünschten Drucker mittels des *Printer Migrator* importiert. Nach erfolgreichem Import, erfolgt die Testphase (Ablauf siehe Abbildung 6.7 auf Seite 89).

5. Als letzter Schritt wird der primäre Domänencontroller (PDC) virtualisiert. Dieser muss nun in der virtuellen Umgebung mit den BDCs kommunizieren. Die Virtualisierung des Servers erfolgt wie im ersten Schritt. Nach erfolgreichem Testen, muss der PDC konfiguriert werden. Durch die Erstellung zwei neuer VMs in Schritt 2, ist der Name des neuen BDCs nicht mehr bekannt und muss daher eingerichtet werden. Danach muss eine ausführliche Testphase vorgenommen werden, ob die Konfiguration auch erfolgreich war. Ist diese erfolgreich, sind alle gewünschten physikalischen Maschinen migriert worden und der Anwendungsfall ist abgeschlossen (Ablauf siehe Abbildung 6.8 auf Seite 90).

Wie die beschriebene Vorgehensweise zeigt, sind nach jedem Schritt Testphasen eingeplant. So wird nicht die komplette NT4 Umgebung virtualisiert, auf die ein gesamter Test erfolgt, sondern hier bietet sich die schrittweise Virtualisierung mit anschließendem Testen an. Dadurch wurde sukzessive ein Server migriert und in der vorhandenen Umgebung getestet. Eine genaue Beschreibung der Testphase erfolgt in Abschnitt 6.2.3.
Bevor es aber dazu kommt, wird im nächsten Punkt die Umsetzung des zweiten Anwendungsfall vorgestellt.

Bereitstellung virtueller Server auf Basis von Templates

Die Umsetzung dieses Anwendungsfalls stellt kaum Herausforderungen an die technische Seite. Wichtig sind die Vorbedingungen und der komplette Ablauf, der sich an der ITIL orientiert. Der Use Case wurde bereits in Abschnitt 4.1.3 detailliert besprochen und wird auch so umgesetzt. Der Ablauf der Umsetzung ist in Abbildung 6.9 auf Seite 91 dargestellt. Dazu wird im ersten Teil ein Template mit dem gewünschten Betriebssystem installiert. Dies ist im vorherigen Fall bereits mit dem NT4 Server System geschehen und steht als erstes Template zur Verfügung. Weitere Templates werden auf Basis von Windows 2003 Server und Windows XP erstellt. Windows 2003 Server ist das Standard-Betriebssystem, dass im Unternehmen eingesetzt wird - fast alle Serveranfragen basieren darauf. Windows XP wird für Tests in der IT Abteilung benötigt, um Fehlerfälle zu simulieren oder neue Programme zu testen. Sind die Templates erstellt und getestet worden, ist die erste Phase abgeschlossen. Erfolgt nun eine Anfrage für einen Server, wird diese überprüft, ob die Rahmenbedingungen

eingehalten werden können. Welche das genau sind, können im Abschnitt 4.1.3 nachgelesen werden. Kann die Anfrage von der technischen Seite her durchgeführt werden, muss zuvor ein Vertrag mit dem Projektleiter geschlossen werden. In diesem sind die Bedingungen und SLAs festgehalten, wie beispielsweise die Betreuung und die Abbrechnung des Servers erfolgen. Wie bereits in Abschnitt 4.3.3 erwähnt, kommt es hier zu keiner näheren Definition der SLAs. Dies würde den Rahmen der Arbeit sprengen und es laufen bei Astrium aktuell Projekte, um SLA Verträge nach ITIL zu formen.
Sind die Konditionen geklärt und von beiden Seiten akzeptiert, wird aus dem Template eine virtuelle Maschine erstellt. Diese wird an die zuvor festgelegten Bedingungen angepasst und eingerichtet. So muss Servername, IP Adresse und anderes konfiguriert werden. Als letztes müssen die Zugriffsrechte für den Projektleiter und mögliche andere Personen eingerichtet werden. Ist die Konfiguration komplett, erfolgt eine kurze Testphase, ob alle Einstellungen korrekt sind. Ist dies der Fall werden die Daten an den Projektleiter übergeben und der Fall ist vorerst abgeschlossen.
Nach Ablauf der vereinbarten Zeit werden Administrator und Projektleiter per Email erinnert, dass die VM demnächst deaktiviert wird. Der Projektleiter überprüft, ob sich alle Daten auf entsprechenden Netzlaufwerken befinden und dadurch alle Daten gesichert sind. Je nach Festlegung in den SLAs wird die VM entweder gesichert oder kann nach einiger Zeit gelöscht werden. Sobald die Maschine deaktiviert wurde, stehen die Ressourcen wieder zur Verfügung.
Bisher konnte dieser Use Case bei Astrium nur teilweise angewendet werden. So gab es bereits eine Serveranfrage, die aber von der IT Abteilung eines anderen Standortes erfolgt ist. Dieser virtuelle Server wird für die bessere Kommunikation beider Standorte benötigt. Da es sich in diesem Fall um eine interne Anfrage handelt, müssen keine bestimmten Leistungsbedingungen oder SLAs ausgehandelt werden. Auch ein Ablauf der VM ist nicht geplant worden, da die Maschine auf unbestimmte Zeit läuft und im Moment ausreichende Ressourcen vorhanden sind. Hier war die Umsetzung nur technisch relevant, da diese auf dem zuvor erstellten Template basiert. Dies war erfolgreich und die VM ist nun produktiv in Betrieb.

Nach den beiden Umsetzungen der Anwendungsfälle, erfolgt im nächsten Schritt die Testphase der Use Cases. Es wurde bereits darauf hingewiesen, dass nach jeder Virtualisierung eines Servers, erst die Testphase durchgeführt wurde, bevor es zu einer weiteren Virtualisierung kommt. Wie die Testphase bei den Anwendungsfällen aussieht, wird im nächsten Abschnitt besprochen.

6.2.3 Testphase anhand der Use Cases

Die Testphase ist in den Ablaufdiagrammen der Use Cases am Ende eingezeichnet. Eine Testphase erfolgt immer am Ende der Umsetzung eines Schrittes und nicht nur am Ende des gesamten Anwendungsfalls. Bei der Virtualisierung der NT4 Domäne wurde als erstes ein BDC virtualisiert. Ist dies erfolgreich geschehen, ist weiterhin der physikalische Server in Betrieb, aber es steht zusätzlich die virtuelle Maschine bereit. Da es sich hier um keine besonders kritische Maschine handelt, wurde keine eigene Testumgebung aufgebaut, sondern über Nacht ist die physikalische Maschine heruntergefahren und die VM hochgefahren worden. Dadurch ist ein Austausch erfolgt und die VM befindet sich im Produktivsystem. Dennoch wird der ursprüngliche Server noch nicht abgebaut, sondern kann im Notfall jederzeit wieder hochgefahren werden. Nach dem Anschalten der VM, wird überprüft, ob der PDC mit der VM kommunizieren kann. Danach wird diese Konstellation für mehrere Tage beobachtet, ob Probleme auftreten. Wenn dies nicht der Fall ist, folgt der zweite Schritt. Hier existieren durch den Ablauf zwei virtuelle Server, wobei der erste Server der Domänencontroller ist. Der zweite Server ist der neu erstellte Druckerserver (siehe Ablaufdiagramm 6.5). War die Erstellung der Server erfolgreich, wird im Anschluss der physikalische Server am Abend abgeschaltet und die neuen VMs hochgefahren. Dieses Vorgehen hat mehrere Gründe: Zum einem handelt es sich auch hier um einen BDC, der nicht primär benötigt wird, sondern als Ausfallsicherheit und Lastverteilung existiert. Beides ist in dieser Umgebung nicht notwendig, da ein anderer BDC zur Verfügung steht und dieser für die kurze Testphase genügt. Des Weiteren ist durch dieses Vorgehen der alte Druckerserver nicht mehr unter dem vorherigen Namen bekannt (da er neu erstellt und konfiguriert wurde). Dies hat den beabsichtigen Effekt, dass der Druckerserver nicht mehr genutzt werden kann. Nur bestimmte Personen sollen den neuen virtuellen Server verwenden dürfen, die über die Umstellung informiert wurden. Bei diesen Personen erfolgt die Anbindung auf den „neuen” Druckerserver. Alle anderen User, die nicht informiert werden, müssen zwangsweise auf einen anderen Druckerserver (weder der alte physikalische, noch der virtuelle) ausweichen, der seit Jahren bereit steht. Dies ist zwar ein radikaler

Schritt, aber notwendig, da die Umstellung auf den neuen Server schon vor Jahren hätte vorgenommen werden müssen. Die User sind darüber mehrfach informiert worden und diejenigen, die dies nicht getan haben, werden nun so gezwungen die Umstellung vorzunehmen.
Durch diese Umstellungen entstehen mehrere kritische Punkte: Sollte der neue virtuelle Druckerserver nicht funktionieren, können die User vorrübergehend auf andere Drucker (die auf einem anderen Server liegen) ausweichen. Kann das Problem innerhalb einer bestimmten Zeit nicht gelöst werden, kann als letzter Schritt die physikalische Maschine wieder aktiviert werden. Dazu müssen aber beide VMs wieder heruntergefahren werden. Der virtuelle BDC kann soweit getestet werden, muss aber erst auf dem PDC eingerichtet werden. Diese Einrichtung erfolgt erst, sobald der PDC virtualisiert worden ist. Wie schon erwähnt, ist der BDC im Moment nicht von großer Bedeutung und muss daher nicht weiter getestet werden.
Bei der Erstellung eines NT4 Server Templates im dritten Schritt, bezieht sich die Testphase auf das erstellte Template. Tests erfolgen hier nur in Bezug auf Netzwerkkommunikation und Installation von einigen wenigen Programmen. Sind diese erfolgreich abgelaufen, kann das Template für den nächsten Schritt verwendet werden. In diesem wird ein zweiter Druckerserver auf Basis von NT4 eingerichtet, der für interne Abläufe notwendig ist. Nach dem Import der Drucker vom virtuellen Druckerserver aus dem zweiten Schritt via *Printer Migrator* muss getestet werden, ob die gewünschten Drucker sich auch ansteuern lassen. Dies war nur eine Nebenaufgabe und hätte bei Nichterfolg keine besonderen Auswirkungen gehabt. Der Import der Drucker war erfolgreich und konnten entsprechend verwendet werden.
Der letzte Schritt war der wichtigste, denn hier musste der PDC virtualisiert werden. Nach der Virtualisierung des Servers, wurde eine Testphase für ein Wochenende ausgerufen, an dem offiziell diese Domäne nicht erreichbar war. Dazu wurde im Vorfeld eine Email per User Help Desk (UHD) versandt, dass in diesem Zeitraum die Domäne nicht verwendet werden kann. Am angegebenen Tag, kam es dann zur Abschaltung der physikalischen Maschine und der virtuelle PDC wurde angeschlossen. Nach dem erfolgreichen Start, wurde der PDC so konfiguriert, dass auch der BDC aus dem zweiten Schritt verwendet werden kann. Daraufhin erfolgt eine Synchronisation aller Maschinen der Domäne und es gibt mehrere Anmeldetests aus unterschiedlichen Netzen, die alle den Domänencontroller erreichen müssen. Auch hier könnte im Fehlerfall die physikalische Maschine wieder angeschaltet werden, wenn es zu unlösbaren Fehlern kommt. Wenn hier alle Tests erfolgreich laufen, können die virtuellen Maschinen verwendet werden.
Für den zweiten Use Case gibt es keine explizite Testphase, da es sich um einen neu erstellten Server handelt, der keine ausführlichen Tests benötigt. Hier muss nach dem erfolgreichen Erstellen nur getestet werden, ob die VM nun auch funktioniert. Daher passt dieser Schritt des Konzepts für den zweiten Anwendungsfall nicht und es muss zu einer geringfügigen Änderung des Ablaufs kommen. Genaueres dazu wird in Abschnitt 6.3.2 behandelt.

Bevor aber die Maschinen in das endgültige Produktivsystem übergehen, muss noch ein Datensicherungskonzept eingeführt werden. Des Weiteren ist die Sicherheit der virtuellen Maschinen in der Umgebung noch nicht überprüft worden. Das Backupsystem wird im nächsten Abschnitt vorgestellt.

6.2.4 Einführung eines Backupsystems

Das eingeführte Backupsystem wird mit zwei Programmen bewerkstelligt. Im ersten Schritt werden die ESX Server einmalig auf eine externe Platte gesichert, um die Konfiguration der Maschinen zu speichern. Die Sicherung erfolgt mit *Norton Ghost* auf eine angeschlossene USB Platte, wenn sich der ESX Server im „Maintenance Modus” befindet. Daraufhin wird per Boot CD das Sicherungsprogramm gestartet, um danach mittels Norton Ghost die Sicherung vorzunehmen. Dieses Backup dauert einige Zeit, da eine Komplettsicherung aller neun Partitionen (siehe Tabelle 6.1) vorgenommen wird. Nach der Sicherung, wird der Host wieder aus dem Wartungsmodus herausgenommen und derselbe Vorgang läuft am anderen ESX Server ab. Diese Sicherung ist für den Notfall gedacht, wenn ein kompletter ESX Server ausfällt und/oder irreparabel beschädigt ist. Um die Sicherung hier zu testen, werden bei einem Server nach der Sicherung die Festplatten gegen fabrikneue Platten ausgetauscht. Danach wird die Rücksicherung gestartet, um alle Partitionen und Einstellungen wieder zu erhalten. Der Test zeigte in der Praxis, dass es nach der Rücksicherung kleine Probleme mit der Swap Partition gab, die nicht richtig erkannt wurde. Dieses Problem ist aber bei VMware bekannt und konnte mit Hilfe des offiziellen Forums gelöst werden. Da es sich nach der Rücksicherung nur um eine kleine Einstellung handelt, wurde diese in der Installations-Dokumentation vermerkt und es fiel die Entscheidung, dass keine andere Soft-

ware verwendet wird. Neben den ESX Servern ist es wichtig, die virtuellen Maschinen zu sichern. Hier gibt es zwei Möglichkeiten der Sicherung von unterschiedlicher Art. Bevor Veränderungen oder Einstellungen an einer VM vorgenommen werden, wird diese mittels eines Snapshots gesichert. Dies erfolgt über das Virtual Center für die gewünschte Maschine und ist je nach Plattengröße in kurzer Zeit abgeschlossen. Das Aufrufen eines Wiederherstellungspunktes wurde mehrfach getestet. Gerade bei den anfälligen NT4 Servern, war die Funktion besonders wichtig. Diese waren schon zuvor sehr fehleranfällig. Aus diesem Grund wurde an diesen auch kaum was geändert. Nach der Migration kamen einige Installationen, wie die *VMware Tools*, hinzu, die nicht immer unbeschadet durchgeführt werden konnten. Mit Hilfe der Snapshots konnte der „stabile" Zustand zuvor gesichert werden, bevor an der Maschine Veränderungen vorgenommen wurde. Diese Technik hat im vorliegenden Fall immer funktioniert.
Die zweite Sicherungsmöglichkeit ist eine komplette Speicherung der virtuellen Maschinen. Wie schon mehrfach angesprochen, gibt es die Möglichkeit eines „Cold Backups" (Sicherung im ausgeschalteten Zustand) oder eines „Hot Backups" (Sicherung im laufenden Betrieb). Idealerweise kann mit dem Backupprogramm die zweite Variante verwendet werden. VMware bietet mit ihrer eigenen Software *Consolidated Backup* eine Erweiterung für die gängigen Backupprogramme an, unter anderem auch das in der Firma eingesetzte *Veritas NetBackup*. Nach einigen Tests und mit Absprache eines externen Dienstleisters hat sich dann herausgestellt, dass die Sicherung mit diesen beiden Programmen funktioniert, aber das Zurücksichern schwer bis unmöglich ist. Die dabei verwendete Version von VMwares Lösung lag dabei noch in der Version 1.0 vor, die auch laut Forum noch einige Probleme hat. Mittlerweile ist Version 1.3 erschienen, die einige Verbesserungen mitliefert. Diese kann aber im Rahmen der Arbeit nicht mehr getestet werden. So ist der momentane Vorgehen, dass die VMs in einem Wartungsfenster ausgeschaltet werden, um dann die Sicherung mittels *NetBackup* vorzunehmen. Dies kann im Moment ohne Probleme durchgeführt werden, da sich keine hochverfügbaren Maschinen am Netz befinden. Die kurze (geplante) Ausfallzeit ist möglich und stellt die momentane Lösung dar. Dazu kann mittels Terminplan die Maschine zu einer bestimmten Zeit herunter- und wieder heraufgefahren werden. Das Backupskript hat dann die Möglichkeit auf die ausgeschaltete VM zuzugreifen und diese auf ein Bandlaufwerk zu sichern.
Die Sicherung der virtuellen Maschinen ist im Moment noch nicht ideal und wird in Zukunft noch verbessert. Ob dabei nochmal *Consolidated Backup* oder eine andere Backuplösung, die VMware unterstützt, eingesetzt wird, muss aber noch geklärt werden.

Neben der Sicherung aller relevanten Daten in der Virtualisierungsumgebung, fehlt in einem letzten Schritt die Überprüfung der Sicherheit. Welche Punkte dabei von Bedeutung sind, werden im nächsten Abschnitt besprochen.

6.2.5 Überprüfung der Sicherheit

Bei der Ermittlung der Sicherheit in einer Virtualisierungsumgebung gibt es eine Vielzahl von Punkten zu beachten. Für den hier vorliegenden Fall, werden die wichtigsten vorgestellt und beschrieben. Zuerst sei gesagt, dass sich alle Server in einem abgeschlossenen Rechenzentrum befinden, in welches nur wenige Personen Zutritt haben. Des Weiteren befinden sich die Maschinen in einem internen Netz, dass durch eine Firewall gegenüber der DMZ (Demilitarized Zone) geschützt ist. Zwischen der Verbindung nach Außen und der DMZ liegt eine weitere Firewall. Zusätzlich gibt es weitere Schutzmechanismen gegen Angreifer von Außen, die aber aus Sicherheitsgründen nicht genannt werden dürfen. Aus diesem Grund handelt es sich bei den folgenden Aspekten um die Überprüfung von internen Punkten, die eine verbesserte Sicherheit gewährleisten sollen. Dabei geht es in erster Linie um die Sicherheit der physikalischen Maschinen. Diese betreiben ein RAID 1+0 (Redundant Array of Independent Disks) System mit insgesamt vier Platten. Bei diesem Verfahren werden zuerst je zwei Festplatten gespiegelt (RAID 1), danach die zwei logischen Laufwerke zu einem sogenannten Stripeset (RAID 0) verbunden. Durch dieses Verfahren stehen die Kapazitäten von zwei Festplatten zur Verfügung. So steht bei einem Festplattenausfall immer noch die gespiegelte Platte zur Verfügung und im Idealfall kann das System ohne Probleme weiterarbeiten. Dies bietet aber nicht hundertprozentigen Schutz: wenn ein Fehler in der Schreiboperation vorkommt, geschieht dies auch auf der gespiegelten Platte. Dennoch bietet das System einen guten Schutz in der Praxis, dass durch die Sicherung im vorherigen Punkt einen guten Ansatz bietet. Neben der RAID Technik, die mittlerweile alle gängigen Server anbieten, befinden sich die zwei ESX Server in einem jeweils anderen abgesperrten Rechenzentrum am Standort. Dadurch ist bei einem

Ausfall eines Raumes (bzgl. Strom, Netzwerk, Klimagerät, etc.) gewährleistet, dass der andere Host weiterarbeiten kann. Auch verbessert sich die Sicherheit, wenn sie die Maschinen in voneinander getrennten Räumen befinden. Dies erschwert das Eindringen auf einen ESX Server vor Ort und falls dies doch gelingt, ist nur ein Server betroffen.
Auch die Virtualisierungsumgebung bietet durch die richtige Konfiguration einen gewissen Ausfallschutz. Wie in Abschnitt 6.2.1 beschrieben, wurden die Netzwerkports so konfiguriert, dass bei Ausfall der internen oder externen Netzwerkanschlüsse das System weiterhin betrieben werden kann. Die Konfiguration muss für alle ESX Server nochmals überprüft werden, ob diese korrekt ist. Als Test wurde über die HP Managementkonsole die externe Karte deaktiviert, um zu überprüfen, ob die Service Konsole und die VMs weiterhin funktionieren. Dazu wurde im Vorfeld einige wenige VMs ausgewählt, die nicht produktiv am Netz sind. Nach der Deaktivierung, ging die Verbindung zur Service Konsole verloren („Connection lost to the host"). Nach kurzer Zeit, konnte die Verbindung wiederhergestellt werden und die Konsole hat den Ausfall sofort angezeigt. Die VMs haben in der Zeit normal weitergearbeitet, soweit sich das überprüfen ließ. Dadurch konnte durch diesen Test die korrekte Konfiguration festgestellt werden.
Ein weiterer wichtiger Sicherheitsaspekt, ist die Pflege durch regelmäßige Updates der ESX Server und virtuellen Maschinen. Wie schon beschrieben, ist das Patchen der ESX Server umständlich gehandhabt (siehe 6.2.1), aber dennoch ein wichtiger Punkt, da hier neben der Stabilität des Systems auch viele sicherheitskritische Punkte verbessert werden. Daher sollte in dem Schritt nochmal überprüft werden, ob auch alle ESX Server auf dem aktuellen Patch-Stand sind. Dies gilt auch für die Gastsysteme der virtuellen Maschinen, die immer auf den neuesten Stand gebracht werden müssen. Bei den NT4 Servern ist das nicht möglich, da der Support seitens Microsoft schon seit Jahren erlöscht ist. Aber für das aktuelle Windows 2003 Server Betriebssystem erscheinen weiterhin neue Updates, die installiert werden müssen. Dazu wird bei Astrium der WSUS (Windows Server Update Services) eingesetzt, der eine zentrale Verteilung der Updates auf alle Windows 2003 Server zulässt. Der WSUS speichert den Versionsstand aller zu überwachenden Server und kann immer überprüfen, wie der Stand der Patches einer Maschine ist. Zentrale Verteilung der Patches ist damit möglich und auch die Installation zu einem bestimmten Zeitpunkt kann damit vorgenommen werden. Dieser Update Service ist bereits für die physikalischen Maschinen vorhanden und wurde für die virtuellen Maschinen erweitert. Dadurch werden diese in den Patchzyklen mitberücksichtigt und befinden sich immer auf dem neuesten Stand.
Neben den Patches befinden sich auf allen VMs auch ein Virenscanner, der auf allen Maschinen (unabhängig ob Server oder Workstation) im Unternehmen installiert ist. Über einen zentralen Server, den auch die VMs erreichen müssen, erhalten alle Maschinen immer die neuesten Virendefinitionen. Auf allen VMs wurde überprüft, ob der Server erreichbar ist und ob die VMs die neueste Version des Virenscanners installiert haben. Dies war bei allen Maschinen der Fall, wodurch auch eine Sicherheit vor Virenfall gegeben ist. Auch für die NT4 Maschinen existiert noch ein Virenscanner, der aber nicht mehr auf den neuesten Stand gebracht werden kann. Die Gefahr eines Angriffs auf einen NT4 Server wird als gering eingestuft, womit dies als Schutz hier ausreicht.
Im letzten Schritt, wurden auf allen VMs die Zugriffsrechte überprüft, ob die Administratoren und Gruppen korrekt eingetragen sind. Dies stellt sicher, dass durch die Migration der Server nicht alte Rechte mitgenommen wurden. Des Weiteren wurden auch in der Virtualisierungsumgebung bestimmte Rechte vergeben, um nur wenigen Leute den Zugriff auf das Virtual Center zu geben. Im VC können auch Rechte für bestimmte VMs zugeteilt werden, was beispielsweise für einen Projektleiter sinnvoll ist, wenn er die VM ausschalten will. Da dieser Use Case bisher noch nicht vorgekommen ist, wurden diese Rechte an einer Testmaschine eingerichtet, um zu sehen, welche Möglichkeiten der Manipulation vorhanden sind. Im Virtual Center können die Rechte sehr spezifisch eingestellt werden, welche in den Tests auch so vorzufinden waren. Es kann hier die Sicherheit so eingestellt werden, wie es für eine einzelne Person gewünscht ist.

Nachdem nun diese Sicherheitsaspekte integriert und überprüft worden sind, kann nun eine Inbetriebnahme in das Produktivsystem erfolgen. Anhand des Konzeptes wurden alle wichtigen Schritte durchgeführt, bevor es zu einer endgültigen Realisierung kommt. Wie diese abgelaufen ist, wird im nächsten Abschnitt vorgestellt.

6.2.6 Überführung in den Produktivbetrieb

Bevor es zu einer endgültigen Überführung in die Praxis kommt, muss nochmal überprüft werden, ob durch die Migration der Server sich Einstellungen, wie Servername, IP Adresse, etc. geändert haben. So ist beispielswei-

se beim ersten Use Case ein neuer Druckerserver entstanden, der den berechtigten Personen mitgeteilt werden muss, wenn das Umschalten erfolgt ist. Auch bei der Umsetzung des zweiten Use Cases muss der Projektleiter über die Zugangsdaten informiert werden, wenn der Server aufgesetzt wurde. Dies sollte kurz nach erfolgreichen Testen und Überprüfen erfolgen, da sich sonst der Server im Leerlauf befindet und nur Ressourcen verbraucht.
Die Überführung des ersten Anwendungsfalls ist an einem Wochenende vorgenommen worden, so dass am folgenden Montag die VMs bereit standen. Dazu wurden die physikalischen Server heruntergefahren, aber noch nicht abgebaut. Dabei muss beachtet werden, dass es bei NT4 Servern kein „Herunterfahren" auf Betriebssystem-Ebene gibt, sondern der Host muss vor Ort ausgeschaltet werden. Die Maschinen befinden sich auch in dieser Phase noch als Backup im Rechenzentrum und können im äußersten Notfall erneut aktiviert werden. Erst wenn der Produktiveinsatz erfolgreich läuft, werden die Maschinen nach und nach abgebaut. In der ersten Phase nach dem Wochenende wurden die virtuellen Maschinen von mehreren Administratoren genau beobachtet, ob sich Abweichungen oder ein Fehlverhalten zeigt. Dies ist deshalb notwendig, weil die Verwendung einer Domäne in der Praxis eine andere Nutzung aufweist, als in der vorherigen Testumgebung. Daher kam es in der ersten Zeit immer wieder zur Durchführung von Anmeldeversuchen und Tests. Nebenbei wurden mittels Virtual Center die virtuellen Server beobachtet, ob ein anderes Leistungsverhalten zu sehen ist. Dies war bei allen VMs nicht der Fall und es gab dabei keine Komplikationen. Dennoch sind die ursprünglichen Hosts noch im Rechenzentrum und werden erst zum Ende des Jahres zur Entsorgung abgebaut.
Neben dem Beobachten der Maschinen, gab es für einige andere Administratoren eine Einführung in die virtuelle Umgebung, am Beispiel des ersten Use Cases. So wurde die virtuelle Infrastruktur, das Virtual Center und die Möglichkeiten, die sich dadurch ergeben, genauer vorgestellt. Das war notwendig, um das Wissen über diese neue Technik mit mehreren Personen zu teilen, so dass im Fehlerfall mehrere Personen entsprechend reagieren können. Zusätzlich ist eine Dokumentation über die Einrichtung der Infrastruktur und das Umsetzen der Virtualisierung aufgesetzt worden, um einen Leitfaden zu stellen, an dem alle Einstellungen nachvollzogen werden können. Anhand der Beschreibung können alle Administratoren neue ESX Server erstellen, virtuelle Maschinen anlegen oder neue Anwendungsfälle umsetzen, wenn dies benötigt wird.
Es sei an dieser Stelle erneut erwähnt, dass die Realisierung des zweiten Use Cases bisher noch nicht durchgeführt werden konnte, da es noch keine Anfrage eines Projektleiters gegeben hat. Bisher wurden nur zwei interne Anfragen umgesetzt, die ohne Probleme durchgeführt werden konnten. In diesem Fall gibt es auch keine Umsetzungs- und Realisierungsphase, da diese beiden Schritte zu einem zusammengefasst werden.

Damit ist die Realisierung der Virtualisierungsumgebung und der Use Cases abgeschlossen. Diese hat sich am Konzept orientiert und konnte in den meisten Fällen auch so umgesetzt werden, wie es in Kapitel 5 vorgestellt wurde. Dennoch sind kleine Probleme und Schwierigkeiten aufgetaucht, die bereits Erwähnung fanden, aber noch nicht detailliert besprochen wurden. Im nächsten Abschnitt werden diese noch einmal zusammenfassend genannt und bewertet. Dabei wird auch auf Abweichungen vom ursprünglichen Konzept eingegangen.

6.3 Probleme bei der Realisierung

Bei den aufgetretenen Problemen, müssen zwei Arten unterschieden werden: Probleme, die durch eigene Fehler entstanden sind und diese, die aufgrund der Programme zu Schwierigkeiten geführt haben. Die selbstverursachten Probleme waren dabei von geringer Zahl, sind aber auf Grund von Nachlässigkeit aufgetreten. So ist zuvor erwähnt worden, dass ein NT4 Server über das Betriebssystem nicht heruntergefahren werden kann. Es gibt zwar die Möglichkeit, aber er steht dann in einem „Wartezustand", in dem die Maschine physikalisch ausgeschaltet werden muss. Ansonsten befindet sich das Gerät noch am Netz, ist aber nicht einsatzbereit. Wenn jetzt die migrierte VM hochgefahren wird, gibt es zwei identische Maschinen mit denselben IP Adressen im Netz, das zu einem Netzwerkproblem führt. Des Weiteren sind kleinere Einstellungsprobleme zu Beginn der Virtualisierungsumgebung eingetreten, die auf Grund des Lernprozesses mit der neuen Technik gemacht wurden. Ansonsten haben sich Probleme aufgrund der eingesetzten Programme vorgetan. Um welche es sich dabei handelt, wird im nächsten Abschnitt beschrieben. Als Abschluss dieses Kapitels erfolgt im darauffolgenden Punkt, eine Anpassung des Konzeptes für den hier vorliegenden Fall.

6.3.1 Technische Probleme bei der Umsetzung

Die Virtualisierungsumgebung lief in der gesamten Zeit dieser Arbeit sehr stabil und es gab so gut wie keine Probleme. Bei Fragen oder Schwierigkeiten, hat das offizielle Forum praktikable Anleitungen und Hilfen angeboten. Dennoch gab es gerade zu Beginn ein Problem mit der Hochverfügbarkeitlösung HA. Es sei nochmal kurz erklärt, dass mittels HA auf einen ausgefallenen Server rechtzeitig reagiert werden kann, indem über den zentralen Datenspeicher bekannt ist, welche VMs auf welchem Host laufen. Fällt ein Host aus, können nach kurzem Timeout die VMs auf einem anderen ESX Server neu gestartet werden. Das Problem ist aber, dass HA teilweise labil läuft und auf den DNS Server nicht immer reagiert. Im hier vorliegenden Fall, waren die Server im DNS korrekt angelegt, in den HA Konfigurationsdateien waren beide Server vollständig angeben. Dennoch konnte kein HA System zwischen den beiden Servern aufgebaut werden. Auch das Forum half hier nicht weiter und es musste gleich zu Beginn des Aufbaus ein Problemticket bei VMware direkt aufgegeben werden. Diese haben aufgrund zuvor hochgeladener Loginformationen eine Datei gefunden, die nicht direkt mit HA zu tun hat, aber in der sich noch falsch eingetragene Server befanden. Laut Helpdesk von VMware, sollte dies aber keinen Einfluss haben. Nach Änderung dieser Datei, konnte auf HA aktiviert werden. Ein späterer Test hat gezeigt, dass bei erneuter Veränderung dieser Datei HA nicht mehr davon beeinflusst war. Damit ist der Fehler nicht vollständig nachvollziehbar, ist aber seitdem nicht mehr aufgetreten.
Ein weiteres Problem, dass bereits Erwähnung fand, ist der Einsatz von *VMwares Consolidated Backup*. Dieses Backupsystem, in Kombination mit *Veritas NetBackup*, konnte zwar aufgebaut und eingerichtet werden, aber der Restore hat keinen Erfolg gebracht. Die Sicherung läuft über das Snapshotsystem und diese konnten zwar zurückgesichert werden, haben aber meistens zu Fehlern geführt. Teilweise konnte die VM nicht mehr gestartet werden oder es traten Fehler beim Startvorgang auf, die zuvor nicht vorhanden waren. Eine kurze Fehlersuche hat keinen Erfolg gebracht und da dieses Programm nicht überzeugt hat, wurde in Absprache mit den Administratoren darauf verzichtet. Daraufhin wurden die VMs im ausgeschalteten Zustand gesichert und es wird seitdem nach einer geeigneteren Lösung gesucht. Ein Einsatz einer neuen lizenzpflichtigen Software, wird aber erst im nächsten Jahr vorgenommen.
Neben dem Backupprogramm bietet VMware für die Gastbetriebssysteme die *VMware Tools* an, die für eine bessere Leistung sorgen. Des Weiteren werden Netzwerkkarten- und Grafikkartentreiber installiert, um korrekt arbeiten zu können. Dies hat bei einer VM besonders zu Schwierigkeiten geführt. Diese Maschine auf Basis von NT4 Server hatte diverse Probleme bei der Installation von den *VMware Tools*. Dies hat sogar soweit geführt, dass bei einer Installation der Grafiktreiber, die Maschine nach dem Neustart einen Bootfehler hervorgerufen hat und daraufhin neu migriert werden musste. Zusätzlich hat diese Maschine eine Vollauslastung der CPU angezeigt, solange die VMware Netzwerkkartentreiber nicht installiert waren. Erst danach ging die Auslastung herunter und es konnte mit der Maschine gearbeitet werden. Neben dem Problem der neu installierten Treiber, sorgte auf der bereits installierte Array-Controller von Compaq für einige Probleme. Dieser ließ sich nicht entfernen und da diese physikalische Komponente nicht mehr vorlag, kam es immer wieder zu Fehlermeldungen. Die Deinstallation konnte erst durch das Bereinigung der Registry behoben werden. Dies hat aber auch mehrere Tests benötigt, denn wenn zu viel gelöscht wurde, kam es auch wieder zu Bootfehlern. Hier war die mehrfstufige Snapshotfunktion von großer Hilfe, mit der jedes erfolgreiche Vorgehen gesichert werden konnte. Im Fehlerfall ist der zuvor gespeicherte Wiederherstellungspunkt aufgerufen worden. Dadurch konnten die Compaqtreiber und -programme soweit entfernt werden.
Als letztes ist der bereits zuvor genannte Fehler bei der Sicherung der ESX Server mittels *Norton Ghost* genannt. So enthielt die neue Swap Partition eine neue UUID, aber beim Booten der Partitionen ist noch die alte eingetragen. Dadurch kann diese Partition nicht erkannt werden und VMware gibt in der Konsole Warnmeldungen bezüglich eines Einsatzes dieses Hosts aus. Hier konnte aber wieder das Forum helfen, wie die neue UUID herausgefunden und eingetragen werden kann. Mittels einiger Linuxbefehle konnte das in kurzer Zeit erledigt werden und nach einem Neustart ist der Fehler nicht mehr aufgetreten. Das System lief dann auch einige Zeit mit den zurückgesicherten Platten, um zu überprüfen, ob noch andere Fehler auftreten. Dies war aber nicht der Fall und so wurde diese Schwierigkeit erfolgreich abgehandelt.

Dies zeigt, dass immer wieder kleinere Probleme aufgetreten sind, die aber im Großen und Ganzen gelöst werden konnten. Ansonsten kann es über den Einsatz von VMware und dessen Produkte keine Beschwerden geben, vor allem die Livemigration via *VMotion* funktioniert einwandfrei und ist für die Administration ein kaum wegzudenkendes Werkzeug. Dennoch gab es bei der Umsetzung einige kleinere Abweichungen vom vorgestellten Konzept, die im letzten Punkt berücksichtigt werden.

6.3.2 Abweichung vom ursprünglichen Konzept

Bei der Realisierung gab es zwei größere Abweichungen vom eigentlichen Konzept. Die erste betrifft die Vorbedingungen, die zu einer optimalen Auswahl an Servern mit der dafür am besten geeigneten Virtualisierungsumgebung. Dabei sollte, wie in Abschnitt 5.1 beschrieben, zuerst eine Bestandsaufnahme durchgeführt werden. Im nächsten Schritt erfolgt eine Auswahl der Server, die sich für eine Virtualisierung eignen. Im letzten Schritt ergibt sich aus dieser Liste und einigen zusätzlichen Bedingungen, beispielsweise die Wahl der Virtualisierungsumgebung. All diese Punkte sind vor der Arbeit geklärt worden, wodurch keine Auswirkung auf die Wahl der Server oder der Umgebung erfolgen konnte. Die Server wurden auf Grund der Erfahrung und dem Wissen der Administratoren für eine Virtualisierung ausgewählt, doch kamen keine genauen Analysen aller möglichen Rechner zum Einsatz, die vielleicht eine wesentlich höhere Serveranzahl ergeben hätte. Auch eine kurze Bestands- und Testphase unterschiedlicher Virtualisierungsumgebungen hätte zuvor durchgeführt werden können. Alle größeren Produkte hätten für eine Testphase kostenlos bezogen werden können, um die Wahl an den Eigenschaften der Umgebungen treffen zu können. Dies war aber nicht der Fall, sondern auf Grund erster Erfahrungen an einem anderen Standort mit VMware, fiel die Wahl auch hier auf dieses Produkt. Es sei gesagt, dass die Wahl für diesen Anwendungsfall keinesfalls schlecht war, doch wäre zu überlegen gewesen, ob auch ein günstigeres Produkt in Frage gekommen wäre. VMware ist mit der Lizenzierung der meisten Eigenschaften, wie VMotion, DRS oder HA, die teuerste Alternative, bietet aber auch schon seit längerem diese umfangreichen Möglichkeiten. Der Vergleich mit einem ähnlichen Produkt, wie die kostengünstigere *XenEnterprise* Lösung von XenSource hätte zu interessanten Ergebnissen führen können.
Neben der nicht vorhandenen Analyse bei den Voraussetzungen, die beide Use Cases betrifft, bezieht sich die zweite größere Abweichung, auf die Bereitstellung von Servern auf Basis von Templates. Bei diesem Anwendungsfall ist das genaue Einhalten des Konzeptes nicht ideal. Dies liegt daran, dass eine Implementierungs- und Testphase hier nicht getrennt, sondern zu einem Schritt zusammengefasst werden. Der neue Server basiert nicht auf eine bereits existierende Maschine und muss daher keinem umfangreichen Funktionstest unterzogen werden. Nach der erfolgreichen Erstellung, genügt eine Überprüfungsphase, ob die Maschine am Netz ist (falls das gewünscht ist) und ob die Installation erfolgreich verlaufen ist. Dies genügt, um dem Projektleiter die Zugangsdaten zu übergeben, damit dieser die gewünschten Programme installieren kann. Nach dieser Ersteinrichtung von dem Projektleiter, macht es Sinn, die Maschine zu sichern. Des Weiteren kann an dieser Stelle eine erneute Sicherheitsüberprüfung erfolgen, ob für das installierte Programm auch die neuesten Updates und Patches installiert sind. Sind beide Schritte (Sicherung und Sicherheitsüberprüfung) abgeschlossen, wird die VM endgültig in die Verantwortung des Projektleiters übergeben. Der Administrator hat weiterhin die VM in der Virtualisierungsumgebung unter Beobachtung und kann bei einem Sicherheitsrisiko eingreifen. So erfolgen auch hier Sicherheitsupdates über den WSUS, wenn es sich um einen Windows Server (NT4, 2000/2003 Server) handelt.

Mit diesem Punkt, ist das Kapitel der Realisierung abgeschlossen. Es wurde die Umsetzung des Konzeptes ausführlich beschrieben, welche Produkte Verwendung fanden und wie die Use Cases realisiert wurden. Des Weiteren wurde auf die Probleme bei der Umsetzung eingegangen, die aber keine größeren Änderungen oder Umstellungen verursacht haben. Die bisherige Beschreibung hat aber noch keinen Wert auf die Qualität der Realisierung gelegt, allen voran, ob die Anforderungen in Abschnitt 4.2 auch erfüllt worden sind. Zusätzlich ist bisher noch nichts zu der Performanz des Systems und der virtuellen Maschinen gesagt worden, ob diese ein ähnliches Verhalten wie die physikalischen Maschinen aufweisen. All diese Punkte werden im nächsten Kapitel genau besprochen, wodurch eine Bewertung der Realisierung erfolgen kann.

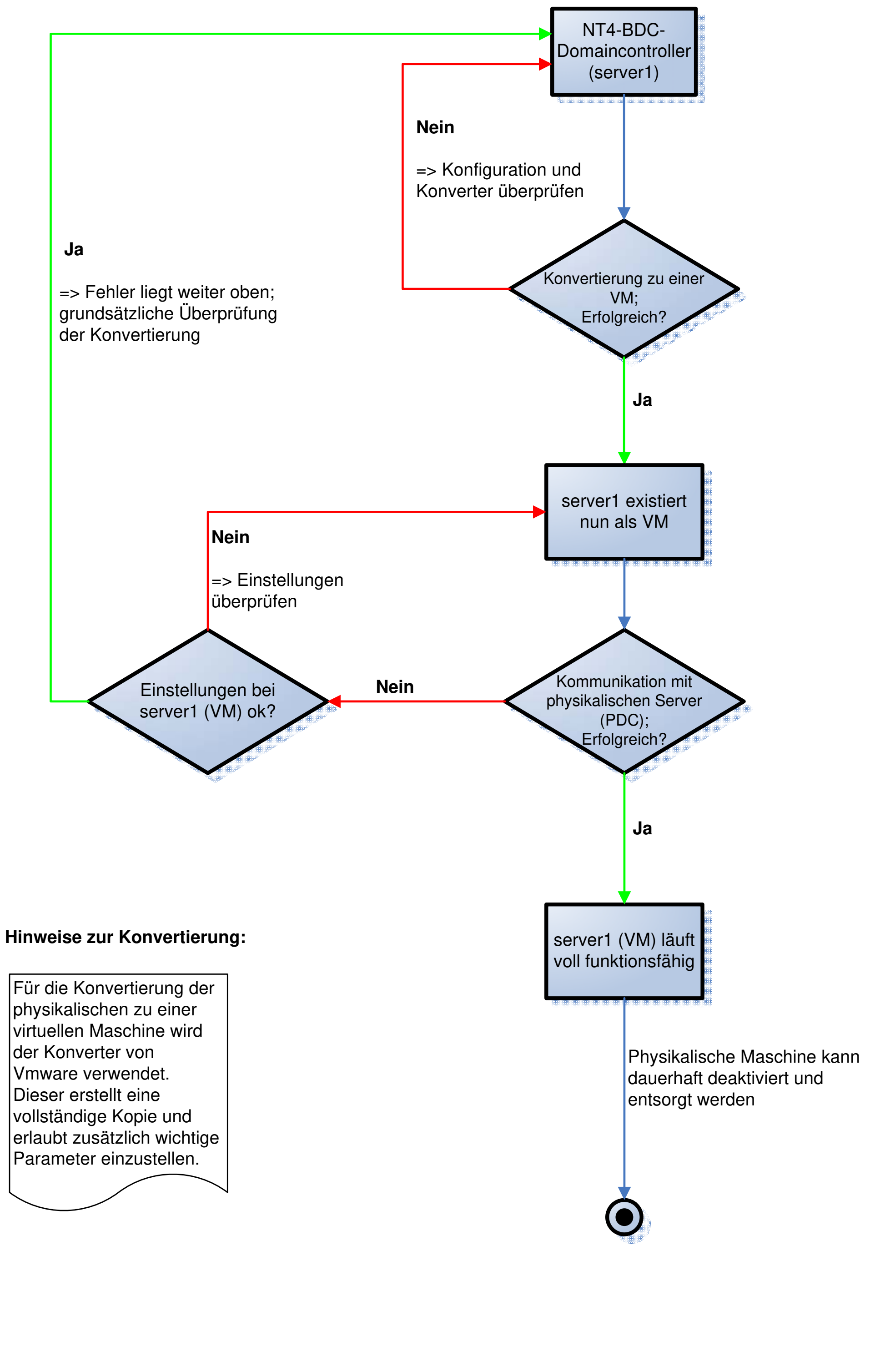

Abbildung 6.4: Ablaufdiagramm des ersten Use Cases: Schritt 1

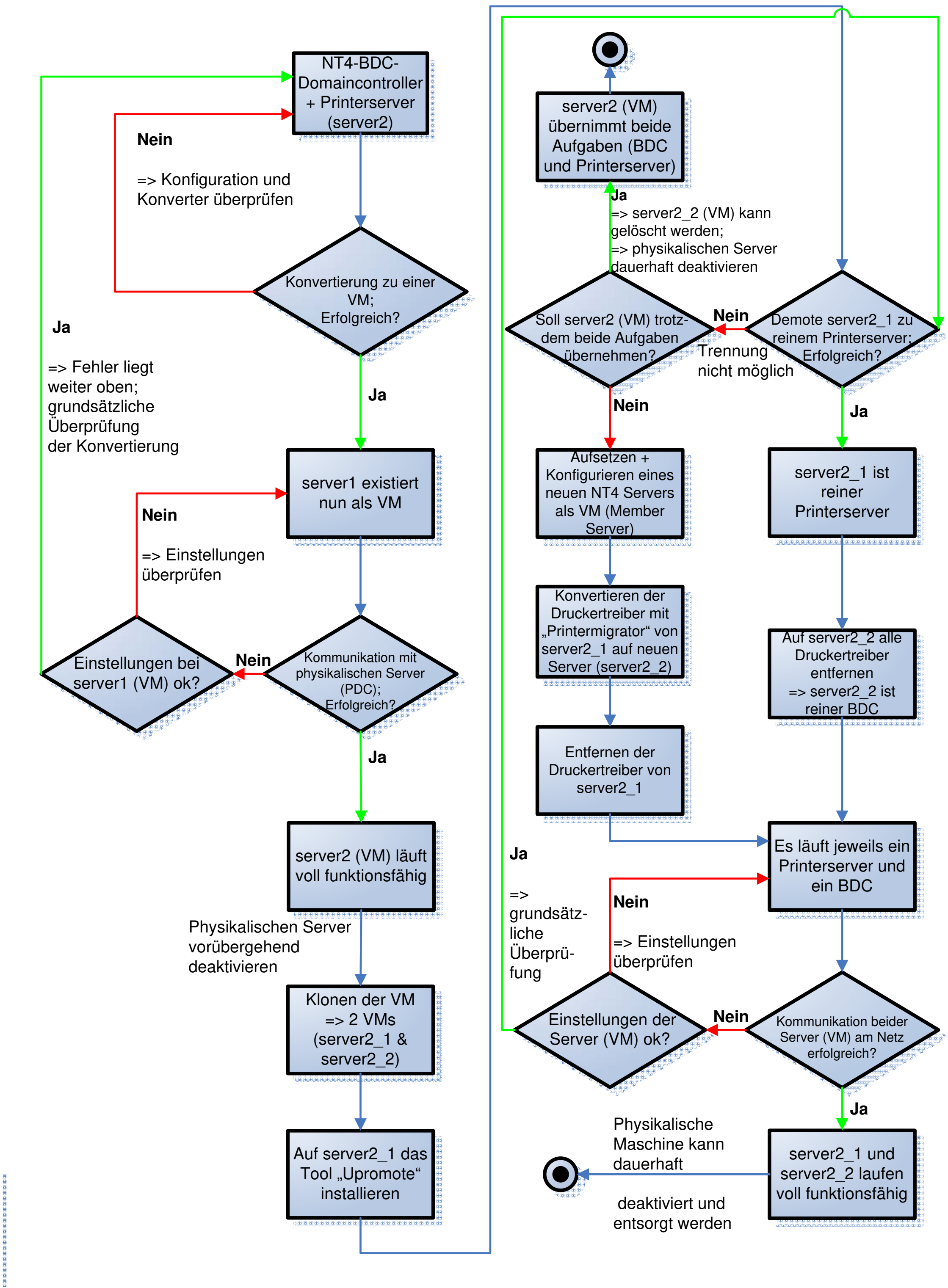

Abbildung 6.5: Ablaufdiagramm des ersten Use Cases: Schritt 2

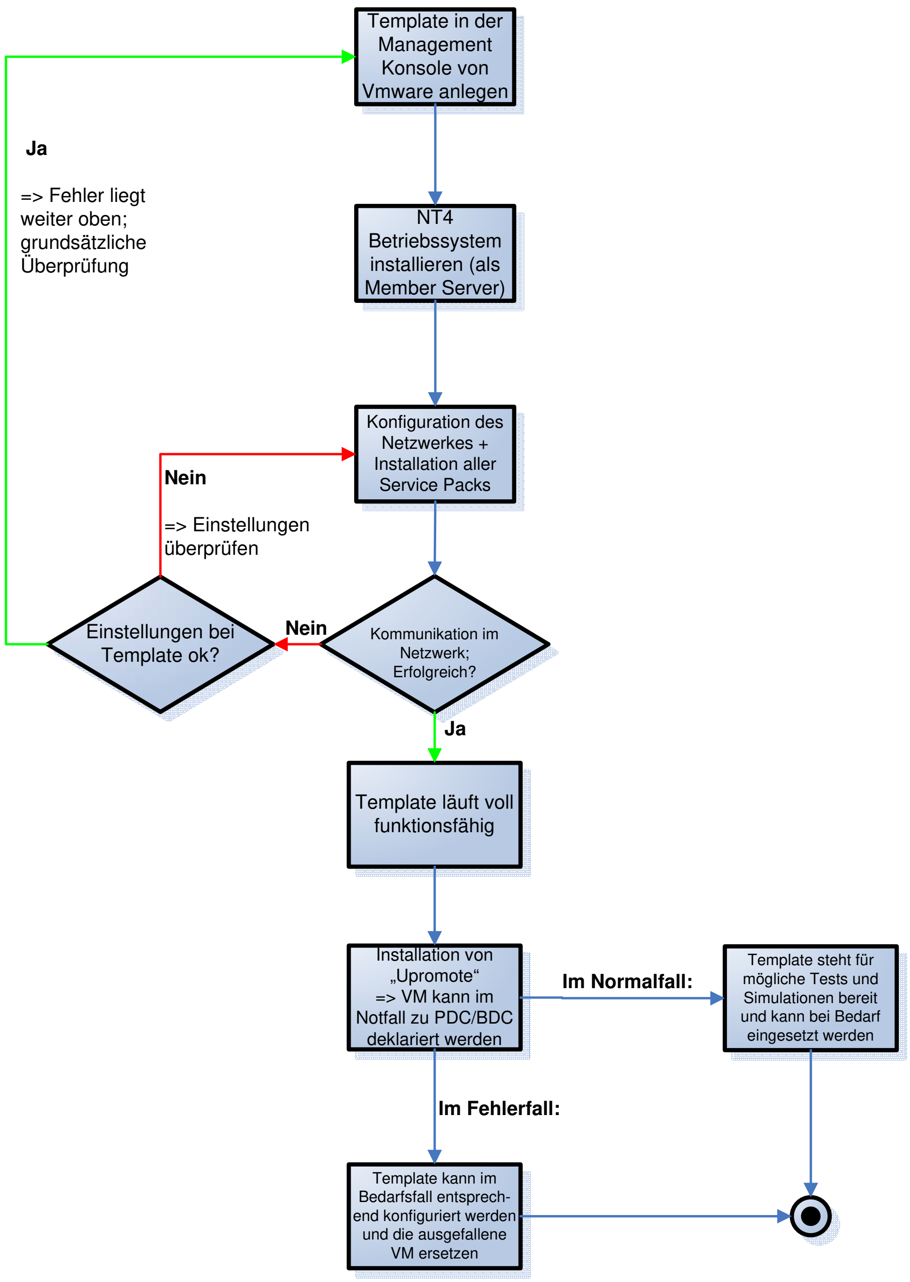

Abbildung 6.6: Ablaufdiagramm des ersten Use Cases: Schritt 3

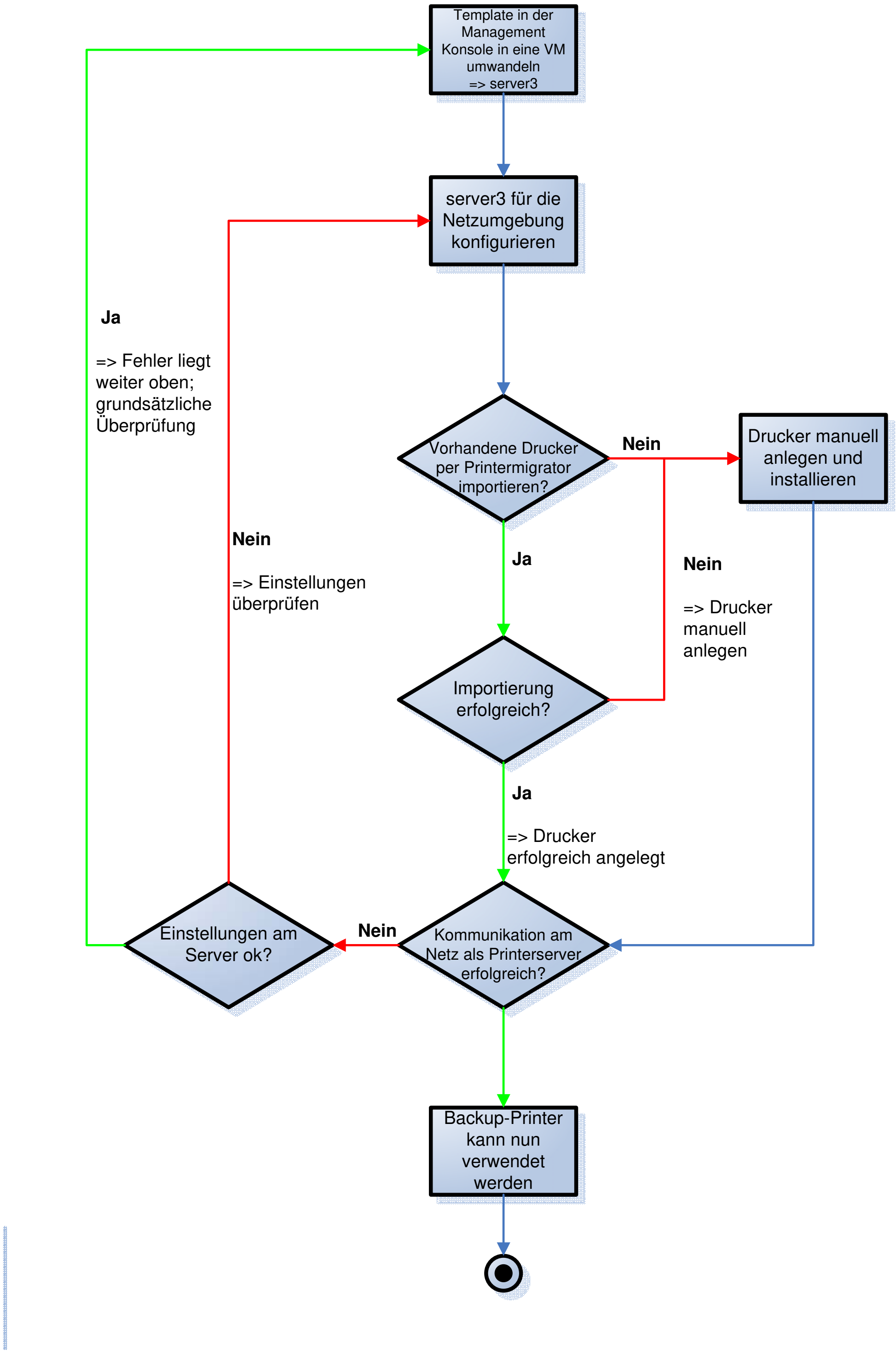

Abbildung 6.7: Ablaufdiagramm des ersten Use Cases: Schritt 4

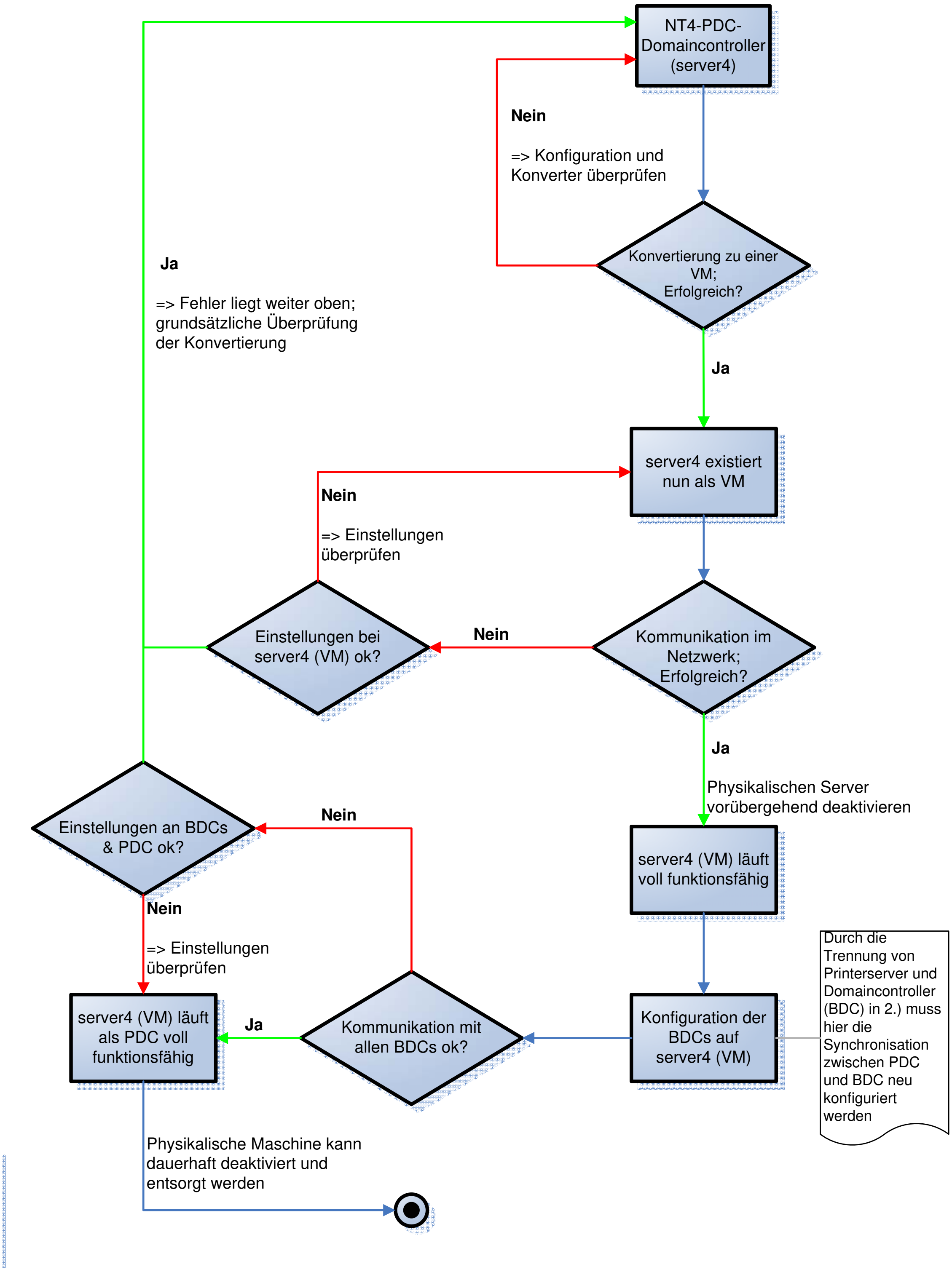

Abbildung 6.8: Ablaufdiagramm des ersten Use Cases: Schritt 5

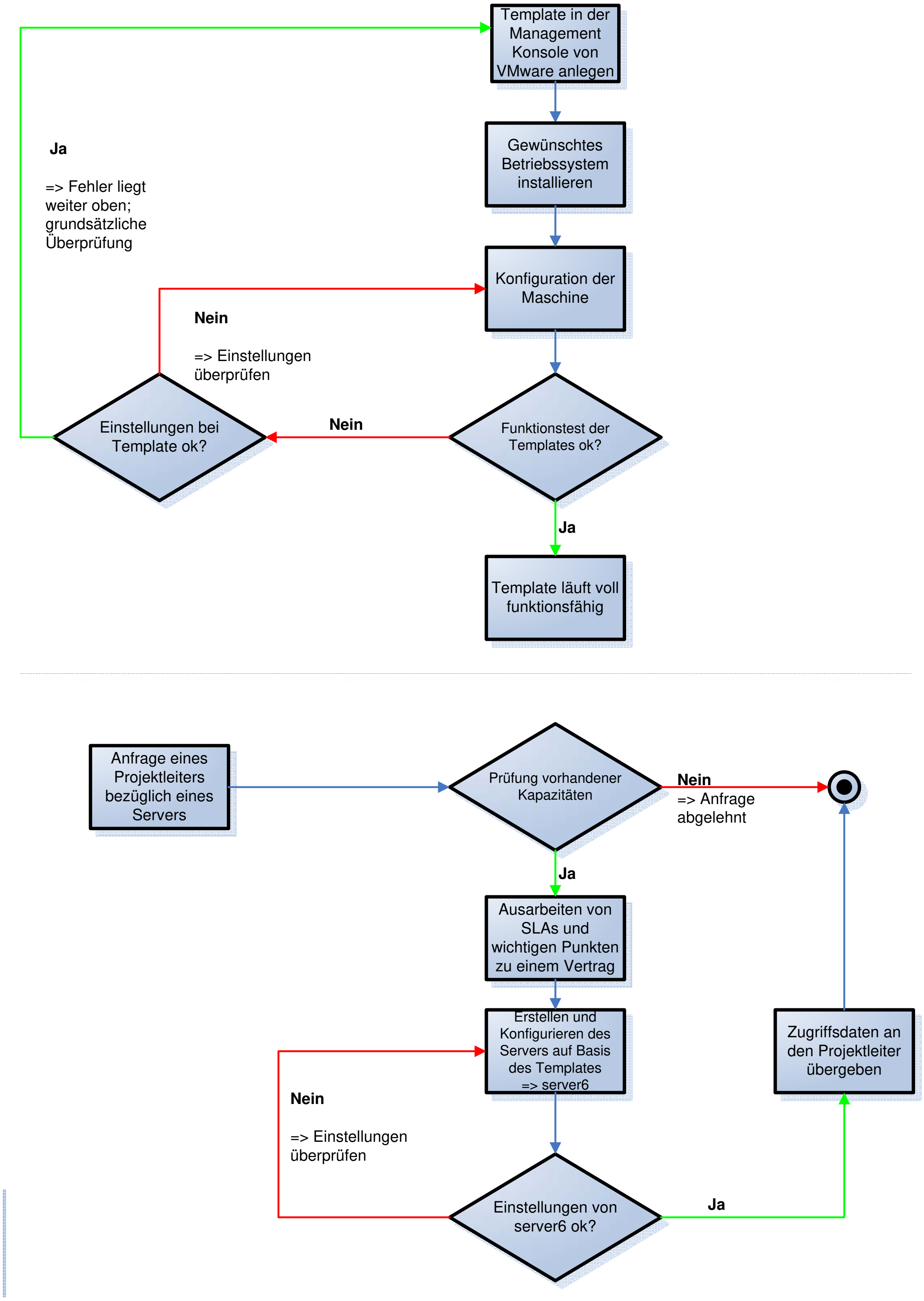

Abbildung 6.9: Ablaufdiagramm für den zweiten Use Case

7 Bewertung

In diesem Kapitel muss sich die Realisierung einer Analyse unterziehen, um festzustellen, wie effizient und qualitativ die Umsetzung war. So spielt vor allem der erarbeitete Anforderungskatalog eine große Rolle, der durch seine Katalogisierung und Gruppierung gewichtete Anforderungen aufgestellt hat. Dabei müssen alle Punkte der ersten Gruppe erfüllt sein, ansonsten gilt die Realisierung als gescheitert. Aber auch die anderen Punkte spielen für den realistischen Einsatz eine wichtige Rolle. Ob alle Anforderungen erfüllt sind und welche Punkte nur teilweise oder gar nicht beachtet wurden, wird im Abschnitt 7.1 beschrieben. Ein besonderes Augenmerk wird auf die Performanz gelegt, die mit einigen Benchmarktests belegt wird. Dabei kommen Vergleiche zwischen einer physikalischen und einer virtuellen Maschine mit gleichen Grundvoraussetzungen (CPU, Speicher, etc.) zum Vergleich. Aus diesen Informationen erfolgt dann im zweiten Abschnitt (siehe 7.2) die Bewertung aus dem zuvor getesteten Verhalten. So kann überlegt werden, wenn größere Anforderungen nicht erfüllt worden sind, ob bei der Realisierung oder am Konzept etwas geändert werden muss. Auch gibt es noch einmal eine finales Resümee, wie die komplette Realisierung zu bewerten ist.

7.1 Erfüllung der Anforderungen

Die Anforderungen in der Tabelle 4.1 auf Seite 50 müssen nun Schritt für Schritt überprüft und bewertet werden. Dazu wird jede Kategorie im Detail betrachtet, ob die Punkte in der Praxis erfüllt worden sind oder ob Abstriche gemacht werden müssen. Wie schon zuvor erwähnt, erhält das Leistungsverhalten eine besondere Stellung, da mit der Performanz der VMs ein sinnvoller Einsatz steht oder fällt. Bei zu starken Einbrüchen gegenüber einer vergleichbaren physikalischen Maschine, wird die verwendete Virtualisierungsumgebung als eingeschränkt tauglich eingestuft. Doch zuerst werden im nächsten Abschnitt die restlichen Anforderungen betrachtet.

7.1.1 Bewertung aller Anforderungen im Überblick

Kosteneinsparung: In der ersten Anforderung in dieser Kategorie handelt es sich um die Verwendung von mehreren Betriebssystemen und VMs auf einem physikalischem Host. Diese Anforderung ist erfüllt, denn neben *Windows NT4 Server* und *Windows 2003 Server*, laufen einige Testumgebungen mit dem Betriebssystem *Gentoo Linux* auf einem ESX Server. Auch arbeiten mehrere virtuelle Maschinen mit den zuvor genannten Betriebssystemen auf demselben Host und während dieser Arbeit sind keine Probleme im Betrieb vorgekommen. Daher wird dieser Punkt der ersten Gruppe als erfüllt betrachtet. Die zweite Anforderung dieser Kategorie ist der Abbau von Servern und Hardwarekomponenten. Dies konnte auch erreicht werden, da die zwei Server der NT4 Domäne mittlerweile abgeschaltet und entfernt worden sind. Zusätzlich konnte durch diesen Schritt Verkabelung und ein Switch eingespart werden, wodurch die Komplexität verringert werden konnte. Weitere Server stehen zum Abbau bereit, die zwar schon abgeschaltet, aber noch nicht entsorgt wurden. Dadurch sind alle Anforderungen dieser Kategorie vollständig erfüllt worden.

Einfacheres Management: In dieser Kategorie sind sechs Anforderungen enthalten, wobei die Zeiteinsparung durch einfachere Handhabung der VMs zu den Wichtigsten zählt. Hierbei geht es um bessere Übersicht mit einer zentralen Komponente, dem Virtual Center Server. Dieses Ziel wird mit dem VC Server auch erreicht, da nun alle virtualisierten Maschinen über eine zentrale Stelle überwacht und verwaltet werden können. Über die Managementkonsole konnten auch die weiteren Anforderungen wie das Klonen, die Erstellung von Snapshots und die Livemigration vorgenommen werden. Beide Funktionen konnten ohne Probleme durchgeführt werden, wobei vor allem das Verschieben im laufenden Betrieb stets einwandfrei durchgeführt werden konnte. Die Migration von physikalischen zu virtuellen Maschinen wurde mit dem *VMware Converter* durchgeführt, der im Anwendungsfall einwandfrei funktionierte. Auch der Import von VMs die mit *VMware Workstation* erstellt worden sind, konnten erfolgreich durchgeführt worden. Dies war für die Use Cases nicht direkt von Bedeutung, aber diente zur Konsolidierung verstreuter Maschinen. Als letzten Punkt dieser Kategorie gilt es noch die individuelle Vergabe von Benutzerrechten zu prüfen. Hier bietet VMware eine Vielzahl an Einstellungen an, um die Rechte für den einzelnen User genau anzupassen. So kann sogar festgelegt werden, welche Konfiguration z.B. ein Projektleiter an einer VM vornehmen kann. Es können aber auch komplette Gruppen, die über das Active Directory verwaltet werden, eingetragen und bearbeitet werden. Mit diesem letzten Punkt, sind auch in dieser Kategorie in diesem Anwendungsfall alle Anforderungen erfüllt.

Flexiblere Reaktion: Die hier wichtige Anforderung ist die schnelle Bereitstellung von Servern bei Anfragen oder in Stoßzeiten. Diese Anforderung kann nicht vollkommen bewertet werden, da es bisher noch keine externe Anfrage auf Serverkapazitäten gegeben hat. An sich ist von der technischen Seite alles Notwendige für diesen Prozess vorbereitet, aber noch nicht in der Praxis getestet worden. Auch die Bereitstellung, wenn es zu Engpässen kommt, konnte nicht getestet werden und erhält daher keine Bewertung. Templates mit den eingesetzten Servern sind vorhanden, aber ob diese zum Zug kommen, falls es zu Engpässen kommt, ist nicht geklärt. Daher kann zu dieser Anforderung keine genaue Aussage geliefert werden. Die Verwendung von Templates wurde dagegen eingesetzt und kam auch bei den Anwendungsfällen zum Einsatz. Auch die Erstellung brachte keine Probleme und daher gilt diese Anforderung als erfolgreich erfüllt. Eine weitere Anforderung, die der individuellen Konfiguration einer VM, ist vollkommen erfüllt. So ist es im Nachhinein möglich, den Hauptspeicher, die durchgereichten CPU-Kerne, die zur Verfügung stehenden Netzwerkports oder neue virtuelle Platten entsprechend der Anforderung zu ändern, auch wenn die Maschine schon angelegt ist. So können Maschinen nachträglich optimiert werden, falls ihnen beispielsweise zu viel Hauptspeicher zugeteilt wurde. Auch bei steigender Auslastung kann eine Anpassung erfolgen, die in der Praxis einwandfrei funktioniert hat. So muss zwar die VM heruntergefahren werden, bevor die Einstellungen vorgenommen werden können, aber danach stehen, je nach Auswahl, die gewünschten Ressourcen bereit. Aus diesen Gründen kann für diese Kategorie gesagt werden, dass alle Punkte, soweit sie überprüfbar waren, erfüllt worden sind. Ob die Bereitstellung der Server auch korrekt abläuft, kann hier nicht gesagt werden und ist daher nicht uneingeschränkt erfüllt. Dies kann erst die Praxis zeigen, ob die vorgestellte Ablauf korrekt implementiert werden kann.

Service Qualität: In der letzten Kategorie, sind die meisten Anforderungen der Gruppe I aufgeführt. Daher müssen diese alle genau überprüft werden.Wie schon zuvor beschrieben, wird das Leistungsverhalten in nächsten Abschnitt gesondert behandelt. Die Anforderungen in Bezug auf „Funktionalität", „Sicherung" und „Sicherheit" der VMs sind eigene Punkte des Konzeptes und wurden ausreichend behandelt. Die Umsetzung zeigt, dass diese auch erfolgreich beachtet wurden. Eine Einschränkung entsteht bei der Sicherung von VMs, da dies nicht im laufenden Betrieb funktioniert. Da im Anwendungsfall momentan keine hochverfügbaren Maschinen arbeiten, ist daher eine kurze Ausfallzeit möglich. Des Weiteren wird in naher Zukunft ein entsprechendes Programm, mit dem auch „Hot Backups" möglich sind, eingesetzt. Die Gefahr, dass die wenigen Netzwerkschnittstellen auf einem Host einen „Flaschenhals" darstellen, hat sich in der Praxis nicht bewahrheitet. Bei der Auswahl der zu virtualisierenden Server, wurden gerade Maschinen genommen, die wenig Auslastung, auch in Bezug auf das Netzwerk, haben. So sorgte der Netzverkehr an den beiden Ports für keine Überbelastung, auch als alle virtuellen Maschinen kurzzeitig auf einem Host liefen (dies ist hier im Wartungsfall eines ESX Servers der Fall). Wenn es um die Gewährleistung von Hochverfügbarkeit von Hosts und VMs geht, muss dies getrennt betrachtet werden. So gibt es mittels *VMwares HA* eine Möglichkeit, die den Ausfall von Hosts überwacht und darauf reagiert. Dies wurde in einem Test durchgeführt, in dem einem ESX Server mit einigen Testmaschinen die Stromversorgung gekappt wurde. Daraufhin waren die darauf laufenden VMs nicht mehr zu Verfügung gestanden. Nach kurzer Zeit registrierte über HA der andere ESX Server den Ausfall und startete, entsprechend der Einstellung, die VMs bei sich neu. Nach ca. 3 Minuten waren die Maschinen wieder vorhanden und konnten eingesetzt werden. Einen entsprechenden Ausfallschutz, gibt es für eine einzelne virtuelle Maschine nicht. Hier erfolgt die Überwachung nur über den VC Server, bei dem von Zeit zu Zeit der Status der VMs überprüft wird. Spezielle Clusterlösungen werden nicht eingesetzt und sind hier auch nicht nötig. Dennoch ist die formale Anforderung nicht komplett erfüllt, auch wenn sie für den vorliegenden Anwendungsfall nicht so sehr von Bedeutung ist. Die Livemigration mittels

VMotion dient als Basis von VMwares Lastverteilungsfunktion *DRS*. Dies gewährleistet eine bessere Lastverteilung der VMs, ohne dass der Administrator eingreifen muss. Je nach Einstellungen, kann eine Lastverteilung stark oder schwach forciert werden. In der Praxis hat sich diese Funktion unbemerkt in den Virtualisierungsumgebung integriert. So wurden neu erstellte VMs immer auf dem Host gestartet, der eine geringere Ressourcenauslastung besaß. Auch im laufenden Betrieb, kam es zu Verschiebungen, die bei einer moderaten Konfiguration, immer sinnvoll erschienen. Bei der Installation von Updates der ESX Server, rät VMware in den „Maintenance Modus" zu wechseln, bevor die Patches ausgeführt werden. Dies gewährleistet keine Beeinflussung der VMs, da diese zuvor auf den anderen Host verschoben werden. Deshalb kann es zu keiner Beeinträchtigung der virtuellen Maschinen kommen und auch diese Anforderung ist daher erfüllt. Die vorletzte Punkt behandelt die Orientierung an ITIL, bei der Erstellung von virtuellen Maschinen. Die Use Cases bei Astrium wurden bereits anhand der ITIL Prozesse beschrieben (siehe Abschnitt 4.3.3), sind aber nicht so detailiert umgesetzt worden. Bisher sind allgemeine ITIL Prozesse bei Astrium nicht implementiert, wodurch weder eine CMDB (Configuration Management Database) noch die Rollen (Change, Release, etc.) vorhanden sind. Dadurch ist der Change Prozess von einem Administrator durchgeführt worden, der die neuen Informationen (z.B. virtuellem statt physikalischem Server) in einer lokalen Datenbank gespeichert hat. Es sind einige Punkte anders behandelt worden und orientieren sich nur lose an den ITIL Prozessen. Eine Einführung von ITIL ist aber in Planung, wovon vor allem der zweite Anwendungsfall profitieren kann. Dieser wurde auch in Anlehnung an der ITIL entwickelt und kann, wie in Abschnitt 4.1.3 vorgestellt, umgesetzt werden. Die letzte Anforderung befasst sich mit der Anbindung von verschiedenen Datenspeicher, wie lokale Platten oder SAN. Dieser Punkt ist vor allem für das Leistungsverhalten im letzten Abschnitt wichtig, denn die virtuelle Maschine war im Test lokal gespeichert. So konnten mögliche Verzögerungen zum Datenspeicher ausgeschlossen werden, was einen besseren Vergleich zum physikalischen Host ermöglicht. Auch zu Beginn der Einrichtung der Virtualisierungsumgebung, wurde die erste Testmaschine lokal und nicht auf dem SAN gespeichert. Eine Anbindung mittels iSCSI kam nicht zum Einsatz, wodurch auch darüber keine Informationen gegeben werden kann. Insgesamt wurden auch hier fast alle Anforderungen vollständig erfüllt. Abstriche müssen nur bei der Sicherung von VMs im laufenden Betrieb, Gewährleistung von Hochverfügbarkeit bei VMs und die Umsetzung der ITIL Prozesse vorgenommen werden.

Wie die zuvor beschriebenen Anforderungen zeigen, werden fast alle Punkte nach der Umsetzung erfüllt. In den wenigen Fällen, wo dies nicht der Fall ist, erfolgte eine entsprechende Bewertung, ob es sich um essentielle Probleme handelt. Meist waren die Anforderungen nur eingeschränkt erfüllt und haben für den hier vorliegenden Anwendungsfall eine untergeordnete Rolle gespielt. So ist insgesamt die Messung an dem Anforderungskatalog erfolgreich, wenn dies auch für das Leistungsverhalten zutrifft. Welche Punkte dabei untersucht wurden und welche Ergebnisse die Testfälle lieferten, werden im nächsten Abschnitt genau vorgestellt.

7.1.2 Das Leistungsverhalten im Detail

Um das Leistungsverhalten zu ermitteln, gibt es mehrere Punkte, die untersucht werden müssen. So können sowohl E/A Operationen, Bussysteme, CPU, Speicher oder die Netzwerkschnittstellen auf ihre Leistungsfähigkeit getestet werden. Dazu bietet VMware seit kurzem ein Programm, namens *VMmark*, an, mit dem ein umfangreicher Testfall aufgebaut werden kann (vgl. [vmh 07]). Dazu durchlaufen mehrere Referenzmaschinen, wie Email-, Datenbank- oder Webserver, mehrere Benchmarks und diese zeigen, wie performant das System ist. Dazu muss im Vorfeld ein umfangreiches Testfeld aufgebaut werden, in dem die Durchführung stattfindet. Dies wurde auch bei Astrium durchgeführt, doch leider konnte es nicht in Betrieb genommen werden. Die Testroutinen basieren auf mehreren Java Frameworks, die im hier vorliegenden Fall mehrere Fehler (*Exceptions*) geworfen haben. Auch mit der identischen Installation, wie in der Anleitung beschrieben, kam es gleich zu Beginn zu verschiedenen Fehlern, die ein Testen unmöglich machten. Daher kommt hier ein anderes Testsystem zum Einsatz, dass nicht von VMware ist. So handelt es sich um unabhängige Ergebnisse, die ermittelt werden können. Bei einem VMware Produkt besteht die Gefahr, dass die Ergebnisse hinterher nicht korrekt sind.

Für den vorliegenden Anwendungsfall werden nur die Leistungen der CPU und des Hauptspeichers getestet. Dazu existieren zwei identische Maschinen von HP (der ProLiant Serie), die beide mit zwei Dual-Core AMD Opteron Prozessoren ($\Rightarrow$ vier Prozessorkerne) ausgestattet sind. Des Weiteren sind beide Maschinen mit 4 GB

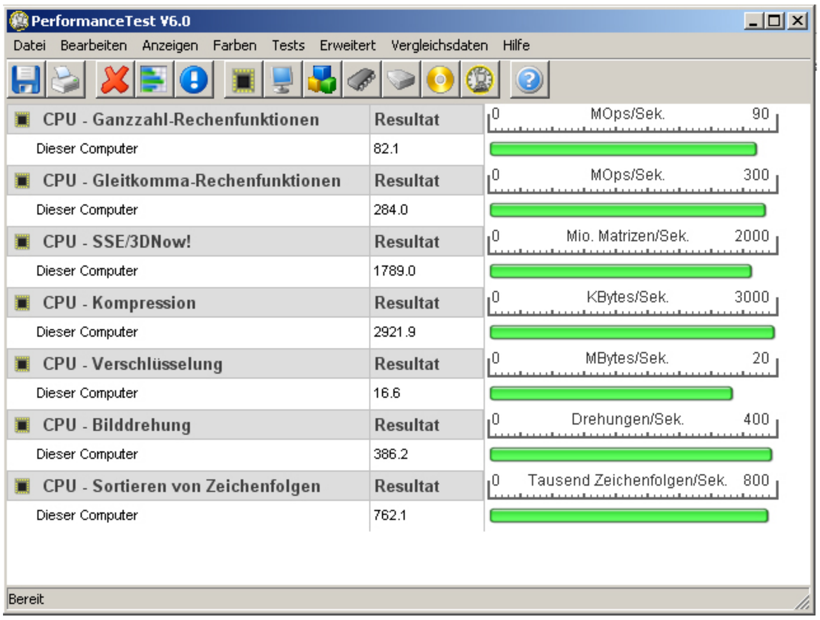

Abbildung 7.1: Die grafische Oberfläche des Benchmark-Tools *Passmark PerformanceTest* (Quelle: [pas 07])

Hauptspeicher ausgestattet, wobei es sich um identische Speichermodule handelt. Da auch die Architektur der Rechner identisch ist, befinden sich dieselben Bussysteme und auch Festplatten in den Rechnern. Dadurch ist ein optimale Vergleichsmöglichkeit gegeben, um mehrere Performanztests durchzuführen. Der Referenzserver wird mit *Windows 2003 Server SP1 Standard* installiert und hat neben dem Antivirenprogramm keine zusätzlichen Dienste oder Programme laufen. Die virtuelle Maschine befindet sich lokal auf einem ESX Server, auf dem ansonsten keine weitere Maschine läuft. In diesem Fall dient dieser Host nur für die eingerichtete Testmaschine. Diese wird nach demselben Vorbild, wie die Referenzmaschine installiert. Es werden alle vier Prozessorkerne an die VM durchgereicht und der physikalische Speicher wird auf 4 GB festgelegt. Das Betriebssystem ist dasselbe und neben dem Antivirenprogramm werden nur zusätzlich die *VMware Tools* installiert. Ansonsten läuft auch hier kein anderes Programm im Hintergrund. Sind beide Maschinen soweit vorbereitet, kann nun das Benchmarkprogramm installiert werden. Dazu wird das Programm *Passmark PerformanceTest 6.0* [pas 07] verwendet, das mehrere Testroutinen, sowohl bei der CPU, als auch beim Speicher durchführt. Die einzelnen Tests werden in den nächsten Abschnitten genauer vorgestellt. Ein Überblick, wie das Programm aufgebaut ist, kann in Abbildung 7.1 gesehen werden.
Es wurden mehrere Testdurchläufe durchgeführt, die alle nach demselben Prinzip abliefen. Auf den Testservern lief die Routine fünf mal hintereinander, danach wurde ein Neustart durchgeführt. Daraufhin gab es erneut fünf Durchläufe, deren Ergebnisse zu einem Durchschnittswert zusammengefasst wurde. So können die Werte gemittelt werden und es kommt zu keinen extremen Schwankungen. Der Neustart soll zeigen, ob das System nach einem Reboot ein anderes Verhalten zeigt. Dies war in allen Tests nicht der Fall. Dadurch ist hier die Korrektheit der Daten bestätigt worden.
Welche Maschinen miteinander verglichen wurden, ist sowohl bei der CPU, als auch beim Speicher identisch. Daher ist im Folgenden eine kurze Liste dargestellt, die alle Testmaschinen vorstellt:

- Vergleich zwischen einer VM und einem physikalischem Server mit zwei Prozessorkernen
- Vergleich zwischen einer VM und einem physikalischem Server mit vier Prozessorkernen
- Vergleich zwischen einer VM mit zwei Prozessorkernen gegenüber einer VM mit vier Kernen
- Vergleich zwischen einem physikalischem Host mit zwei Prozessorkernen gegenüber einem Host mit vier Kernen
- Vergleich zwischen zwei parallel laufenden VMs mit jeweils zwei Prozessorkernen gegenüber einem physikalischem Server mit zwei Kernen.

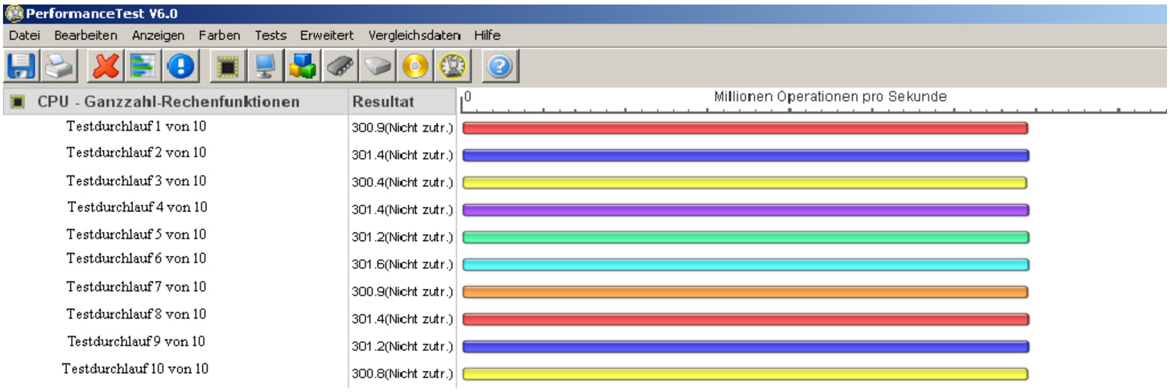

Abbildung 7.2: Übersicht bei zehn Durchläufen des CPU Tests „Ganzzahl-Rechenfunktionen”

Der letzte Punkt fällt etwas aus dem Rahmen, da hier ein Vergleich von mehreren Maschinen vorliegt. Dabei sollte untersucht werden, wie sich die Leistung der VMs verhält, wenn der ESX Server zwei Maschinen verwalten muss. Für diesen Testfall wurde die virtuelle Testmaschine geklont und lokal auf dem ESX Server gespeichert. Beide Maschinen haben jeweils zwei Kerne erhalten, mit jeweils 4 GB RAM. Für den Benchmark auf der Referenzmaschine wurde ein Dual-Core Prozessor ausgebaut, damit diesem nur noch ein Dual-Core (mit zwei Kernen) zur Verfügung steht. So konnte ein optimaler Vergleich gewährleistet werden. Im nächsten Abschnitt werden nun die Tests genauer vorgestellt. Danach erfolgen die Ergebnisse und eine Bewertung, wie diese zu deuten sind.

Benchmarkergebnisse CPU

Die Suite für die CPU besteht aus sieben Tests, die im Folgenden kurz vorgestellt werden:

- Ganzzahl-Rechenfunktionen (32-Bit- und 64-Bit-Addition, -Subtraktion, -Multiplikation und -Division); Wert: Million Operations per second (MOps/sec.)
- Gleitkomma-Rechenfunktionen (32-Bit- und 64-Bit-Addition, -Subtraktion, -Multiplikation und -Division); Wert: Million Operations per second (MOps/sec.)
- SSE/3DNow! (hier: 128-Bit-SSE-Vorgänge wie Addition, Subtraktion und Multiplikation); Wert: Million Matrices per second
- Kompression; Wert: Kilobytes per second (KBytes/sec.)
- Verschlüsselung; Wert: Megabytes per second (MBytes/sec.)
- Bilddrehung; Wert: Image rotations per second;
- Sortieren von Zeichenfolgen; Wert: Thousand Strings per second

Alle Tests werden in dieser Reihenfolge ausgeführt, und das Programm zeigt die Ergebnisse in einem mehrfarbigen Balkendiagramm. Abbildung 7.1 zeigt den CPU Testdurchlauf. Für zehn Durchläufe sieht es beispielsweise so aus, wie es in Abbildung 7.2 dargestellt ist. Diese Daten können aber auch über eine **.csv* Datei in ein entsprechendes Programm (z.B. *Microsoft Excel*) importiert werden. In Excel gibt es dann die Möglichkeit die jeweiligen Durchschnittswerte zu berechnen. Dies kann auch mit dem Vergleichsgerät erfolgen, wodurch später die Möglichkeit besteht, diese gegenüber zu stellen.
Im Folgenden werden nun die Ergebnisse aus den Tests vorgestellt, wie sie im vorherigen Abschnitt genannt worden. Dabei stellt der physikalische Host immer die Referenz mit 100% dar. Auf Basis der ermittelten Werte, wurde der Unterschied gegenüber der VM berechnet und in Prozent angegeben. Dieser Prozentwert wurde von der Referenzmaschine abgezogen und ergibt den Leistungswert der virtuellen Maschine. Hier ein Lesebeispiel für die Abbildung 7.3: „Der Leistungsverlust der VM im Vergleich mit dem physikalischem Host beträgt bei den Ganzzahl-Rechenfunktionen 6,07%. Dadurch arbeitet die virtuelle Maschine gegenüber dem Referenzgerät mit einer Leistung von 93,93%.” Nach diesem Schema sind alle folgenden Tabellen aufgebaut

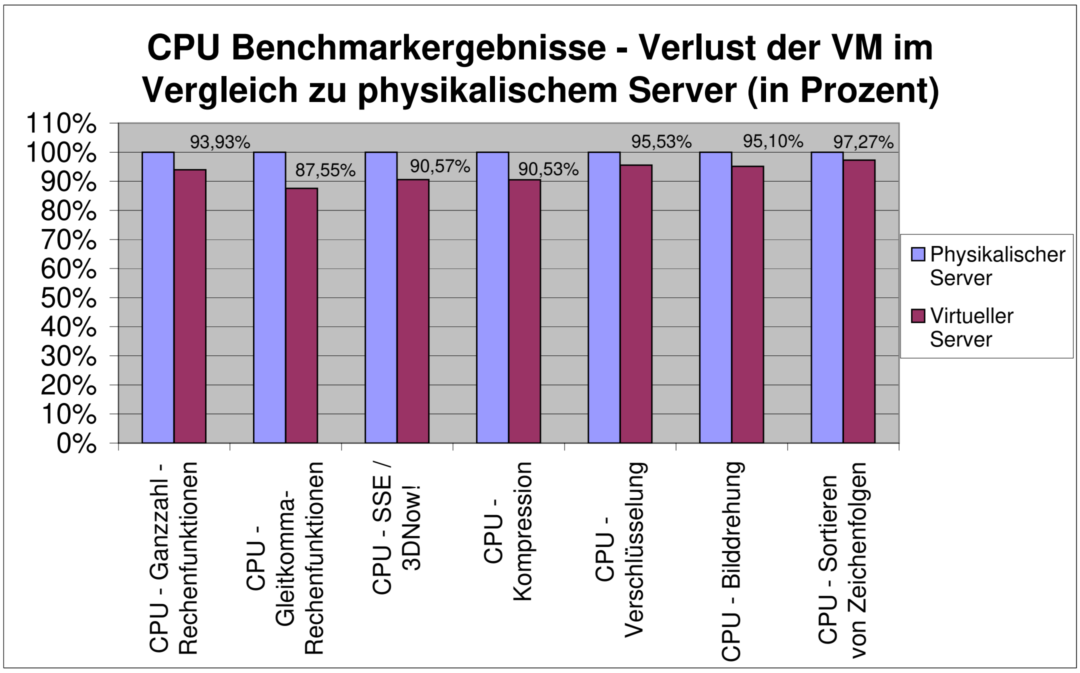

Abbildung 7.3: Prozentuale Abweichung (CPU) einer VM im Vergleich zu einem physikalischem Server, der mit seinen Ergebnis die 100% darstellt - für 2 Prozessorkerne

und werden dementsprechend interpretiert. Bei allen Versuchen entsteht ein bestimmter Verlust durch die Virtualisierungsschicht, die dazwischen geschaltet ist. Die folgenden Performanztests zeigen, wie stark dieser ausfällt und welche Operationen besser durchgereicht werden als Andere.

Testcase1: Als erstes erfolgt der Vergleich zwischen einem physikalischem und einem virtuellen Server mit jeweils zwei Prozessorkernen. Die ermittelten Werte sind in Abbildung 7.3 zu sehen. Dieser zeigt die stärkste Abweichung bei den Gleitkomma-Rechenfunktionen und die geringste bei der Sortierung von Zeichenfolgen. Der Durchschnittswert über alle Abweichungen ergibt einen Wert von 7,09%. Wird der Leistungseinbruch bei einem Gast aus der Abbildung 3.19 auf Seite 36 als Referenz genommen, so liegen alle Werte in diesem Bereich. So kann laut [Fert 06] der Leistungsverlust bei einem Gast mit VMware zwischen 3% und 18% liegen. So liegt die größte Abweichung mit ca. 12,5% knapp 6 Prozentpunkte unter dem angegebenen Höchstverlust. Insgesamt zeigt dieser Vergleich, dass eine VM unter VMware in den Bereichen „Verschlüsselung", „Bilddrehung" und „Sortieren von Zeichenfolgen" besonders gut arbeitet, wogegen die „SSE Berechnung", „Kompression" und vor allem die „Gleitkomma-Rechenfunktionen" im vorliegenden Fall schlecht abschneiden.
Testcase2: In diesem Testfall erfolgt die gleiche Gegenüberstellung, wie im Test zuvor, außer dass hier jeweils vier Prozessorkerne als Basis dienen. Die Tests waren diesselben und wurden nach dem gleichen Verfahren durchgeführt. Interessanterweise ist hier die größte Abweichung bei der Sortierung von Zeichenfolgen, die beim vorherigen Test noch den geringsten Leistungseinbruch dargestellt hat. Wie zuvor sind die Berechnungen bei der „Verschlüsselung" und der „Bilddrehung" sehr performant, wie in Abbildung 7.4 zu sehen ist. Die Tests ergaben dabei eine sehr geringe Abweichung von 0,77% bzw. 1,60%. Auch die Gleitkomma- und SSE Berechnungen fallen wie zuvor nicht gut aus. Insgesamt ist aber die durchschnittliche Abweichungen aller Berechnungen um über einen Prozentpunkt besser (hier: 5,71%). Ausnahme bildet, wie schon erwähnt, die Sortierung von Zeichenfolgen, die nach diesen Ergebnissen wesentlich schlechter, gegenüber der Referenzmaschine, mit vier Prozessorkernen arbeitet. Dennoch befindet sich auch hier der Wert mit knapp 13% Leistungsverlust innerhalb des gegebenen Rahmens. Ob sich diese Ergebnisse in anderen Testumgebungen mit möglichen anderen Programmen wiederholen lassen, müssten weitere Versuche durchgeführt werden.
Testcase3: Dieser Vergleich dient zur Gegenüberstellung der Werte zwischen einer physikalischen Maschine mit zwei und vier Prozessorkernen. Dies zeigt, ob eine Maschine mit zwei Kernen, auch nur halb so performant

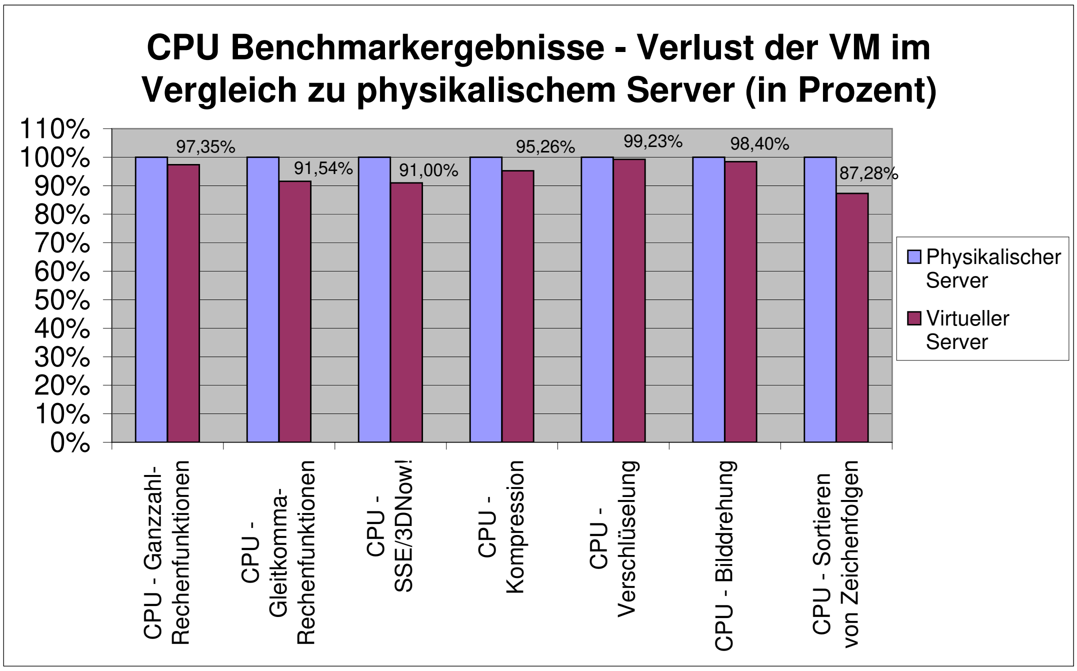

Abbildung 7.4: Prozentuale Abweichung (CPU) einer VM im Vergleich zu einem physikalischem Server, der mit seinen Ergebnis die 100% darstellt - für 4 Prozessorkerne

ist, als eine Maschine mit vier Prozessorkernen. Die Maschine mit vier Kernen dient dabei als Referenz, an der die andere Maschine sich messen muss. Abbildung 7.5 zeigt die Werte, die mit dem Benchmarkprogramm ermittelt worden sind. Dabei liegen alle Werte etwas über 50%, wobei auch hier die Sortierung von Zeichenfolgen mit 52,34% am Höchsten ist. Daher zeigt sich hier eine leichte Tendenz, dass bei der Sortierung eine Verteilung auf vier Kerne nicht so optimiert werden kann, wie auf zwei Kerne. Auch die Gleitkommaberechnungen liegen etwas erhöht (52,23%), aber noch im Rahmen. Insgesamt zeigt dieser Vergleich, dass folgende Aussage getroffen werden kann: Doppelt so viele CPU Kerne bringen auch eine (fast) doppelte Leistung. Auf Basis dieser Werte, ist nun interessant, ob dies auch bei einer VM gesagt werden kann.
Testcase4: Wenn sich die virtuellen Maschinen genauso verhalten, wie zuvor die physikalischen, dann wäre das vor allem für den zweiten Anwendungsfall interessant. Wird ein Server bereitgestellt und der Projektleiter benötigt zu einem späteren Zeitpunkt mehr Ressourcen, könnte auf Grund der Bechmarktests gewährleistet werden, dass eine entsprechende Leistungssteigerung danach vorliegt. Ob ein ähnliches Verhalten vorliegt, zeigt sich in Abbildung 7.6. Dabei waren die Ergebnisse der virtuellen Maschine mit vier Kernen die Referenz und die VM mit nur zwei durchgereichten Prozessorkernen musste sich daran messen. Dabei fällt auf, dass bis auf den letzten Punkt, alle Berechnungen ziemlich genau die Hälfte zum Referenzgerät leisten. Bei der Kompression liegt der Wert knapp 1% unter der Hälfte, aber befindet sich so noch in der Messtoleranz. Bei dem Sortiervorgang von Zeichenfolgen ist ein deutlich höherer Wert, als bei den übrigen Berechnungen, ermittelt worden. War es im vorherigen Testfall noch eine leichte Tendenz, sind es hier über 8%, die die Maschine mit zwei Kernen leistet. So ist eine optimierte Verteilung auf alle vier Prozessorkernen durch die Virtualisierungsschicht, weitaus schlechter, als dies im vorherigen Testcase der Fall war. Dieses Verhalten hat sich auch schon in den ersten beiden Testfällen gezeigt, dass VMware hier ein abweichendes Verhalten zeigt. Es sei nochmal erwähnt, dass dieses Verhalten durch andere Tests mit anderen Programmen überprüft werden muss, bevor hier definitive Aussagen getroffen werden können. Dennoch sollte bei Programmen, die Sortierungsalgorithmen abarbeiten, geprüft werden, ob sich dabei ein anderes Leistungsverhalten zeigt, wenn vier anstatt zwei Prozessorkerne verwendet werden. Doch auch hier, befindet sich die Abweichung innerhalb der gegebenen Grenzen.
Testcase5: Im letzten Testfall für die CPU, kommt es zum Vergleich zwischen zwei parallel laufenden VMs mit jeweils zwei Kernen auf einem ESX Server. Als Referenzmaschine dienen die ermittelten Werte aus dem vorherigen Fall von einem physikalischem Server mit zwei Prozessorkernen. Die Ergebnisse dieses Tests sind in der Abbildung 7.7 zu sehen, wobei sich die angegebenen Prozentwerte immer im Verhältnis zum Refe-

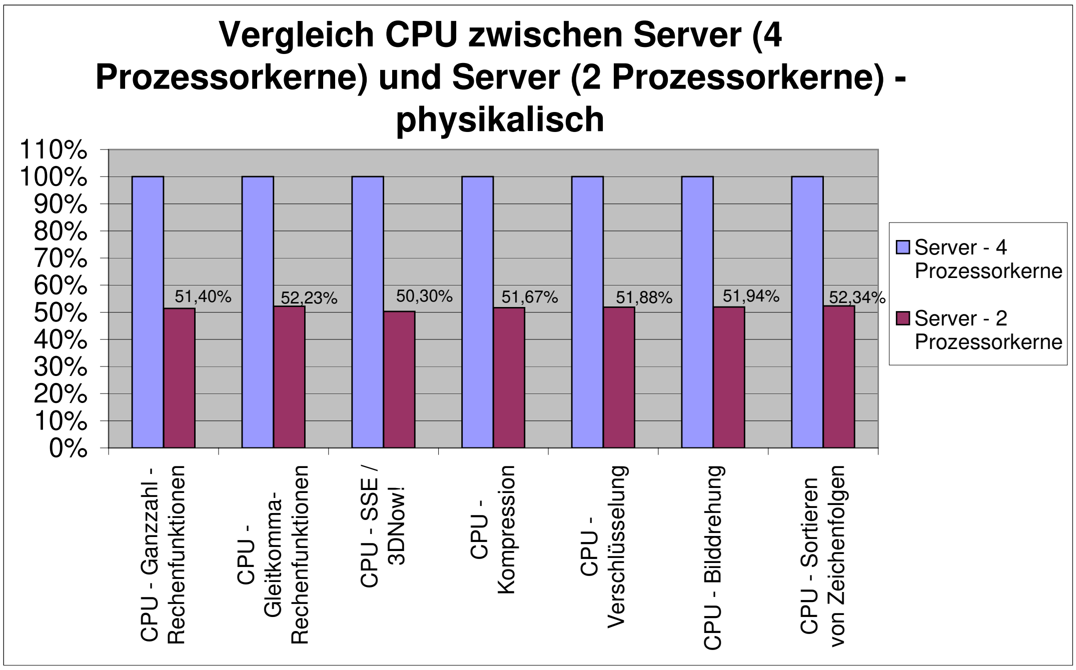

Abbildung 7.5: Prozentuale Abweichung (CPU) einer physikalischen Maschine mit 2 Prozessorkernen von einer Maschine mit 4 Kernen

renzgerät beziehen. Die virtuellen Maschinen waren über eine NTP Zeitquelle synchronisiert, so dass mittels Skript, der Benchmark gleichzeitig starten konnte. Während der Testdurchläufe wurden die Maschinen auch beobachtet, ob das Skript auch korrekt startet. Dies war auch immer der Fall, dennoch fällt in der Abbildung auf, dass der zweite Server immer etwas besser abschneidet. Diese Abweichungen liegen bei ca. 1 bis 3 Prozent zwischen den beiden VMs. Werden die Werte mit dem ersten Testcase verglichen, so fällt auf, dass das Verhalten mit zwei parallel laufenden Maschinen ähnlich zu einer Maschine ist. Bei den SSE Berechnungen ist der Wert etwas schlechter, aber auch hier ist die Sortierung von Reihenfolgen das beste Ergebnis. Insgesamt ist der durchschnittliche Leistungseinbruch bei der ersten 8,11% und bei der zweiten VM 6,23%. Der Durchschnitt über beide Maschinen beträgt 7,17% und ist fast identisch zu dem ermittelten Wert im ersten Testfall (dort lag der Wert bei 7,09%). Daher kann gesagt werden, dass bei zwei parallel laufende VMs auf einem lokal gespeicherten ESX Server, der Leistungseinbruch minimal ist. Bei der einen Maschine hat sich der Wert um ca. einen Prozentpunkt verbessert, bei der anderen um einen verschlechtert. Diese Werte liegen innerhalb der Messtoleranz und auch hier müssten weitere Tests zeigen, ob sich dieses Verhalten auch bei anderen Testumgebungen zeigt. Außerdem wäre es interessant, wie sich mehrere laufende Maschinen verhalten, ob beispielsweise bei vier parallelen VMs, es zu einem Einbruch kommt oder nicht.

Alle durchgeführten Tests haben gezeigt, dass sich der Leistungsverlust bei den meisten Berechnungen in Grenzen hält. Der Maximalwert von 18 Prozent Leistungseinbruch (siehe [Fert 06]), wurde bei keinem Test annähernd erreicht, der stärkste Einbruch war im letzten Testcase mit knapp 14% (siehe Abbildung 7.7 bei den Gleitkomma-Rechenfunktionen). Interessant wäre ein Vergleich mit dem Benchmarkprogramm *VMmark* von VMware. Durch *VMmark* hätte sich zeigen können, ob in dieser Umgebung es zu ähnlichen oder besseren Werten gekommen wäre. Leider, wie zuvor beschrieben, konnte das Programm aber nicht zum Laufen gebracht werden, womit dieser Vergleich hier fehlt. Dennoch geben die ermittelten Werte mit Passmarks *PerformanceTest* einen ersten Eindruck, bei welchen Aufgaben die virtuelle Maschine gut abschneidet und bei welchen Punkten es zu schwächeren Ergebnissen kommt. Im nächsten Abschnitt werden die ersten vier Testfälle für den Speicher betrachtet. Hier wird überprüft, wie stark die Leistungseinbußen sind, wenn die Virtualisierungsschicht die Anfragen durchreichen muss.

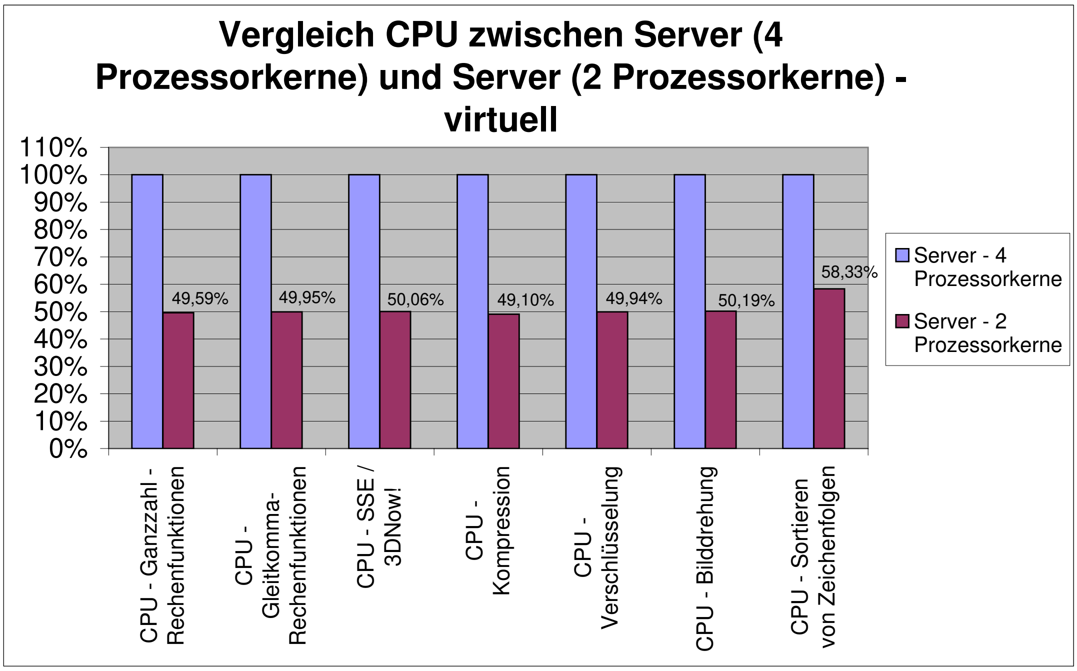

Abbildung 7.6: Prozentuale Abweichung (CPU) einer virtuellen Maschine mit 2 Prozessorkernen von einer Maschine mit 4 Kernen

Benchmarkergebnisse Speicher

Auch die Speichersuite von *PerformanceTest* besteht aus mehreren Tests, die hintereinander durchgeführt werden. Alle Tests arbeiten beim Lesen oder Schreiben vom oder in den Arbeitsspeicher mit einer Kombination aus 32-Bit- und 64-Bit-Daten (vgl. [pas 07]). Dabei werden folgende Benchmarks durchgeführt:

- Kleinen Block zuweisen: Bei diesem Test wird die Zeit gemessen, die benötigt wird, um kleine Nullspeicherblöcke (mit einer Blockgröße von ca. 100 KB) zuzuweisen und freizugeben [pas 07]; Wert: Megabytes per second (Mbytes/sec.)
- Lesen - Mit Cache: Bei diesem Test wird die Zeit gemessen, die benötigt wird, um einen kleinen Speicherblock zu lesen. Der Block ist klein genug, um vollständig im Cache gehalten zu werden [pas 07]; Wert: Megabytes per second (Mbytes/sec.)
- Lesen - Ohne Cache: Bei diesem Test wird die Zeit gemessen, die benötigt wird, um einen großen Speicherblock zu lesen. Der Block ist zu groß, um im Cache-Speicher gehalten zu werden [pas 07]; Wert: Megabytes per second (Mbytes/sec.)
- Schreiben: Bei diesem Test wird die Zeit gemessen, die benötigt wird, um Informationen in den Speicher zu schreiben; Wert: Megabytes per second (Mbytes/sec.)
- Großer RAM-Speicher: Dieser Test misst die Fähigkeit, sehr große RAM-Mengen zuzuweisen, und die für das Lesen dieses RAM-Speichers benötigte Zeit. Der Test ist so konzipiert, dass er die Fähigkeit des Systems misst, extrem RAM-intensive Anwendungen zu unterstützen [pas 07]; Wert: Operations per second

Die Präsentation der Daten verläuft wie beim CPU Benchmark über ein Balkendiagramm (siehe Abbildung 7.2 auf Seite 96). Die Daten wurden auch hier in Excel exportiert und dann entsprechend ausgewertet. Welche Ergebnisse die Daten liefern, werden in den folgenden Testcases vorgestellt. Die Hauptspeicher-Konfiguration ist bei allen Maschinen gleich: 4 GB RAM. Dies war bei der Referenzmaschine auch der tatsächlich verbaute Hauptspeicher. Der ESX Server verfügt insgesamt über 16 GB, wobei für die virtuelle Maschine auch nur 4 GB zur Verfügung gestellt wurden. Mehr als der angegebene Hauptspeicher kann das 32-Bit *Windows 2003 Server Standard* - System auch nicht nutzen, da sich mit 32 Bit nicht mehr Speicherinhalte adressieren las-

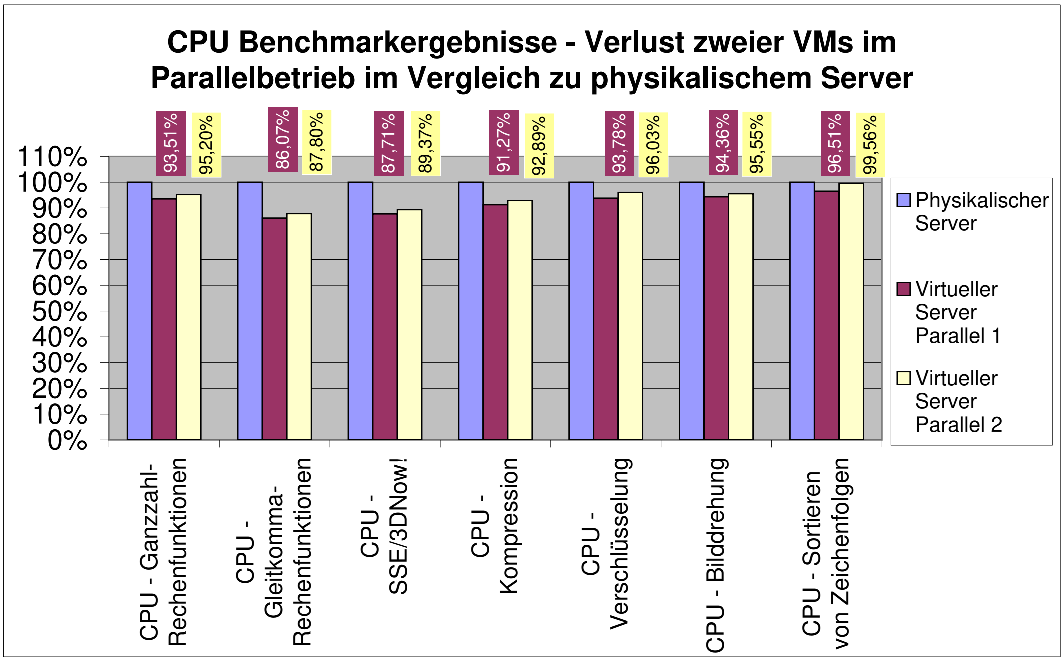

Abbildung 7.7: Prozentuale Abweichung (CPU) einer physikalischen Maschine mit 2 Prozessorkernen von zwei parallel laufenden VMs mit jeweils 2 Kernen

sen (2^{32} = 4.294.967.296 Bytes). Die Standard Version verfügt über keine zusätzlichen Erweiterungen, die mehr Hauptspeicher unterstützen würde. Daher ist in allen Tests immer der maximal mögliche Hauptspeicher im Einsatz. Da es sich um baugleiche Testserver (sowohl die Referenzmaschine, als auch der ESX Server) handelt, arbeiten in beiden Maschinen dieselben Speicherbausteine (Firma, Zugriffsgeschwindigkeit, etc.) mit den selben Bussystemen. Wie genau VMware die Speicheraufteilung löst, kann nicht genau gesagt werden, es zeigt sich aber in den Tests, wie gut Speicheranfragen durchgereicht werden.

Testcase1: Beim ersten Testfall gilt es, wie zuvor das Leistungsverhalten zwischen einem physikalischem Server, der die Referenz bildet und einem virtuellen Server zu vergleichen. Dies sei erwähnt, um festzustellen, ob im zweiten Testcase Unterschiede entstehen, wenn vier Prozessoren als Basis dienen. Abbildung 7.8 zeigt, wie sich die Speicherzugriffe, im Vergleich zur Referenz, verhalten haben. Wie an den Werten zu sehen ist, ist der Leistungseinbruch, bis auf den letzten Test, kaum vorhanden. So ist beim ersten Speichertest kaum ein Unterschied vorhanden (nur 0,40% weniger) und auch die restlichen drei Tests fallen nicht unter zwei Prozent. Auf Grund dieser Ergebnisse ist das Leistungsverhalten bei den ersten vier Tests sehr zufriedenstellend. Der letzte Test fällt hier stark aus dem Rahmen, wenn es um große Speichermengen geht. Dieser Einbruch ist damit zu erklären, dass von den 4 GB zugeteilten Speicher, ein Teil für das Hostsystem (nämlich der ESX Server) zur Verfügung stehen. Dadurch kommt der Test schon wesentlich früher an die ihm zur Verfügung stehende Grenze und muss mittels Paging auf die Festplatte ausweichen. Dadurch befindet sich eine ausgelagerte Speicherdatei auf dem wesentlich langsamen Hintergrundspeicher (hier: lokale Festplatte des ESX Servers), wodurch die Zugriffe sich deutlich verschlechtern. Außerdem muss bei jedem Zugriff berechnet werden, wo sich die gewünschte Seite befindet (entweder im Haupt- oder im Hintergrundspeicher). All diese Vorgänge führen zu dem starken Leistungseinbruch, wie er hier zu sehen ist. Dementsprechend eignen sich hauptspeicherintensive Anwendungen nicht für virtuelle Maschinen. Dies wird von den Anbietern von Virtualisierungsumgebungen auch teilweise genannt, dass sich rechen- und speicherintensive Anwendungen sich nicht als virtuelle Maschinen eignen. In solchen Fällen, sind eigenständige physikalische Server wesentlich besser geeignet, was sich hier im Test auch zeigt. Dennoch könnte solch ein Leistungseinbruch noch wesentlich stärker ausfallen, da die Geschwindigkeitsunterschiede zwischen Haupt- und Festplattenspeicher signifikant hoch sind.

Testcase2: Im zweiten Testfall werden dieselben Tests wie zuvor durchgeführt, außer das diesmal die Maschinen jeweils mit vier Prozessorkernen ausgestattet sind. Dabei fällt auf, dass beim ersten Test (siehe Abbildung 7.9) der Wert wesentlich schlechter als zuvor ist. So ist hier ein Leistungseinbruch von über fünf Prozent. Scheinbar hängt diese Funktion mit der CPU zusammen, die bei diesem Test eine Verarbeitung mit zwei Ker-

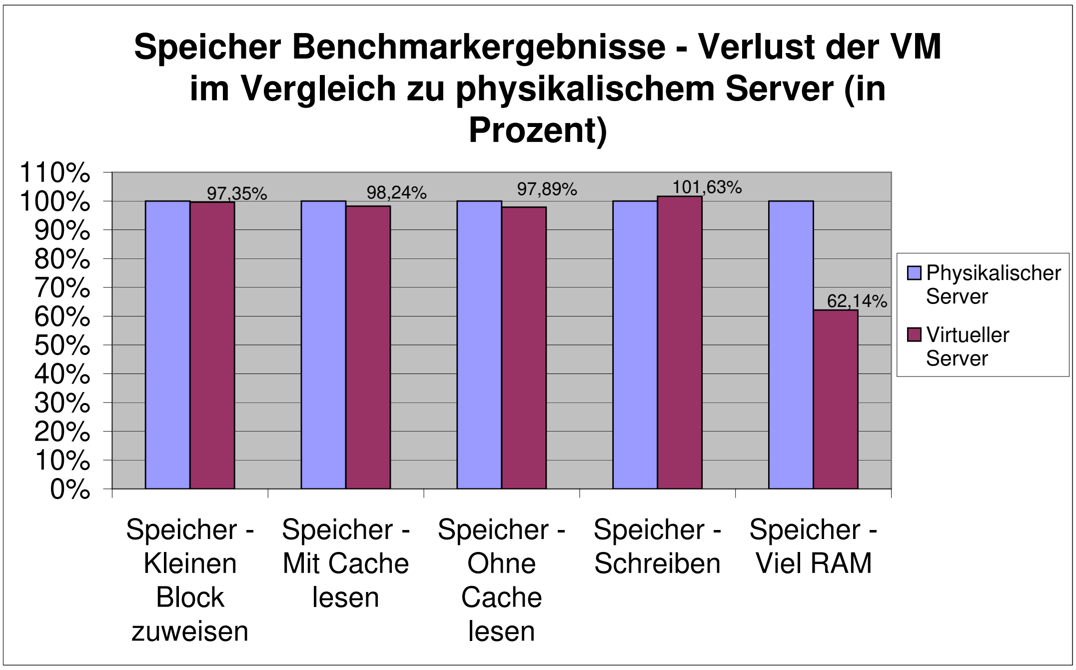

Abbildung 7.8: Prozentuale Abweichung (Speicher) einer VM im Vergleich zu einem physikalischem Server, der mit seinen Ergebnis die 100% darstellt - für 2 Prozessorkerne

nen, wesentlich besser durchgeführt werden kann, als bei vier Kernen. Die restlichen drei Tests weisen wieder Verluste auf, die beim zweiten und vierten Test sogar noch geringer, als im vorherigen Test sind (vergleiche Abbildung 7.8 und 7.9). Ausreißer ist auch hier der letzte Test, bei dem wie zuvor das Problem des Hostsystems besteht. Ist die Grenze des zur Verfügung stehenden Hauptspeichers erreicht, kommt es zu einem starken Rückgang, der hier noch etwas stärker ausfällt (zuvor: 62,14%; jetzt: 57,42%). Es zeigt sich auch hier, dass speicherintensive Anwendungen sich für eine Virtualisierung nicht eignen.
Testcase3: Wie bei den Speichertests erfolgt auch hier ein Vergleich der Maschinen untereinander. Dies soll zeigen, wie sich das Verhalten ändert, wenn der Maschine nur zwei Prozessorkerne zur Verfügung steht. Hat sich im vorherigen Abschnitt gezeigt, dass mit einer doppeltem Kernanzahl, diese auch fast doppelt so leistungsstark sind, muss sich zeigen, ob der erhöhte Verwaltungsaufwand auch Auswirkungen auf die Leistung des Speichers hat. Die ermittelten Werte sind in Abbildung 7.10 zu sehen. Zuerst fällt auf, dass bei dem Test „Viel RAM" die Leistung des Referenzsystems wesentlich besser ist, als wenn nur zwei Kerne arbeiten. Scheinbar können diese hohen Datenmengen über die vier Kerne besser abgearbeitet werden, als bei dem Vergleichsgerät. Auf der anderen Seite fällt aber auf, dass bei drei Tests („Mit Cache lesen", „Ohne Cache lesen" und „Schreiben") die Maschine mit zwei Prozessorkernen leistungsfähiger bei den Speichertests ist, als eine Maschine mit vier Kernen. Beim Schreibtest ist sogar eine Steigerung von über drei Prozent gegenüber der Referenzmaschine. Dieses Phänomen ist überraschend, da sich am Speicher und dem System an sich nichts geändert hat und dies theoretisch gleich sein müsste. Eine mögliche Erklärung wäre, dass das hier verwendete Bussystem des Servers einen Flaschenhals bildet. Bei den Prozessoren handelt es sich um zwei Dual-Core AMD Opterons, bei denen die Speicherzugriffe über den Prozessor laufen. Alle vier Prozessorkerne greifen auf ein Bussystem zu, dass möglicherweise hier bei bestimmten Tests zu einer Engstelle fungieren könnte. Leider liegen von den Testabläufen keine genaueren Informationen vor, so dass dieses Verhalten nicht genau erklärt werden kann. Dazu müsste die Leistungsfähigkeit des Bussystems und in wieweit dies ausgelastet wird genauer untersucht werden. Dennoch ist dieses Verhalten ein interessanter Ansatz, der nun überprüft werden muss, ob es sich bei den virtuellen Maschinen auch so verhält.
Testcase4: Bei einem Vergleich zwischen virtuellen Maschinen mit zwei und vier Prozessorkernen zeigt sich ein ähnliches Verhalten (Ergebnisse siehe Abbildung 7.11). Erste Besonderheit ist, dass der Speichereinbruch bei dem Test „Viel RAM" hier nicht vorhanden ist, denn hier fällt der Test für die VM mit zwei Kernen etwas besser aus gegenüber der Referenzmaschine (0,75% besser). Insgesamt liegt aber nur ein Wert knapp unter der Referenz (siehe „Speicher - Mit Cache"), ansonsten sind auch hier die Werte etwas besser, als zur Maschi-

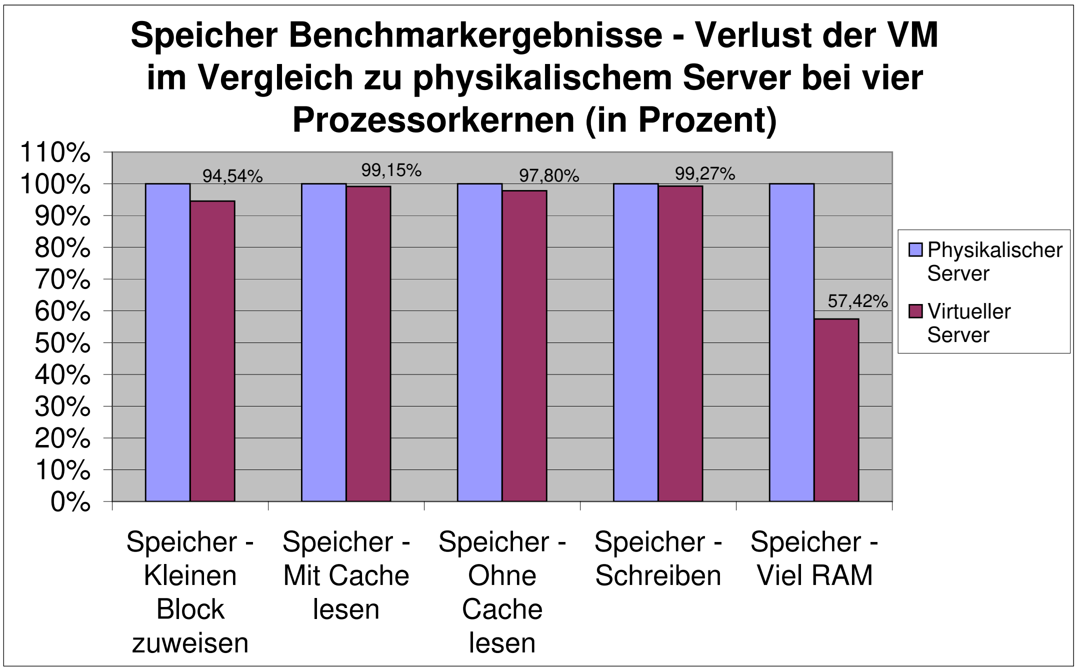

Abbildung 7.9: Prozentuale Abweichung (Speicher) einer VM im Vergleich zu einem physikalischem Server, der mit seinen Ergebnis die 100% darstellt - für 4 Prozessorkerne

ne mit vier Prozessorkernen. Die Abweichungsvarianz ist hier etwas geringer, als im Test zuvor und hat den höchsten Peak bei ca. zwei Prozentpunkten. Da es sich um eine baugleiche Maschine zum Test davor handelt, ist auch hier die Vermutung, dass das Bussystem einen Flaschenhals darstellt. Doch sei auch hier nochmal darauf hingewiesen, dass dies nur eine Vermutung ist und keine weiteren konkreten Daten über das System und die Test Suite vorliegt. Auch hier müssten weitere Tests erfolgen, um dieses Auftreten weiter zu untersuchen. Mit den vorliegenden Daten könnte aber die Aussage getroffen werden, dass mit vier Prozessorkernen die Speicherleistung sich leicht verschlechtert gegenüber einer virtuellen Maschine mit zwei Kernen. Dieses Phänomen war auch schon bei der physikalischen Testmaschine aufgetreten.

Insgesamt ist das Leistungsverhalten, in Bezug auf den Speicher, bei den virtuellen Maschinen sehr gut und es gibt meist nur einen Verlust von wenigen Prozentpunkten. Ausnahme zeigen die Tests, sobald große RAM Mengen abgehandelt werden. Dabei stößt das System an seine Grenzen, da für den Host ein gewisser Speicherbereich freigehalten wird. So steht der komplett zugeteilte Hauptspeicher nicht zur Verfügung und es kommt ab einem gewissen Punkt zum Auslagern des Speichers. Dies führt zu einem starken Einbruch der Leistung, wenn der wesentlich langsamere Hintergrundspeicher hinzugezogen wird. Daher wird empfohlen, keine speicherintensive Programme in einer virtuellen Maschine laufen zu lassen (vgl. [AHN 07] und [ZIM 06]). Dies haben die durchgeführten Tests auch belegt. Ein interessantes Verhalten ist in Bezug auf die Verwendung von mehreren Kernen aufgetreten. Hier scheint das vorliegende Bussystem an seine Grenzen zu stoßen, wenn anstatt zwei vier Kerne verwendet werden. Ob dieses Verhalten nur Zufall oder ein generelles Problem darstellt, kann aber in dieser Testumgebung nicht genauer bestimmt werden. Dazu fehlen einige Informationen über die durchgeführten Tests, das Bussystem und die Leistungsmerkmale der verwendeten Prozessoren.
Im letzten Abschnitt kommt es zu einer Zusammenfassung aller ermittelten Ergebnisse und welche Schlussfolgerungen daraus gezogen werden können.

7.2 Schlussfolgerungen aus dem Verhalten

Werden nun auch die Ergebnisse aus den Benchmarks in der Anforderungsanalyse miteinbezogen, dann ergibt sich ein recht positives Bild von der Umsetzung der Virtualisierungsumgebung und der Use Cases. Die

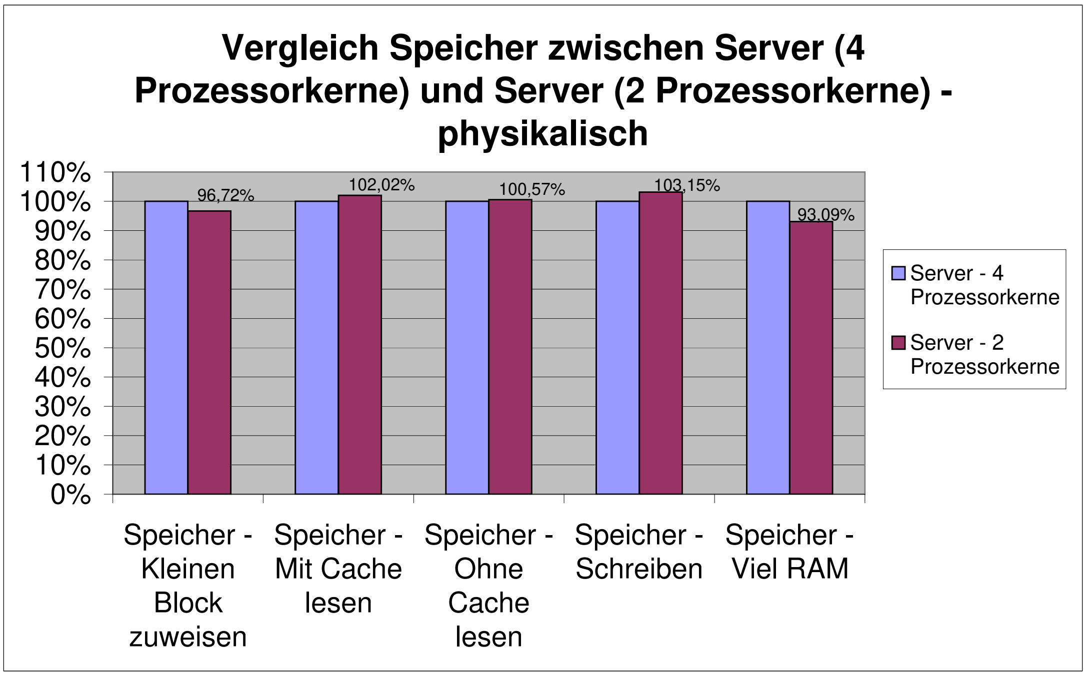

Abbildung 7.10: Prozentuale Abweichung (Speicher) einer physikalischen Maschine mit 2 Prozessorkernen von einer Maschine mit 4 Kernen

Testfälle haben gezeigt, dass die Performanz bei ausgelasteter CPU meist nur wenige Prozentpunkte hinter der Referenzmaschine liegt. Diese Tests sind so konzipiert, dass sie die CPU in verschiedenen Punkten auslasten, was in der vorliegenden Virtualisierungsumgebung kaum passiert. Die meisten virtuellen Maschinen nutzen nur ein Bruchteil der ihnen zur Verfügung stehenden CPU und Speicher. Dadurch erreichen sie die Grenzen nicht, aber die Testfälle haben gezeigt, dass diese nicht signifikant hinter der einer physikalischen Maschine liegen. Interessant wird das Verhalten der Leistung, je mehr Maschinen hinzukommen. Dies hätte beispielsweise *VMmark* durchgeführt, bei dem eine bestimmte Anzahl an Testmaschinen laufen, um deren erreichte Leistung mit der erwarteten zu vergleichen. Leider war dies, wie zuvor beschrieben, nicht möglich, da im vorliegenden Umfeld das Programm nicht zum Laufen gebracht werden konnte. So können nur die Ergebnisse des Benchmarkprogramms von Passmark herangezogen werden, die bereits ausführlich beschrieben wurden.

Insgesamt hat sich gezeigt, dass mit VMware eine professionelle Virtualisierungsumgebung aufgebaut werden kann, die mit den vielen Funktionen eine umfangreiche Administration gewährleistet. VMware betrachtet sowohl Sicherheits-, als auch Leistungsaspekte, um eine praxistaugliche Virtualisierung zu gewährleisten. Die Realisierung hat gezeigt, dass bis auf kleinere Probleme, die Umsetzung gut durchzuführen ist. Auch die Performanz der virtuellen Maschinen hat sich positiv hervorgetan und hat für den Anwendungsfall bei Astrium vollkommen ausgereicht. Dieses Produkt mit seinen Erweiterungen hat aber auch seinen Preis und ist für größere Unternehmen und Einrichtungen nur dann sinnvoll, wenn die Eigenschaften auch genutzt werden. Bei kleineren Umgebungen, sollte auf andere Produkte von VMware oder anderen Herstellern zurückgegriffen werden. Mittlerweile existiert auf dem Markt ein großer Konkurrenzkampf, dessen Auswirkung für den Kunden, durch günstiger und leistungsstärkere Produkte, nur von Vorteil sein kann. Diese Arbeit bietet mit der Umsetzung auf Basis von VMware eine Vergleichsmöglichkeit an, an der sich weitere Umsetzungen messen können. Hier wäre zum Beispiel interessant, wie sich das kommerzielle XenSource gegenüber VMware in den einzelnen Bereichen verhält. Gerade beim Leistungsverhalten sind einige interessante Fragestellungen aufgekommen, die für weitere Projekte und Arbeiten interessant wären.

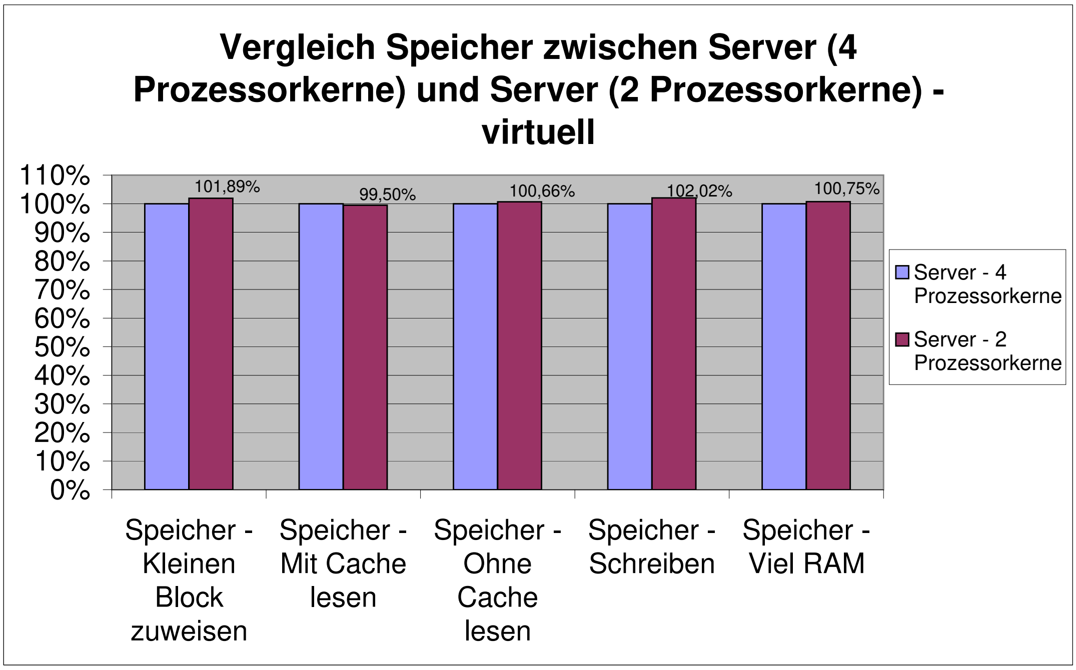

Abbildung 7.11: Prozentuale Abweichung (Speicher) einer virtuellen Maschine mit 2 Prozessorkernen von einer Maschine mit 4 Kernen

8 Zusammenfassung und Ausblick

Insgesamt hat die Arbeit gezeigt, welche vielseitigen Möglichkeiten in einer modernen Virtualisierungsumgebung vorhanden sind. Dabei ist aufgefallen, wie wenig von den Ressourcen aktueller Systeme genutzt werden. Um diese sinnvoll zu verteilen, ist mit der Virtualisierung eine Technik gegeben, die eine verbesserte Ausnutzung bietet. Der Markt entwickelt sich so rasant, dass aktuelle Produkte fortwährend verbessert werden, um eine noch effektivere Nutzung der Ressourcen zu ermöglichen. Zusätzlich kommt die Entwicklung von hardware-basierter Virtualisierung hinzu, die mit Intels und AMDs neuer Prozessorgeneration erst am Anfang ihrer Möglichkeiten steht. Je tiefer die Virtualisierung im System unterstützt wird, desto weniger Verlust entsteht durch software-basierte Zwischenschichten. So bietet VMware in Kooperation mit einigen Serverherstellern Ende 2007 eine neue Variante des ESX Servers (*ESX Server 3i* genannt) an, der künftig als Flash-Modul in den Servern eingebaut ist. Damit befindet sich der auf 32 MByte geschrumpfte Server im Gerät und ermöglicht virtuelle Maschinen direkt auszuführen, so dass ein Hostsystem nicht mehr notwendig sein wird. Auch die aktuellen Produkte zeigen, welches Potential in ihnen steckt und der Markt signalisiert großes Interesse an der Entwicklung dieser Technologie.
Gerade das Eintauchen in eine neue Technologie hat die Bearbeitung der Aufgabe sehr interessant gemacht. Zwar wurde mit VMware das Produkt im Vorfeld bereits ausgewählt, aber die wichtigen Punkte in Bezug auf Aufbau, Einrichtung und Verwaltung waren nicht fest vorgegeben und ließen dadurch genügend Spielraum, eine sinnvolle Umsetzung zu implementieren. Weitere Punkte wie Sicherheit, Backuplösungen und Migration der Server sind bedacht und erarbeitet worden. Die typischen Anforderungen aus der Praxis führten dazu, dass diese in einem allgemeinen Konzept behandelt wurden. Denn für eine professionelle Virtualisierung, unabhängig welches Produkt eingesetzt wird, sind (fast) immer die zuvor genannten Punkte zu beachten. So kam es zu dem vorgestellten Konzept, dass für den Anwendungsfall „Virtualisierung von verschiedenen Servern mit unterschiedlichen Betriebssystemen" gedacht ist.
VMware gehört mit seiner Produktpalette zum „Platzhirsch" in diesem Bereich und bietet für fast alle Einsatzgebiete unterschiedliche Produkte an. Das bei der Astrium GmbH zum Einsatz gekommene *VMware Infrastructure 3* zeichnet sich durch umfangreiche Möglichkeiten aus, die gerade im Datacenter-Bereich große Verwendung finden. Durch die ausführliche Dokumentation, die einerseits von VMware, aber auch durch die Erfahrung vieler anderer Anwender zur Verfügung steht, ist eine Umsetzung einfach und komfortabel zu erreichen. Aufgrund der umfangreichen Möglichkeiten dieses Produktes liegt die Gefahr in der richtigen Konfiguration. Durch die Vielzahl an Möglichkeiten ergeben sich Fehler, die rechtzeitig vom Fachpersonal entdeckt werden müssen. An dieser Stelle spielt das „Know How" der Administratoren eine große Rolle. Sind aber alle Einstellungen korrekt vorgenommen, entsteht schnell eine verbesserte Administration der virtuellen Maschinen. Beispielsweise ist nach einiger Zeit die Livemigration nicht mehr wegzudenken. Das Verschieben von VMs läuft einfacher und sicherer. Dabei wird fast vergessen, dass es sich um einen Server handelt, der hier migriert wird. Aber auch die restlichen Funktionen arbeiteten bei der Umsetzung einwandfrei und das aufgebaute System, bestehend aus zwei ESX Servern mit einem Virtual Center Server, lief seit der Einrichtungsphase weitestgehend stabil. Des Weiteren lief das Update der ESX Server von Version 3.0.1 auf 3.0.2 (eine größere Umstellung, als dies auf den ersten Blick erscheint) ohne Probleme und führte zu keiner Beeinflussung des aufgebauten Systems.
Insgesamt war bei der Umsetzung zu beachten, dass es einerseits zu keiner Beeinträchtigung des bisherigen Ablaufs kommt und andererseits alle Schritte nachvollziehbar umgesetzt werden. Ein wichtiger Punkt ist auch, dass Administratoren, die nicht mit der Materie vertraut sind, mit Hilfe einer erstellten Dokumentation schnell das notwendige Wissen erarbeiten können. Dies spart dem Unternehmen in erster Linie Zeit und Geld. All dies war eine interessante Herausforderung, einerseits die Virtualisierungsumgebung mit all ihren Möglichkeiten zu nutzen und andererseits alle Handlungsschritte logisch darzulegen, warum welche Eigenschaften so genutzt wurden. Besonders das Hinterfragen von Einstellungen und Vorgehensweisen half, die Technik detailliert zu verstehen und diese Erfahrung in das Konzept einfließen zu lassen. Am Anfang stand ein Basiskonzept, das durch die Praxis immer wieder verfeinert wurde. Aufgrund dieser ständigen Bearbeitung existiert jetzt ein praxiserprobter Leitfaden, mit dem eine Virtualisierung durchgeführt werden kann. Dieser kann nicht für den

Anwendungsfall Astrium, sondern für eine beliebige Hostvirtualisierung eingesetzt werden.
Aber nicht nur die Umsetzung und Bedienung muss komfortabel sein, sondern auch die Leistung muss dem Vorgänger-System entsprechen. Gerade hier hat sich gezeigt, dass bei VMware mit Leistungseinbußen zu rechnen ist. Diese halten sich aber in Grenzen (d.h. Kosten-Nutzen-Verhältnis ist hinnehmbar) und haben für den Anwendungsfall bei Astrium keine Auswirkungen. Dennoch ist ein interessantes Verhalten bei den Speichertests aufgetreten, das auf den ersten Blick nicht ohne weiteres zu erklären ist. So scheint *ein* AMD Dual-Core Prozessor im Benchmarktest performanter zu sein als wenn *zwei* Dual-Core Prozessoren eingesetzt werden. Dieses Phänomen hängt nicht direkt mit der Virtualisierung zusammen, hat aber auch Einfluss auf die Leistung, wenn diese Prozessorarchitektur an dieser Stelle verwendet wird. Hier wären weitergehende Forschungen interessant um zu klären, ob es sich um ein lokales oder ein generelles Problem handelt.
Als letzten Punkt sei noch einmal darauf hingewiesen, dass durch die Virtualisierung völlig neue Abrechnungssysteme entwickelt werden müssen. Denn es existiert nach der Virtualisierung kein physikalischer Server mehr, der Kosten durch Platz, Strom und Verwaltung verursacht. Inzwischen gibt es virtuelle Server, die nur einen Teil der Ressourcen belegen, keinen Platz im Rechenzentrum brauchen und dadurch ein ganz neues Abrechnungsverfahren benötigen. Diese Punkte wurden in der Arbeit zwar immer wieder angesprochen, konnten aber in diesem Rahmen nicht ausführlich behandelt werden. Dabei spielen noch weitere Aspekte eine Rolle, die vor allem bei Firmen zunehmend an Bedeutung gewinnen werden. Der IT Manager benötigt eine möglichst exakte Aufschlüsselung des Nutzungsverhalten der VM, um eine exakte Berechnung folgen zu lassen. Anbieter von virtuellen Webservern haben bereits Berechnungsmodelle, die sich bisher meist noch an den alten Abrechnungen von physikalischen Servern orientieren. Daher könnte ein Abrechnungssystem für virtuelle Systeme eine interessante interdisziplinäre Arbeit zwischen der Informatik und der Betriebswirtschaft sein.

Literaturverzeichnis

[Ahle 07] AHLENSTORF, ANDREAS: *InfoWeekOnline: Linux als Mehrfamilienhaus*. Website, 2007. Available online at `http://www.infoweek.ch/archive/ar_single.cfm?ar_id=18399&ar_subid=2&sid=0`; visited on September 24th 2007.

[AHN 07] AHNERT, SVEN: *Virtuelle Maschinen mit VMware und Microsoft*. Addison-Wesley Verlag, ISBN 3-8273-2374-6, 2007.

[Ahne 07] AHNERT, SVEN: *Transparente Verbindlichkeiten - Stärken und Schwächen von VMwares Infrastructure 3*. iX 9/2007, 2007.

[amd 07] *Introducing AMD Virtualization*. Website, 2007. Available online at `http://www.amd.com/us-en/Processors/ProductInformation/0,,30_118_8796_14287,00.html`; visited on September 24th 2007.

[ast 07a] *Die Geschichte der Astrium*. Website, 2007. Available online at `http://www.eads.com/1024/de/pressdb/pressdb/20070621_eads_astrium_lola.html`; visited on September 24th 2007.

[ast 07b] *EADS Astrium Satellites*. Website, 2007. Available online at `http://www.eads.com/1024/de/businet/eads_astrium/astrium_satellites.html`; visited on September 24th 2007.

[Baad 06] BAADER, HANS-JOACHIM: *Interview mit Kir (Kirill) Kolyshkin: "Weniger Overhead als Xen"*. Website, 2006. Available online at `http://www.pro-linux.de/berichte/interview-openvz.html`; visited on September 24th 2007.

[Bach 06] BACHFELD, DANIEL: *Rootkit verschiebt Windows in virtuelle Maschine*. Website, 2006. Available online at `http://www.heise.de/newsticker/meldung/79676`; visited on September 24th 2007.

[Bach 07] BACHFELD, DANIEL: *Hasch mich, ich bin ein Rootkit*. Website, 2007. Available online at `http://www.heise.de/newsticker/meldung/92176`; visited on September 24th 2007.

[Beie 06] BEIER, ANDREAS: *Realitätenkabinett - Virtualisierungsprodukte für PCs*. c't 16/2006, 2006. Available online at `http://www.heise.de/ct/06/16/064/`; visited on September 24th 2007.

[BHea 03] BERKHOUT, MICHIEL, ROY HARROW und ET AL.: *ITIL - The key to managing IT Services - Service Support*. Galileo Computing Verlag, ISBN 3-89842-822-4, 2003.

[Bote 07] BOTELHO, BRIDGET: *Blades und Virtualisierung: Kühlung, Strom und hohe Packungsdichten*. Website, 2007. Available online at `http://www.searchdatacenter.de/themenkanaele/virtualisierung/strategien/articles/69210/`; visited on September 24th 2007.

[COC 03] COCKBURN, ALISTAIR: *Use Cases effektiv erstellen*. MITP Verlag, ISBN 3-8266-1344-9, 2003.

[del 07] *Homepage von Dell*, 2007. `www.dell.com`.

[Died 07] DIEDRICH, DR. OLIVER: *VirtualBox*. Website, 2007. Available online at `http://www.heise.de/open/artikel/83678`; visited on September 24th 2007.

[Ecke 02] ECKEL, PETER: *Stille Helfer unter Beschuss*. Webseite, 2002. Available online at `http://www.heise.de/ct/02/05/046/`; visited on September 24th 2007.

[Enom 07] ENOMALISM: *Enomaly Inc.* Website, 2007. Available online at http://www.enomalism.com; visited on September 24th 2007.

[fcs 07] *Fibre Channel Industry Association (FCIA).* Webseite, 2007. Available online at www.fibrechannel.org/; visited on September 24th 2007.

[Fert 06] FERTSCH, CHRISTIAN: *XEN - Ein neuer Stern am Himmel.* Website, 2006. Available online at http://www.ordix.biz/ORDIXNews/3_2006/linux/xen_virtualisierung.html; visited on September 24th 2007.

[Fors 07] FORSTER, PETER: *Microsoft TechNet: Artikelserie: Virtualisierung - Teil 1.* Website, 2007. Available online at http://www.microsoft.com/austria/technet/articles/virtualisierung_teil1.mspx; visited on September 24th 2007.

[gho 07] *Symantec Norton Ghost 12 - Overview.* Website, 2007. Available online at http://www.symantec.com/de/de/home_homeoffice/products/overview.jsp?pcid=br&pvid=ghost12; visited on September 24th 2007.

[GKea 03] GRAUPNER, SVEN, RALF KÖNIG und ET AL.: *Impact of Virtualization on Management Systems.* Webseite, 2003. Available online at http://www.cs.ncl.ac.uk/research/pubs/trNN/papers/144.pdf; visited on September 24th 2007.

[gps 07] *GPS - Global Positioning System.* Website, 2007. Available online at www.gps.gov; visited on September 24th 2007.

[HAN 99] HEGERING, H.-G., S. ABECK und B. NEUMAIR: *Integrated Management of Networked Systems – Concepts, Architectures and their Operational Application.* Morgan Kaufmann Publishers, ISBN 1-55860-571-1, 1999. 651 p.

[HAN 99a] HEGERING, H.-G., S. ABECK und B. NEUMAIR: *Integriertes Management vernetzter Systeme — Konzepte, Architekturen und deren betrieblicher Einsatz.* dpunkt-Verlag, ISBN 3-932588-16-9, 1999, http://www.dpunkt.de/produkte/management.html . 607 S.

[Herm 07] HERMANN, LARS: *Paravirtualisierung bringt Performance.* Computer Zeitung, 2007. Available online at http://computer-zeitung.de/themen/infrastruktur/article.html?thes=9789&art=/articles/2007029/31120363_ha_CZ.html; visited on September 24th 2007.

[Hoex 06] HOEXER, HANS-JOERG: *Virtuelle Maschinen.* Website, 2006. Available online at http://www3.informatik.uni-erlangen.de/Lehre/virME/SS2006/slides1.pdf; visited on September 24th 2007.

[hph 07] *Homepage von Hewlett-Packard.* Website, 2007. Available online at www.hp.com; visited on September 24th 2007.

[Hüls 06] HÜLSENBUSCH, RALPH: *Klingen kreuzen - Blade Server fürs Rack.* iX 5/2006, 2006. pages 106-113.

[ibm 07] *IBM stellt neue Software zur Reduktion der Komplexität in Rechenzentren vor.* Webseite, 2007. Available online at http://www-05.ibm.com/de/pressroom/presseinfos/2007/06/19_2.html; visited on September 24th 2007.

[inn 07] *Homepage von VirtualBox.* Website, 2007. Available online at http://www.virtualbox.org/; visited on September 24th 2007.

[int 05] *Intel Virtualization Technology.* Website, 2005. Available online at http://www.intel.com/technology/itj/2006/v10i3/1-hardware/6-vt-x-vt-i-solutions.htm; visited on September 24th 2007.

[iSC 07] *iSCSI Technical White Paper.* Storage Networking Industry Association, 2007. Available online at http://www.snia.org/ipstorage/about/iscsi/iSCSI_Technical_whitepaper.PDF; visited on September 24th 2007.

[ITIL 02] BON, JAN VAN, GEORGES KEMMERLING und ET AL.: *IT Service Management, eine Einführung*. Van Haren Publishing, ISBN 90-806713-5-5, 2002. Seiten 91-119.

[ITIL 07] ITIL.ORG: *Das Portal für Informationen rund um ITIL und ISO20000*. Website, 2007. Available online at `http://www.itil.org/de/`; visited on September 24th 2007.

[jav 07] *Über die Java-Technologie*. Webseite, 2007. Available online at `http://www.java.com/de/about`; visited on September 24th 2007.

[Kers 05] KERSTEN, CHRISTIAN: *Blockseminar der Universität Saarbrücken: Aktuelle Hardwaretechnologien und ihr Einfluss auf die Betriebssystementwicklung, Hardware-Virtualisierung auf der IA-32*. Website, 2005. Available online at `http://hs-sonne.cs.uni-sb.de:8080/lehrstuhl/SS2005/Seminar_Aktuelle_Technologien/library/04F_-_Kersten_-_Hardware-Virtualisierung.pdf`; visited on September 24th 2007.

[KiCh 06] KING, SAMUEL T. und PETER M. CHEN: *SubVirt: Implementing malware with virtual machines*. Website, 2006. Available online at `http://www.eecs.umich.edu/Rio/papers/king06.pdf`; visited on September 24th 2007.

[Kitz 04] KITZ, ANDREAS: *Anforderungsanalyse in IT-Projekten*. Website, 2004. Available online at `http://www.projekthandbuch.de/`; visited on September 24th 2007.

[Klee 07] KLEEMANN, ULI: *Geschichte der Virtualisierung*. Website, 2007. Available online at `http://www.uli-kleemann.de/index.php?option=com_content&task=blogsection&id=0&Itemid=9`; visited on September 24th 2007.

[LAR 07] LARISCH, DIRK: *Praxisbuch - VMware Server*. Carl Hanser Verlag, ISBN 3-446-40901-7, 2007.

[LUE 07] LÜDEMANN, NICO: *Applikationsvirtualisierung mit Microsoft SoftGrid 4*. Galileo Computing, ISBN 978-3-89842-851-4, 2007. Parts available online at `http://www.galileocomputing.de/katalog/buecher/titel/gp/titelID-1347?GalileoSession=55064259A3JG38-HV4I`; visited on September 24th 2007.

[Malf 05] MALFITANO, GIOVANNI: *Definition bzw. Erklärung: WABI*. Website, 2005. Available online at `http://www.bullhost.de/w/wabi.html`; visited on September 24th 2007.

[Moor 07] MOORE, SUSAN: *Virtualization Will Drive Major Change in IT Infrastructure and Operations in the Next Three Years*. Gartner Inc. - IT research and advisory company, 2007. Available online at `http://www.gartner.com/it/page.jsp?id=505040`; visited on September 24th 2007.

[net 07a] *Homepage von NetApp FlexShare*. Website, 2007. Available online at `http://www-de.netapp.com/products/enterprise-software/storage-system-software/performance-management/flexshare.html`; visited on September 24th 2007.

[net 07b] *Veritas NetBackup - Datenblatt*. Website, 2007. Available online at `http://eval.symantec.com/mktginfo/products/Sales_Docs/Data_Protection/nbu_6_0_ent_server_dsht.pdf`; visited on September 24th 2007.

[ope 07] *Homepage von OpenVZ*. Website, 2007. Available online at `http://openvz.org/`; visited on September 24th 2007.

[pas 07] *Passmark PerformanceTest 6.0 - Overview*. Website, 2007. Available online at `http://www.passmark.com/products/pt.htm`; visited on September 24th 2007.

[pcw 07] *PC-Welt Wiki: Grundlagen der Virtualisierung*. Website, 2007. Available online at `http://pcwelt-wiki.de/wiki/Virtualisierung`; visited on September 24th 2007.

[PoGo 74] POPEK, GERALD J. und ROBERT P. GOLDBERG: *Formal requirements for virtualizable third generation architectures*. Communications of the ACM, Volume17, Issue 7, 1974. Available online at `http://portal.acm.org/citation.cfm?doid=361011.361073`; visited on September 24th 2007.

[pow 07] *Platespin Powerconvert*. Website, 2007. Available online at `http://www.platespin.com/products/powerconvert`; visited on September 24th 2007.

[pri 07] *Homepage von Microsoft Print Migrator 3.1*. Website, 2007. Available online at `http://www.microsoft.com/WindowsServer2003/techinfo/overview/printmigrator3.1.mspx`; visited on SSeptember 24th 2007.

[Pull 06] PULLEN, MARCUS: *Anwendungsvirtualisierung... und deren Auswirkung auf die Kosten*. Website - HP IT Symposium 2006, 2006. PDF available online at `https://www.decus.de/slides/sy2006/16_05/1D03.pdf`; visited on September 24th 2007.

[put 07] *Homepage von PuTTY: A Free Telnet/SSH Client*. Website, 2007. Available online at `http://www.chiark.greenend.org.uk/~sgtatham/putty/`; visited on September 24th 2007.

[Rado 06] RADONIC, ANDREJ: *Xen 3 wird zur VMware-Alternative*. TecChannel Webseite, 2006. Available online at `http://testberichte-tecchannel-afp.2a.premium-link.net/server/virtualisierung/434326/`; visited on September 24th 2007.

[ref 06] *Sicherheit in virtuellen Umgebungen*. Website, 2006. Available online at `http://www.reflex-security.de/White%20Paper%20VSA%20-%20Deutsch.pdf`; visited on September 24th 2007.

[Rode 07] RODERER, ULRICH: *Sicherheitsaspekte der Virtualisierung*. Website, 2007. Available online at `http://www.searchdatacenter.de/themenkanaele/virtualisierung/management/articles/68450/`; visited on September 24th 2007.

[Sage 06] SAGER, FLORIAN: *Konzeptentwicklung für Confguration Management in einem Rechenzentrum nach ITIL und MOF*. Diplomarbeit am Institut der Informatik der TU München, 2006. Available online at `http://www.agitos.de/pub/ITIL-MOF-Configuration-Management.pdf`; visited on September 24th 2007.

[Schm 06] SCHMITT, KATHRIN: *Blades kommen (noch) ohne Standards aus*. Website, 2006. Available online at `http://www.silicon.de/enid/client_server_host/16842`; visited on September 24th 2007.

[Schm 07] SCHMITZ, DR. WILFRIED: *Virtualisierung erfordert neue Konzepte in der IT-Sicherheit*. Website, 2007. Available online at `http://www.securitymanager.de/magazin/artikel_1400_virtualisierung_erfordert_it-sicherheit.html`; visited on September 24th 2007.

[Seeg 06] SEEGER, JÜRGEN: *VMware kommt auf Macs ...* Website, 2006. Available online at `http://www.golem.de/0611/48843.html`; visited on September 24th 2007.

[Seeg 07] SEEGER, JÜRGEN: *VMware Fusion freigegeben*. Website, 2007. Available online at `http://www.heise.de/newsticker/meldung/93909/from/rss09`; visited on September 24th 2007.

[Sier 06] SIERING, PETER: *Microsoft gibt Virtual Server kostenlos ab*. Website, 2006. Available online at `http://www.heise.de/newsticker/meldung/71583`; visited on September 24th 2007.

[Sing 06] SINGH, AMIT: *An Introduction to Virtualization*. Website, 2006. Available online at `http://www.kernelthread.com/publications/virtualization/`; visited on September 24th 2007.

[ska 07] *Homepage von UML - SKAS Mode,*. Webseite, 2007. Only available online via Google Cache: `http://user-mode-linux.sourceforge.net/skas.html`; visited on September 24th 2007.

[Soll 02] SOLLBACH, WOLFGANG: *Storage Area Networks / Network Attached Storage*. Addison-Wesley Verlag, ISBN 3-8273-1871-8, 2002.

[Stie 06] STIEBERT, JULIUS: *Virtual Iron 3.0 - Virtualisierungslösung in neuer Version*. Website, 2006. Available online at `http://www.golem.de/0610/48286.html`; visited on September 24th 2007.

[SWso 07] SWSOFT: *Betriebssystemvirtualisierung*. Website, 2007. Available online at `http://www.swsoft.com/de/products/virtuozzo/os/`; visited on September 24th 2007.

[sys 01] *How to Use Sysprep: An Introduction*. Website, 2001. Available online at `http://technet.microsoft.com/en-us/library/bb457073.aspx`; visited on September 24th 2007.

[sys 03] *SYSmark 2004 White Paper*. Website, 2003. Available online at `http://www.bapco.com/techdocs/SYSmark2004WhitePaper.pdf`; visited on September 24th 2007.

[TrEr 03] TROPPENS, ULF und RAINER ERKENS: *Speichernetze*. dpunkt.verlag GmbH, ISBN 3-89864-135-X, 2003.

[uml 07] *Homepage von The User-mode Linux Kernel*. Webseite, 2007. Available online at `http://user-mode-linux.sourceforge.net/`; visited on September 24th 2007.

[Vils 05a] VILSBECK, CHRISTIAN: *AMD Pacifica: Virtualisierung von CPU & Speicher*. Website, 2005. Available online at `http://www.tecchannel.de/server/virtualisierung/432777/index1.html`; visited on September 24th 2007.

[Vils 05b] VILSBECK, CHRISTIAN: *Intels Vanderpool virtualisiert CPUs*. Website, 2005. Available online at `http://www.tecchannel.de/server/virtualisierung/402566/index1.html`; visited on September 24th 2007.

[vm0 06] *VMware Infrastructure 3 - Datenblatt*, 2006.

[vmh 07] *Homepage von VMware Inc.* Website, 2007. Available online at `www.vmware.com`; visited on September 24th 2007.

[Wiki 06] WIKIPEDIA: *Die freie Enzyklopädie*. Website, 2006. Available online at `http://de.wikipedia.org/`; visited on September 24th 2007.

[Win 07a] *Homepage von WINE*. Website, 2007. Available online at `http://www.winehq.org`; visited on September 24th 2007.

[win 07b] *Homepage von WinSCP: Free SFTP, FTP and SCP client for Windows*. Website, 2007. Available online at `http://winscp.net/eng/docs/lang:de`; visited on September 24th 2007.

[XEN 06] RADONIC, ANDREJ und FRANK MEYER: *XEN3*. Franzis Verlag GmbH, ISBN 3-7723-7899-4, 2006.

[XEN 07] SPRANG, HENNING, TIMO BENK, JAROSLAW ZDRZALEK und RALPH DEHNER: *XEN - Virtualisierung unter Linux*. Open Source Press, ISBN 978-9-937514-29-1, 2007.

[xen 07a] *Convirt - Controlling Virtual Systems*. Website, 2007. Available online at `http://xenman.sourceforge.net/`; visited on September 24th 2007.

[xen 07b] *Homepage von XenSource Inc.* Website, 2007. Available online at `http://www.xensource.com`; visited on September 24th 2007.

[Zieg 07] ZIEGLER, PETER-MICHAEL: *VMware legt Raketenstart an der Börse hin*. Website, 2007. Available online at `http://www.heise.de/newsticker/meldung/94421`; visited on September 24th 2007.

[ZIM 06] ZIMMER, DENNIS: *VMware Server und VMware Player*. Galileo Computing Verlag, ISBN 3-89842-822-4, 2006.

[Zimm 06] ZIMMER, DENNIS: *Professionelle Virtualisierungsprodukte: Ein Überblick*. iX 5/2006, 2006. pages 64-81.