



Diplomarbeit

**Managementkonzept für virtuelle
Infrastrukturen unter besonderer
Berücksichtigung unterschiedlicher
Nutzeranforderungen**

Mathias Gehrung



Diplomarbeit

Managementkonzept für virtuelle Infrastrukturen unter besonderer Berücksichtigung unterschiedlicher Nutzeranforderungen

Mathias Gehrung

Aufgabensteller: Prof. Dr. Heinz-Gerd Hegering

Betreuer: Silvia Knittl
Tobias Lindinger
Patricia Marcu
Dr. Fritz Schinkel (FSC)

Abgabetermin: 10. Februar 2009

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

München, den 10. Februar 2009

.....
(*Unterschrift des Kandidaten*)

Kurzbeschreibung

In modernen IT-Infrastrukturen findet aus vielfältigen Gründen immer häufiger die Technik der Virtualisierung Einsatz. Durch die Virtualisierung entsteht jedoch in einer IT-Infrastruktur ein neuer zu verwaltender Aspekt. Die Virtualisierung selbst muss ebenso verwaltet werden wie die bisher existierenden Teile der Infrastruktur.

Diese Arbeit befasst sich damit, wie einem Administrator eines solchen virtuellen Systems das Management angeboten werden kann. Einer der zentralen Punkte ist dabei, dass die im speziellen Fall verwendete Technologie für die Virtualisierung nicht entscheidend sein soll. Der Benutzer soll also z.B nichts über die verwendete Server-Virtualisierung und ihre Details, die bei einer anderen Technologie ganz andere wären, erfahren, sondern soll mit einem generischen Modell arbeiten, das unabhängig von den verwendeten Virtualisierungstechniken ist. Ein anderer wichtiger Punkt, der in dieser Arbeit behandelt wird, ist wie man Administratoren mit unterschiedlichem Wissensstand und Anforderungen jeweils das Management in angemessener Form anbieten kann.

Inhaltsverzeichnis

1	Einführung	1
1.1	Motivation	1
1.1.1	Definition des Modell-Begriffs	2
1.2	Grundlagen	3
1.2.1	Virtualisierung	3
1.3	Vorgehen und Gliederung der Arbeit	7
1.4	Zusammenfassung	8
2	Existierende Modelle	9
2.1	PAN	9
2.1.1	Voraussetzungen	9
2.1.2	Struktur	11
2.1.3	Oberfläche	13
2.2	VMware	16
2.2.1	Voraussetzungen	16
2.2.2	Struktur	17
2.2.3	Oberfläche	19
2.3	Virtual Iron	19
2.3.1	Voraussetzungen	19
2.3.2	Struktur	21
2.3.3	Oberfläche	22
2.4	VIOM	24
2.4.1	Voraussetzungen	25
2.4.2	Struktur	25
2.4.3	Oberfläche	26
2.5	Zusammenfassung	28
3	Szenarien und Anforderungen	29
3.1	Beschreibung der Szenarien	29
3.1.1	Szenario 1a	29
3.1.2	Szenario 1b	30
3.1.3	Szenario 2a	32
3.1.4	Szenario 2b	33
3.1.5	Charakterisierung der Szenarien	34
3.2	Anforderungen	34
3.2.1	Aufstellung der Anforderungen	35
3.2.2	Funktionale Anforderungen	36
3.2.3	Nichtfunktionale Anforderungen	40
3.3	Zusammenfassung	42

4	Umsetzung der Szenarien in den Modellen	43
4.1	Szenario 1a	44
4.1.1	Ohne Virtualisierung	44
4.1.2	PAN	47
4.1.3	VMware	50
4.1.4	Virtual Iron	53
4.1.5	VIOM	56
4.1.6	Bewertung für das Szenario 1a	59
4.2	Szenario 1b	59
4.2.1	Ohne Virtualisierung	60
4.2.2	PAN	62
4.2.3	VMware	66
4.2.4	Virtual Iron	70
4.2.5	VIOM	72
4.2.6	Bewertung für das Szenario 1b	74
4.3	Szenario 2a	75
4.3.1	Ohne Virtualisierung	75
4.3.2	PAN	77
4.3.3	VMware	80
4.3.4	Virtual Iron	83
4.3.5	VIOM	85
4.3.6	Bewertung für das Szenario 2a	88
4.4	Szenario 2b	88
4.4.1	Ohne Virtualisierung	88
4.4.2	PAN	91
4.4.3	VMware	94
4.4.4	Virtual Iron	97
4.4.5	VIOM	100
4.4.6	Bewertung für das Szenario 2b	102
4.5	Bewertung der Modelle	103
4.5.1	Ohne Virtualisierung	103
4.5.2	PAN	103
4.5.3	VMware	104
4.5.4	Virtual Iron	104
4.5.5	VIOM	105
4.6	Zusammenfassung	105
5	Entwurf des neuen Modells	107
5.1	Anforderungen	107
5.2	Anbindung an die Management-Plattform	108
5.2.1	Rollen und Rechte	109
5.3	Benutzermodi	109
5.3.1	Der einfache Modus	109
5.3.2	Der komplexe Modus	111
5.3.3	Rollen der Nutzer	111
5.4	Informationsmodell	111

5.5	Managementmodell	112
5.5.1	Objekte des einfachen Modus	113
5.5.2	Objekte des komplexen Modus	113
5.6	Management-Grenzen des Modells	114
5.7	Automationen des Virtualisierungs-Management-Modell	115
5.7.1	Erstellen von virtuellen Maschinen aus Vorlagen	116
5.7.2	Konfiguration von virtuellen Netzen	116
5.7.3	Erstellung von zeitlich gesteuerten Aufgaben	116
5.7.4	Vereinfachung von Meldungen an den Nutzer und Reaktion auf Ereignisse	116
5.7.5	Weitere Automationen	117
5.8	Ansichten	117
5.8.1	Infrastruktur-Ansicht	118
5.8.2	Server-Ansicht	119
5.8.3	Netz-Ansicht	122
5.8.4	Ressourcen-Ansicht	123
5.8.5	Nutzer-Ansicht	124
5.8.6	Modell der Ansichten	126
5.9	Erfüllung der Anforderungen	126
5.10	Zusammenfassung	127
6	Zusammenfassung und Ausblick	129
6.1	Zusammenfassung	129
6.2	Ausblick	130
	Abbildungsverzeichnis	131
	Literaturverzeichnis	133
	Index	137
	Glossar	139

1 Einführung

Diese Arbeit entsteht im Rahmen einer Kooperation der Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung des Instituts für Informatik der LMU, Fujitsu-Siemens Computer und des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften.

Zu Beginn der Arbeit war im Titel der Arbeit der Begriff *Managementkonzept* vorhanden. Im Laufe der Arbeit hat sich anstelle des Begriffs Managementkonzept der Begriff des Modells durchgesetzt, wodurch in dieser Arbeit der Begriff *Modell* verwendet wird.

Zunächst wird in diesem Kapitel die Motivation und die Notwendigkeit für die Erstellung dieser Arbeit begründet. Im Anschluss daran wird in Abschnitt 1.2 auf die nötigen Grundlagen eingegangen. Darunter fallen Grundlagen über Virtualisierung in den in der Diplomarbeit benutzten Bereichen, sowie weitere Begriffserklärungen. Daraufhin wird der Aufbau dieser Ausarbeitung erläutert. Für nicht im Text selbst beschriebene Begriffe ist am Ende der Ausarbeitung ein Glossar vorhanden.

Im Verlauf der Arbeit wurden offene Gespräche mit Mitarbeitern der beteiligten Organisationen geführt, die zum Gelingen der Arbeit einen wichtigen Beitrag leisteten. Diese Personen waren Herr Rothe, Frau Lamers und Herr Berner (alle FSC) mit Unterstützung durch Fachwissen im Bereich PAN und VIOM. Weiterhin haben Herr Güven und Herr Widmer (ebenfalls FSC) durch die Weitergabe ihrer Erfahrungen für Ideen für diese Arbeit gesorgt. Die Herren Roll und Biardzki (beide LRZ) boten mit ihrem Wissen über VMware eine Quelle wichtiger Informationen.

1.1 Motivation

Mit der Verbreitung der Virtualisierung auf der x86 Plattform stehen heutigen IT-Infrastrukturen, die diese Rechnerarchitektur verwenden, viele Möglichkeiten, z.B. zur Senkung von Kosten oder der Verbesserung der Qualität der angebotenen Dienste, zur Verfügung. So können auf der Hardware eines Servers parallel nebeneinander mehrere Instanzen eines oder mehrerer unterschiedlicher Betriebssysteme betrieben werden, in denen einzelne Dienste angeboten werden. Ohne Virtualisierung wäre es unter Umständen nötig, alle Dienste in einer einzigen Instanz des Betriebssystems oder aber für jede einzelne Instanz einen Hardware-Server zu betreiben. Der Betrieb in nur einer Betriebssystem-Instanz könnte aus sicherheitsrelevanten Gründen nicht gewünscht oder möglich sein. So lassen sich durch den Betrieb nur eines Hardware-Servers Kosten für Anschaffung, Wartung und Betrieb verringern. Ein weiterer damit zusammenhängender Effekt ist die damit verbundene Platz- und Energie-Einsparung.

Durch die Virtualisierung kommt im Management solcher Infrastrukturen eine neue zu verwaltende Schicht hinzu. Je nach Architektur der Implementierungen der eingesetzten Virtualisierungslösung gibt es unterschiedliche Elemente, die durch das Management abgedeckt werden müssen. Das in dieser Arbeit entwickelte Modell setzt auf eine Management-

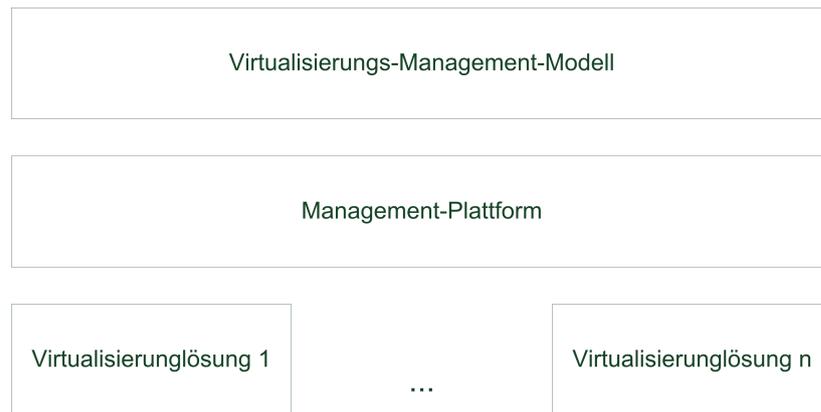


Abbildung 1.1: Einordnung der Aufgabenstellung

Plattform auf, die in der Lage ist, verschiedene Virtualisierungslösungen zu verwalten. Diese Plattform legt das „technische“ Modell einer Management-Architektur mit seinen Teilmodellen Informationsmodell, Funktionsmodell, Organisationsmodell und Kommunikationsmodell (für eine genaue Definition dieser Begriffe siehe [HAN99, S.119 ff]) fest. Das Modell aus dieser Arbeit eine Abstraktionsschicht höher angesiedelt ist und beschreibt, wie Nutzern das Management einer virtuellen Infrastruktur präsentiert werden kann. In dem in der Informatik gebräuchlichen Schichtenmodell ist die Management-Plattform eine untere Schicht, während das Modell dieser Arbeit die obere Schicht darstellt (siehe Abbildung 1.1). Der Frage, wie Virtualisierung in das bestehende Management eingebunden werden kann ging Florian Bittner in seiner Diplomarbeit [Bit08] nach. Die Management-Plattform Bittners kann als ein mögliches Fundament für diese Arbeit verstanden werden, auch wenn bei den Aufgabenstellungen der beiden Arbeiten ein direkter Bezug nicht angedacht war. Für die vorliegende Aufgabenstellung wird das Ergebnis von Florian Bittner nicht als Grundlage vorausgesetzt.

In dieser Arbeit wird weiterhin untersucht, wie bereits existierende Virtualisierungs-Produkte ihren Nutzern Managementinformationen und -möglichkeiten anbieten. Dazu werden die Managementmodelle ausgewählter Virtualisierungslösungen anhand von Szenarien miteinander verglichen. Das Ziel dieser Ausarbeitung ist dann die Erstellung eines generischen Modells, das es möglich machen soll, Nutzer mit unterschiedlicher Qualifikation, die auch unterschiedliche Anforderungen an die Administration stellen, jeweils das Management anzubieten, das sie brauchen. Dabei soll die eingesetzte Technik zur Virtualisierung für den Nutzer keine Bedeutung haben. Es wird darin definiert welche Objekte es darin gibt, welche Möglichkeiten diese Objekte bieten, welche Objekte in Beziehung stehen und wer darauf Zugriff hat. Um das Thema dabei etwas einzuschränken, wird der Schwerpunkt der Betrachtung auf Netze gelegt. Die anderen Teile der Infrastrukturen werden ebenfalls betrachtet, jedoch mit geringerer Tiefe.

1.1.1 Definition des Modell-Begriffs

Der bisher verwendete Begriff „Modell“ ist sehr unspezifisch, deshalb wird an dieser Stelle der Begriff des *Virtualisierungs-Management-Modells* eingeführt. Dieser Begriff bezeichnet ein abstraktes Modell, das Objekte, die Gegenstand des Managements sind, definiert und für Nutzer des Modells den Zugriff auf diese Objekte steuert. Die Objekte beinhalten jeweils

Informationen, die für das Management relevant sind und bieten in der Regel Aktionen an. Weiterhin muss ein Nutzerkonzept in dem Modell enthalten sein, das es ermöglicht unterschiedlichen Nutzern unterschiedliche Rechte für die Sichtbarkeit und die möglichen Aktionen einzuräumen. Dabei liegt der Fokus auf dem Einsatz mit Virtualisierungsprodukten.

Das Virtualisierungs-Management-Modell stellt aber nur ein abstraktes Nutzungskonzept dar, das dann z.B. in der Umsetzung einer Nutzerschnittstelle Anwendung findet.

1.2 Grundlagen

An dieser Stelle werden Grundlagen der Virtualisierung erklärt, die im Verlauf der Arbeit benutzt werden.

1.2.1 Virtualisierung

In der Informationstechnik werden verschiedene Arten der Virtualisierung unterschieden, die jeweils in unterschiedlichen Bereichen Anwendung finden. Virtualisierung ist in der Informatik ein altbekanntes Konzept, das in unterschiedlichen Bereichen schon lange eingesetzt wird (z.B. virtuelle Speicheradressierung, bei der von einer virtuellen Speicheradresse auf eine physikalische Adresse abgebildet wird). An dieser Stelle sollen nur die Arten der Virtualisierung beschrieben werden, die für das Thema der Arbeit interessant sind. Ein Bereich, der für diese Arbeit fundamental wichtig ist, ist die *Plattform-Virtualisierung*, bei der bei einem Rechner eine Abstraktionsschicht eingefügt wird, die es ermöglicht die Hardware zu virtualisieren und so mehrere logische Rechner auf einer Plattform zu betreiben. Dadurch wird eine Trennung der Hardware von dem eingesetzten Betriebssystem erreicht. Bei der Plattform-Virtualisierung gibt es einige unterschiedliche Ansätze, auf die weiter unten eingegangen wird.

Eine andere Art der in dieser Arbeit wichtigen Virtualisierung ist die *Netz-Virtualisierung*, bei der es darum geht, physisch existierende Netze zu virtualisieren. Das heißt es werden durch die Virtualisierung logische Netze auf physischen Netzen erstellt.

Die *Desktopvirtualisierung* wird eingesetzt, um das Management der Desktops zu vereinfachen. Es können dabei auch Kosten gespart werden, da statt vollwertiger PCs an den Arbeitsplätzen nur Thin-Clients benötigt werden.

Bei der *Storage-Virtualisierung* werden die verwendeten Speichersysteme vor dem Nutzer verborgen. Das hat den Vorteil, dass Systeme auf einheitliche Weise auf die Storage zugreifen können, ungeachtet der verwendeten Technologie.

Plattform-Virtualisierung

Nun werden die verschiedenen Ansätze die es gibt, um die Plattform-Virtualisierung durchzuführen, kurz erläutert. Ein Konzept, das dabei verwendet wird, ist das der Verwendung eines Hypervisors der auch Virtual Machine Monitor (VMM)[Rad06] genannt wird. In der Literatur gibt es unterschiedliche Bedeutungen dieser beiden Begriffe, abhängig vom „Ort“ der Ausführung, womit gemeint ist, auf welcher Ebene der Hypervisor ausgeführt wird. Er kann entweder direkt auf der Hardware oder aber innerhalb eines Betriebssystems ausgeführt werden. Um wieder eine einheitliche Nomenklatur zu erlangen, kann eine andere Definition verwendet werden, wobei dann mit dem Begriff *Typ-1 Hypervisor* ein Hypervisor gemeint ist,

der direkt auf der Hardware des zu virtualisierenden Systems ausgeführt wird. Die Gastssysteme benutzen dann direkt die Hardwareressourcen, die vom Hypervisor verwaltet werden. Als *Typ-2 Hypervisor* wird ein Hypervisor bezeichnet, der innerhalb eines Betriebssystems ausgeführt wird und der den Gastsystemen dann die vorhandenen Ressourcen über das Betriebssystem bereit stellt. Diese Definitionen und auch die folgenden Beschreibungen der Virtualisierungsansätze für die Plattform-Virtualisierung sind auch in [Rad06] zu finden.

Der Hypervisor ist, unabhängig der oberen Definition, eine Softwareschicht, die die Zuteilung vorhandener Ressourcen an Gastssysteme übernimmt. Somit ist er eine zentrale Komponente in der Plattform-Virtualisierung, dem die grundlegende Verwaltung der Ressourcen und der Gastssysteme obliegt.

Vollständige Virtualisierung Bei diesem Ansatz wird so viel Hardware eines Computers simuliert, um einem Gastsystem eine Umgebung aus virtuellen Ressourcen zu bieten, die für den Betrieb ausreicht. Dadurch können unmodifizierte Betriebssysteme auf der simulierten Hardware laufen, vor denen verborgen bleibt, dass sie virtualisiert sind. Das Gast-Betriebssystem kennt dabei nur seine simulierte Hardwareumgebung, die es als physikalische Umgebung annimmt. Durch das Simulieren der Systemressourcen und den zusätzlichen Schritt bei der Bearbeitung von Aufrufen an diese Ressourcen sowie bei der Verarbeitung ihrer Antworten entsteht ein Overhead durch den die Performanz der Virtualisierung verschlechtert wird.

Hiervon abzugrenzen ist die Emulation, die auch vollkommen innerhalb eines Betriebssystems stattfindet. Jedoch werden bei der Emulation die gesamten Ressourcen eines Rechners emuliert. Systemaufrufe eines Gastbetriebssystems werden durch den Emulator verarbeitet, das bedeutet, der Emulator führt emulierte Systemaufrufe durch. Erst wenn diese komplett durch den Emulator ausgeführt wurden, gibt der Emulator die Systemaufrufe an das Host-Betriebssystem weiter, das sie dann weiter verarbeitet. Dagegen werden Aufrufe an virtualisierte Ressourcen bei der vollständigen Virtualisierung so früh wie möglich an das Betriebssystem übergeben, das sie weiter verarbeitet und an die Hardware übergibt. Die Emulation erzeugt durch die komplette Verarbeitung der Aufrufe einen größeren Overhead als die vollständige Virtualisierung und ist dadurch weniger performant.

Hardware unterstützte Virtualisierung Bei diesem Ansatz wird die Fähigkeit moderner Prozessoren zur Virtualisierung benutzt. Diese Fähigkeit wird durch einen Befehlssatz im Prozessor realisiert, der für die Verwaltung von Virtuellen Maschinen auf der Ebene des Prozessors gedacht ist. Durch Einsatz eines Hypervisors, der in diesem Fall direkt auf der Maschine läuft, können Virtuelle Maschinen ohne Modifikation durch den Hypervisor gesteuert betrieben werden. Da nur noch der Hypervisor auf der Maschine läuft und die Virtualisierung durch die Prozessoren unterstützt wird, besteht hier nur ein geringer Overhead, was sich positiv auf die Performanz des Systems auswirkt. Die Hardwareunterstützung ist in modernen x86-Prozessoren der Firmen Intel und AMD inzwischen weit verbreitet. Intel verwendet die Bezeichnung VT (Virtualization Technology) und den Codenamen „Vanderpool“, während AMD seine Prozessoren mit diesen Fähigkeiten mit dem Codenamen „Pacifica“ versehen hat [Lin06, S. 19ff].

Paravirtualisierung Bei diesem Ansatz können nur modifizierte Betriebssysteme verwendet werden, die ihre Systemaufrufe nicht direkt an die Hardware absetzen, sondern eine festgelegte API (Application Programming Interface) verwenden, die so genannte Hypercalls

verwenden, die vom Hypervisor des Systems verarbeitet werden. Der Hypervisor ist für die Systemaufrufe und die Weiterleitung der Antworten an das entsprechende Gastsystem verantwortlich. Da auch bei diesem Virtualisierungsansatz der Hypervisor direkt auf der Hardware läuft, entsteht ein vergleichsweise geringer Overhead durch die Virtualisierung, der sich z.B. im Vergleich mit der vollständigen Virtualisierung nur gering auf die Performanz auswirkt. Jedoch ist die Verwendung von modifizierten Betriebssystemen in der Regel insofern ein Problem, als es sich um proprietäre Systeme mit geschlossenem Source-Code handelt, da die jeweiligen Anbieter meist keine angepassten Versionen veröffentlichen. Dadurch bleibt in der Praxis hauptsächlich die Verwendung von Open-Source Betriebssystemen.

Betriebssystem-Virtualisierung Bei der Betriebssystem-Virtualisierung erzeugt ein spezielles Host-Betriebssystem mehrere Instanzen seiner selbst. Jede außer der ursprünglichen Instanz ist eine virtuelle Maschine. Jedoch haben diese virtuellen Maschinen immer dasselbe Betriebssystem in exakt derselben Version. Eine Anpassung des Betriebssystems selbst ist nicht möglich. Da alle Systeme mit demselben Betriebssystem laufen, kann das System sehr schlank gehalten werden, denn Software-Ressourcen, die von allen laufenden Betriebssystemen benötigt werden, müssen nur einmal im Speicher vorhanden sein. Das Host-Betriebssystem ersetzt in diesem Fall den Hypervisor, denn es übernimmt die Steuerung der Gastsysteme und verwaltet deren Systemaufrufe. Dieser Virtualisierungsansatz produziert dadurch einen sehr geringen Overhead, der sich nur marginal auf die Performanz auswirkt.

Netz-Virtualisierung

Es gibt auch Ansätze Netze zu virtualisieren. Ebenso wie bei der Plattform-Virtualisierung vorhandene Hardware benutzt wird, um virtuelle Systeme darauf laufen zu lassen, werden bei virtuellen Netzen physisch vorhandene Netze dazu benutzt, um logische Unterteilungen darauf vorzunehmen.

VLAN Bei der Bildung virtueller LANs (VLANs) werden logische Unterteilungen eines physisch existierenden LANs vorgenommen. VLANs können in portbasierte und Tagged-VLANs unterteilt werden. Bei portbasierten VLANs werden Ports eines Switches einem VLAN zugeteilt. Rechner, die über Ports eines VLANs verbunden sind, sind automatisch Mitglieder dieses VLANs. In dieser Arbeit werden nur Tagged-VLANs (auch dynamische VLANs genannt) benutzt. Für die Realisierung von getaggten (markierten) VLANs gibt es unterschiedliche, meist proprietäre Protokolle. An dieser Stelle wird jedoch der IEEE 802.1Q[The06] Standard verwendet, mit dem Tagged-VLANs gebildet werden können. Bei Verwendung von 802.1Q werden die Pakete auf Schicht zwei des OSI-Modells markiert. Dabei wird ein weiteres Feld (Tag, Markierung) in den Header eingefügt, das von den VLAN-fähigen Switches ausgewertet wird, um es dann nur an die anderen Teile eines VLAN weiterzuleiten. Ein VLAN stellt somit eine eigene Broadcast Domäne dar. Die Tags werden nicht von den Rechnern eines VLAN vergeben, sondern von dem ersten mit dem Paket in Verbindung kommenden VLAN fähigen Switch. Der letzte VLAN fähige Switch auf dem Weg des Pakets zu seinem Ziel entfernt das Tag dann wieder. Die Zuteilung der Rechner zu VLANs passiert auf der Grundlage der MAC-Adressen der Netzwerkadapter. Weitere Informationen zu VLAN und 802.1Q können in [Tan03] nachgelesen werden.

VPN Virtual Private Networks (VPNs) sind virtuelle private Netze. Das bedeutet, dass auf öffentlichen Netzen logische private Teilnetze erstellt werden. Häufig wird dieses Vorgehen verwendet, wenn zwei private Netze verbunden werden sollen, es aber keine praktikable private Verbindungsmöglichkeit, aber dafür ein öffentliches Netz, wie das Internet, als Verbindungsmöglichkeit gibt. Der Unterschied zu den oben erwähnten VLANs liegt darin, dass ein VLAN in der Regel innerhalb eines privaten Netzes eingerichtet wird. Die Errichtung eines VLAN über ein öffentliches Netz hinweg, das möglicherweise von unterschiedlichen Organisationen betrieben wird, ist wenig realistisch, da auf allen entsprechenden Switches (bei Verwendung von 802.1Q wie oben beschrieben) das VLAN eingerichtet werden muss. In einem solchen Fall bietet sich die Verwendung eines VPNs an. Es gibt verschiedene Protokolle mit denen VPNs realisiert werden können. Diese Protokolle arbeiten auf unterschiedlichen Schichten des OSI-Referenzmodells. Häufig verwendete Protokolle sind:

- PPTP (Point-toPoint Tunneling Protocol)/L2TP (Layer 2 Tunneling Protocol)
- TSL (Transport Layer Security)/SSL (Secure Socket Layer)
- IPSec (Internet Protocol Security)
- MPLS (Multi Protocol Label Switching)

Diese Protokolle werden hier nicht näher erklärt, da sie für die vorliegende Arbeit nicht benötigt werden. Weiterführende Informationen sind aber in [Tan03, KR08, Lin06] zu finden.

Desktopvirtualisierung

Die Desktopvirtualisierung verlagert den Ort an dem ein Desktop gespeichert ist von einem PC am Arbeitsplatz des Nutzers auf zentrale Server. Der Nutzer kann wie gewohnt an seinem Arbeitsplatz sitzen und beispielsweise an einem Thin-Client arbeiten, so als ob der Desktop nicht virtualisiert und auf seinem PC gespeichert wäre. Dabei greift der Nutzer über ein Remote-Desktop-Protokoll wie z.B. RDP (Remote Desktop Protocol) auf seinen Desktop, der nun auf einem Server ausgeführt wird, zu. Zunächst gibt es mehrere Möglichkeiten, Desktops für User anzubieten. Es ist möglich, jedem Nutzer denselben Desktop bereitzustellen, ohne dass dieser verändert werden kann. Dabei müssen alle Anwendungen, die von irgendeinem Nutzer benötigt werden, vorhanden sein. Eine andere Möglichkeit ist es den Nutzern einen individuellen Desktop anzubieten, den sie selbst anpassen können. Je nach eingesetzter Technik können dann unterschiedlichen Nutzern oder Nutzergruppen auch unterschiedliche Mengen von Anwendungen bereitgestellt werden. Die Virtualisierung der Desktops bringt unter anderem folgende Vorteile:

- Schnelles Bereitstellen neuer Desktops für neue Nutzer
- Einfache Bereitstellung neuer Software oder von Updates
- Vereinfachtes Management der Desktops
- Erleichterung für User-Helpdesk

Storage-Virtualisierung

Laut [TLM06, Seite 150f] gibt es drei Ebenen auf denen Storage-Virtualisierung durchgeführt werden kann. Auf Server-Ebene, auf der Ebene des Stagesystems und auf Ebene des Netzes. Der folgende Absatz bezieht sich auf die Virtualisierung des Speichers auf der Netzebene. Durch die Storage-Virtualisierung werden die einzelnen Speichersysteme eines Speichernetzes zusammengefasst. Dadurch scheint der gesamte von den Speichersystemen angebotene Speicherplatz von nur einem System angeboten zu werden. Es gibt zwei Ansätze, bei denen die Virtualisierung in unterschiedlichen Komponenten durchgeführt wird. Bei der *In-Band-Virtualisierung* werden die Steuerdaten für die Virtualisierung im gleichen Datenpfad transportiert wie die Nutzdaten. Dabei wird die Virtualisierung auf der Hard- und Software im Datenpfad durchgeführt. Die *Out-Band-Virtualisierung* dagegen verlagert den Fluss der Steuerdaten weg vom Datenpfad. Die Virtualisierung findet hierbei in einem speziellen Server statt. Weitere und detailliertere Informationen sind in [Tat04], [Rob01] und [Lar07] zu finden.

1.3 Vorgehen und Gliederung der Arbeit

Für die Erstellung des generischen Virtualisierungs-Management-Modells, das in Abschnitt 1.1.1 beschrieben wurde, ist es im ersten Schritt sinnvoll einen Eindruck davon zu erhalten, wie die Managementmodelle bereits existierender Virtualisierungslösungen aufgebaut sind. Um einen Eindruck davon zu gewinnen werden die Managementmodelle der Virtualisierungstechniken, die in dieser Arbeit überprüft werden, in Kapitel 2 betrachtet. Es soll festgestellt werden, welche Daten und Aktionen einem Nutzer der Virtualisierungslösung, genauer gesagt, des Virtualisierungs-Management-Modells, angeboten werden. Dazu werden die einzelnen Produkte untersucht und es wird beschrieben, welche Informationen und Aktionen dem Nutzer zu welcher Zeit an welcher Stelle angeboten werden. Obwohl in den meisten Fällen die verwendeten Virtualisierungs-Management-Modelle die Technik oder Architektur der Virtualisierungslösung in gewissem Maße widerspiegeln, soll das in dieser Arbeit wenig Bedeutung finden. Da das zu erstellende Modell unabhängig von konkret verwendeten Technologien sein soll.

Der nächste Teil dieser Ausarbeitung ist die Beschreibung der Szenarien in Kapitel 3, die verwendet werden um einen Test der zu untersuchenden Virtualisierungslösungen durchzuführen. Es werden vier Szenarien ausgearbeitet und beschrieben, die unterschiedliche Anforderungen an die Virtualisierung stellen. So sollen z.B. die Größen der betrachteten Umgebungen oder die erwünschte Dynamik unterschiedlich sein, damit ein großes Spektrum an Einsatzgebieten abgedeckt wird. Im Anschluss an die Szenarien werden die Anforderungen an das Virtualisierungs-Management-Modell abgeleitet. Diese ergeben sich teils aus der Aufgabenstellung, teils aus den Szenarien.

Im Anschluss an die Definition der Szenarien wird in Kapitel 4 beschrieben, wie die Szenarien mit den zuvor beschriebenen Virtualisierungslösungen umsetzbar sind. Es wird jedes Szenario mit jeder bestehenden Technologie umgesetzt. Dadurch können die existierenden Managementmodelle danach bewertet werden, welche ihrer Konzepte auch für das zu erstellende Modell brauchbar sein können oder an welchen Stellen sie nicht ausreichen oder gar unbrauchbar sind. Dadurch kann es vorkommen, dass gewisse Aspekte der Szenarien nicht genau den Szenarien entsprechend oder sich nur unzureichend nachbilden lassen. Dieses Kapitel beinhaltet weiterhin eine Bewertung der bestehenden Modelle.

1 Einführung

Nachdem alle Vorarbeiten für das neue Konzept erledigt sind, geht es in Kapitel 5 an die Erstellung eines neuen Virtualisierungs-Management-Modells, das die besonderen Anforderungen unterschiedlicher Nutzergruppen erfüllt und so weit generisch ist, dass der Benutzer nichts über die darunter arbeitenden Virtualisierungslösungen zu wissen braucht. Das Ziel ist, dem Nutzer die Möglichkeit zu bieten eine komplette virtuelle IT-Infrastruktur zu betreiben ohne zu wissen, wie die Infrastruktur virtualisiert wird. Ein weiteres Ziel ist, dass den Nutzern je nach Bedarf und/oder Fachwissen unterschiedlich detaillierte Informationen und Aktionen angeboten werden sollen. Das erstellte Modell wird dann noch anhand der erhobenen Anforderungen bewertet.

Für das letzte Kapitel bleibt noch eine Erläuterung was im Rahmen dieser Arbeit getan wurde und welche Ziele dabei erreicht wurden. Anschließend wird Zusammengefasst, welche Erweiterungsmöglichkeiten das Virtualisierungs-Management-Modell bietet.

1.4 Zusammenfassung

Dieses Kapitel führte in die Thematik der Diplomarbeit ein. Es wurde die Motivation für das Thema dargelegt und wie die Arbeit thematisch einzuordnen ist. Darauf folgte die Definition des Modell-Begriffs, der für diese Arbeit von grundlegender Wichtigkeit ist. Anschließend wurden Grundlagen der wichtigen Techniken erläutert, die für diese Arbeit relevant sind. Um einen Überblick über die folgenden Kapitel zu geben, wurde der Aufbau der Ausarbeitung dargelegt.

2 Existierende Modelle

In diesem Kapitel werden die Modelle, die als Referenz für das Virtualisierungs-Management-Modell dienen, näher untersucht. Es wird eine Bestandsaufnahme gemacht, wie existierende Produkte, den Benutzern der Management-Anwendungen die Informationen über reale oder virtuelle Objekte, mit denen sie arbeiten, präsentieren. Hierbei wird der Schwerpunkt der Betrachtungen auf die Netze gelegt. Die hier gesammelten Informationen dienen dazu, in Verbindung mit den Anforderungen an ein Virtualisierungs-Management-Modell, ein solches zu entwickeln. Zur Analyse des aktuellen Standes der Technik werden die Modelle bestimmter Produkte benutzt. Bei diesen Produkten handelt es sich um PAN[Ege], VMware ESX[VMwa] mit Virtual Center[VMwb], Virtual Iron[Virc] und VIOM[Fujc].

2.1 PAN

Processing Area Network (PAN, [Ege]) ist ein Konzept, das von der Firma Egenera für Management-Produkte, z.B. für den Einsatz auf Blade-Servern umgesetzt wurde. PAN wird vom Kooperationspartner Fujitsu Siemens Computer eingesetzt und vertrieben. Mit PAN ist es möglich sowohl Server als auch Netze zu virtualisieren. Im folgenden wird darauf eingegangen, wie einem Benutzer der Management-Anwendung von PAN das System präsentiert wird und welche Möglichkeiten dem Nutzer geboten werden. Als Management-Schnittstelle bietet PAN eine Webanwendung als GUI. Es ist zwar auch möglich PAN über ein CLI zu steuern, aber in dieser Arbeit wird, so weit nicht anders angegeben, die GUI verwendet. Als Testumgebung für diese Arbeit steht eine Installation von PAN bei Fujitsu Siemens auf einer Primergy BX 600[Fujb] bereit. PAN kann auch auf anderen Hardwareplattformen, z.B. auf einem BladeFrame[Fuja] betrieben werden.

2.1.1 Voraussetzungen

PAN hat als Systemvoraussetzung einen Primergy BladeFrame[Fuja] oder eine Primergy BX600. Dies sind Systeme von Fujitsu-Siemens, die auf der Blade-Technologie basieren.

PAN kann ein oder mehrere physikalische Einheiten, die sogenannten Frames, verwalten. Ein Frame verfügt intern über Rechen-Ressourcen im Form von Bladeservern und externe Netz- und Storage-Anschlüsse. In einem Frame unterscheidet man drei Arten von Blades. Die einzelnen Blade-Arten sind sehr speziell für eine bestimmte Aufgabe konzipiert, und nur durch den gemeinsamen Einsatz aller drei Blade-Typen ist es möglich eine funktionierende Infrastruktur zu betreiben. Die drei Arten sind:

pBlades Die sogenannten Processing Blades liefern nur Rechenleistung und RAM. Sie brauchen, um sinnvoll betrieben zu werden, noch eine I/O-Schnittstelle nach außen. Die Anzahl an pBlades in einem Frame ist nicht festgelegt aber je nach Typ des Frames nach oben beschränkt.

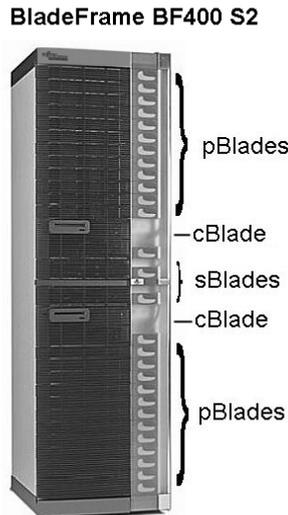


Abbildung 2.1: Hardware Struktur eines BladeFrame auf dem PAN eingesetzt werden kann (aus [Ege07])

cBlades Durch die Control Blades werden dem Blade Frame und die darin enthaltenen Blades Managementfunktionen angeboten. Die cBlades stellen auch ein Gateway zwischen dem internen Netz (siehe sBlade unten) und den externen LAN und SAN dar, für deren Zugang sie NICs und HBAs bereitstellen. Es gibt in einem Frame zwei solcher cBlades, wobei eine redundant ist und für den Failover-Einsatz vorgesehen ist.

sBlades Switch Blades dienen zum Switchen der Pakete, die zum einen intern zwischen den pBlades untereinander und zum andern zwischen pBlades und cBlades eines Frames gesendet werden. Sie sind für die Kommunikation innerhalb eines Frames zuständig und für die Kommunikation nach außen. Wie bei den cBlades gibt es in einem Frame zwei Stück davon, wobei beide redundant eingesetzt werden. Es ist auch möglich eine Bandbreitenbündelung über beide sBlades für logische Verbindungen einzusetzen.

In Abbildung 2.1 ist ein BladeFrame mit den Blade-Arten dargestellt. Nur mit den drei Komponenten für Rechenleistung (pBlades), I/O-Zugriff und Management (cBlades) und für die Kommunikation zwischen den Blades und dem Netz (sBlades) kann eine voll funktionsfähige virtualisierte Infrastruktur aufgebaut werden. Über die cBlades wird, wie eben schon gesagt, die Management-Schnittstelle, der PAN-Manager, angeboten. Da zwei cBlades in einem Frame vorhanden sind, von denen jeweils eines davon als aktives betrieben wird, wird beim Aufruf der IP-Adresse des Managers, der Datenverkehr an das aktive cBlade geleitet. Weiterhin existiert noch ein Management Blade (MMB), über das das „konventionelle“ Management des Frames durchgeführt werden kann, wenn auf PAN verzichtet wird. Beim Einsatz von PAN wird das MMB jedoch nicht angezeigt, sondern der PAN-Manager fragt das MMB ab, um z.B. Informationen über die Blades eines Frames zu bekommen, die vom MMB verwaltet werden. Insofern wird das MMB durch PAN verschattet und stellt nur eine technische Komponente in einem BladeServer Frame dar.

2.1.2 Struktur

Bei PAN hat der Nutzer des PAN-Managers kaum direkt mit Virtualisierung als solcher zu tun. Es wird zwar viel mit virtuellen Objekten gearbeitet, aber der Nutzer hat nur selten Einfluss auf die Durchführung oder auf Details der Virtualisierung. Viele Objekte, die verwendet werden, sind automatisch angelegte virtuelle Objekte oder die Erstellung der virtuellen Objekte wird vor dem Nutzer versteckt. So kann ein Nutzer ein pBlade in virtuelle Blades (vBlades) unterteilen. Diese vBlades sind virtuelle XEN-Maschinen, die im Hintergrund angelegt werden. Es gibt keine Möglichkeit direkt auf die XEN-Domains zuzugreifen. Die komplette Umsetzung der Virtualisierung bleibt vor dem Nutzer verborgen. Auch virtuelle Netzgeräte, wie vSwitches oder vEthS sind in ihrer wirklichen Implementierung vor dem Nutzer verborgen. Auch hier bekommt der Nutzer keine Einflussmöglichkeiten auf die im Hintergrund durchgeführte Virtualisierung. Das komplette PAN-System ist darauf ausgelegt dem Nutzer Objekte des PAN zu präsentieren und die im Hintergrund laufenden Aktionen zu verbergen. Um sich mit PAN zurecht zu finden, muss der Benutzer jedoch dieses PAN-System zuerst verstehen, das sich zwar an Hardware-Objekten der realen Welt orientiert, aber eigene Konzepte in sich birgt.

Ein zentraler Begriff bei PAN ist das LPAN (Logical PAN), das eine gesamte von PAN verwaltete virtuelle Infrastruktur darstellt. In einem LPAN können Server und Netze virtualisiert werden und mit Festplatten und Tape-Laufwerken verbunden werden. In einem PAN kann es mehrere LPAN geben, die logisch gesehen vollkommen unabhängig voneinander sind und von unterschiedlichen Administratoren verwaltet werden können. Ein LPAN besteht aus Zuweisung von Ressourcen und in ihnen erstellten logischen Servern, den sogenannten pServern. In Abbildung 2.2 sind diese Zusammenhänge abgebildet.

Die Verwaltungsmöglichkeiten für LPANs erstrecken sich einmal über die Ressourcen (siehe Seite 15) , die dem entsprechenden LPAN zugewiesen sind und auf der anderen Seite lassen sich mehr oder weniger technische Einstellungen wie Domain-Settings und Einstellungen zur High-Availability durchführen.

Ein konkretes LPAN ist die Zusammenfassung aller physischen und virtuellen Komponenten, die eine Infrastruktur bilden. Anders gesagt stellt ein LPAN einen vernetzten Server-Verbund dar, der auch als solcher gesteuert werden kann. Für die Erstellung einer solchen Infrastruktur werden Ressourcen zu Strukturen zusammengefasst. Einem LPAN werden dazu Ressourcen wie Blades, SCSI-Disks und -Tapes sowie vSwitches, über die die Anbindung an virtuelle Netze realisiert wird zugewiesen. Außerdem werden dem LPAN angeschlossene oder virtuelle DVD-ROM-Laufwerke (bei virtuellen Laufwerken wird ein Pfad zu einem Image angegeben) zugewiesen. Es besteht die Möglichkeit, 'local pBlade Pools' für das LPAN zu definieren. Weiterhin existieren in einem LPAN virtuelle Server, die hier pServer heißen, die die dem LPAN bereitgestellten Ressourcen und die im LPAN definierten local Blade Pools benutzen können. Die Verwendung von Pools ist eine Alternative zur direkten Zuweisung der Blades an ein LPAN. Ist einem pServer ein Pool als Blade zugewiesen, wird das erste Blade in dem Pool benutzt, unabhängig davon, ob es sich um ein pBlade oder ein vBlade handelt. Fällt ein Blade aus, wird das nächste im Pool benutzt. Fällt auch dieses aus, wird so lange das nächste verwendet, bis alle Blades als ausgefallen getestet wurden.

Ein pServer kann die Ressourcen und Pools des LPAN zugewiesen bekommen. Es gibt die Möglichkeit ein Primär- und ein Sekundär-Blade für einen pServer zu definieren. Dabei können die Blades sowohl pBlades, vBlades oder auch Blade Pools sein. Weiterhin können Disks, Tapes und DVD-Laufwerke zugewiesen werden. Für die Kommunikation innerhalb

2 Existierende Modelle

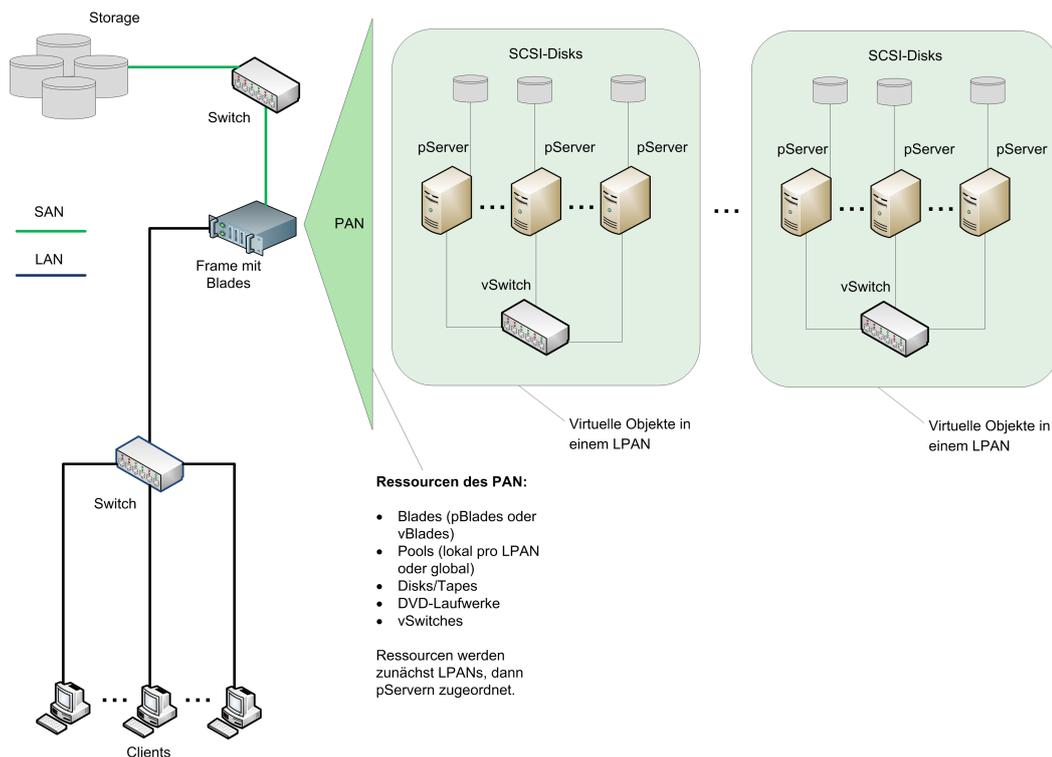


Abbildung 2.2: Logische Struktur von PAN

des PAN oder über ein externes Netz können noch vEth (virtual Ethernet, eine virtuelle Ethernetkarte, die vom Gastbetriebssystem als normale NIC verwendet werden kann) angelegt werden, die, wenn Zugriff auf externe Netze möglich sein soll, mit einem vSwitch verbunden werden können. Einem pServer kann ein Boot-Image zugewiesen werden, das für das Booten eines Systems zuständig ist. Ein Boot-Image ist aber nicht wie der Name evtl. vermuten lässt, ein Betriebssystem-Image, das gebootet werden kann, sondern nur ein kleines System, das es dem pServer ermöglicht die virtualisierte Infrastruktur zu benutzen, um dann das Betriebssystem von angeschlossenen Medien oder über das Netz zu booten. Standardmäßig wird hierfür EVBS (Egenera Virtual Boot System) verwendet, das in etwa dem BIOS herkömmlicher Systeme entspricht.

Netz Management-Modell

Nun wird, entsprechend der Aufgabenstellung, das Managementmodell für Netze bei PAN näher untersucht. In Abbildung 2.3 sind die Teile des Modells aufgezeigt. Dabei handelt es sich um den *pServer*, der keine oder bis zu mehreren *vEth*s zugewiesen bekommen kann. Ein pServer kann jeweils ein *pBlade* oder ein *vBlade* als primäres und als sekundäres Blade zugewiesen bekommen, auf dem gebootet wird. Ein vBlade wird auf einem pBlade gehostet, wobei ein pBlade nicht unbedingt vBlades hosten muss. Eine vEth ist einem vSwitch zugeordnet, während umgekehrt einem vSwitch zwischen 0 und mehreren vEths zugeordnet sind. Der vSwitch selbst benutzt eine *rEth* (redundant Ethernet, siehe nächster Abschnitt) des cBlades. Erst bei der Zuordnung einer rEth zu einem vSwitch wird das Attribut VLAN-Id gesetzt. Die Benutzung von mrEths (mega redundant Ethernet, siehe nächster Abschnitt)

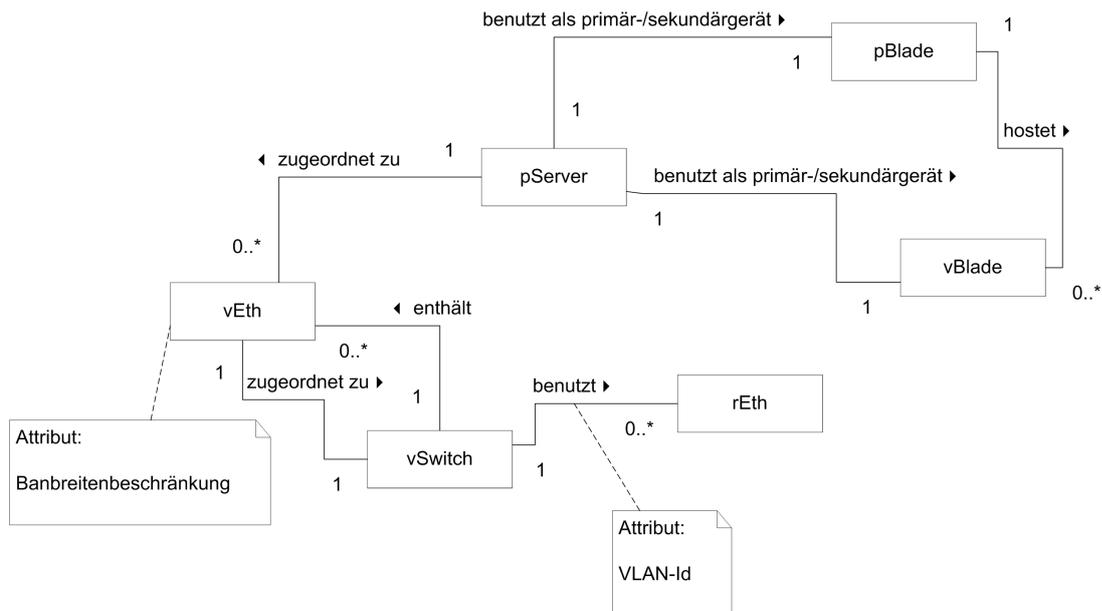


Abbildung 2.3: Das Netz-Management-Modell bei PAN

sowie von Blade-Pools wird hier nicht aufgeführt, da diese Konzepte in dieser Arbeit nicht verwendet werden und das Modell so übersichtlicher gehalten wird.

2.1.3 Oberfläche

Wird die Managementanwendung von PAN über einen Webbrowser aufgerufen, werden nach dem Einloggen zunächst die folgenden Unterteilungen angezeigt:

- Dashboard
- <Name des PAN>
- Discovered PANs
- Security
- Platform
- Resources
- LPANs

Das *Dashboard* (siehe Abbildung 2.4) zeigt eine Übersicht der vorhandenen pServer. Hier wird der Name der pServer, ihr Status (nicht gebootet, bootet, gebootet, herunterfahren) zusammen mit der Uptime und Informationen über die „Gesundheit“ (Health) des pServers angezeigt. Die entsprechenden Events können über das Dashboard eingesehen werden. Die Gesundheit eines pServers richtet sich dabei nach der Schwere der aufgetretenen Events, eingeteilt in drei Schweregrade: rot (schwerwiegender Fehler), gelb (nicht-kritischer Fehler), grün (Warnmeldungen). Weiterhin werden Kontrollelemente angezeigt, mit denen ein

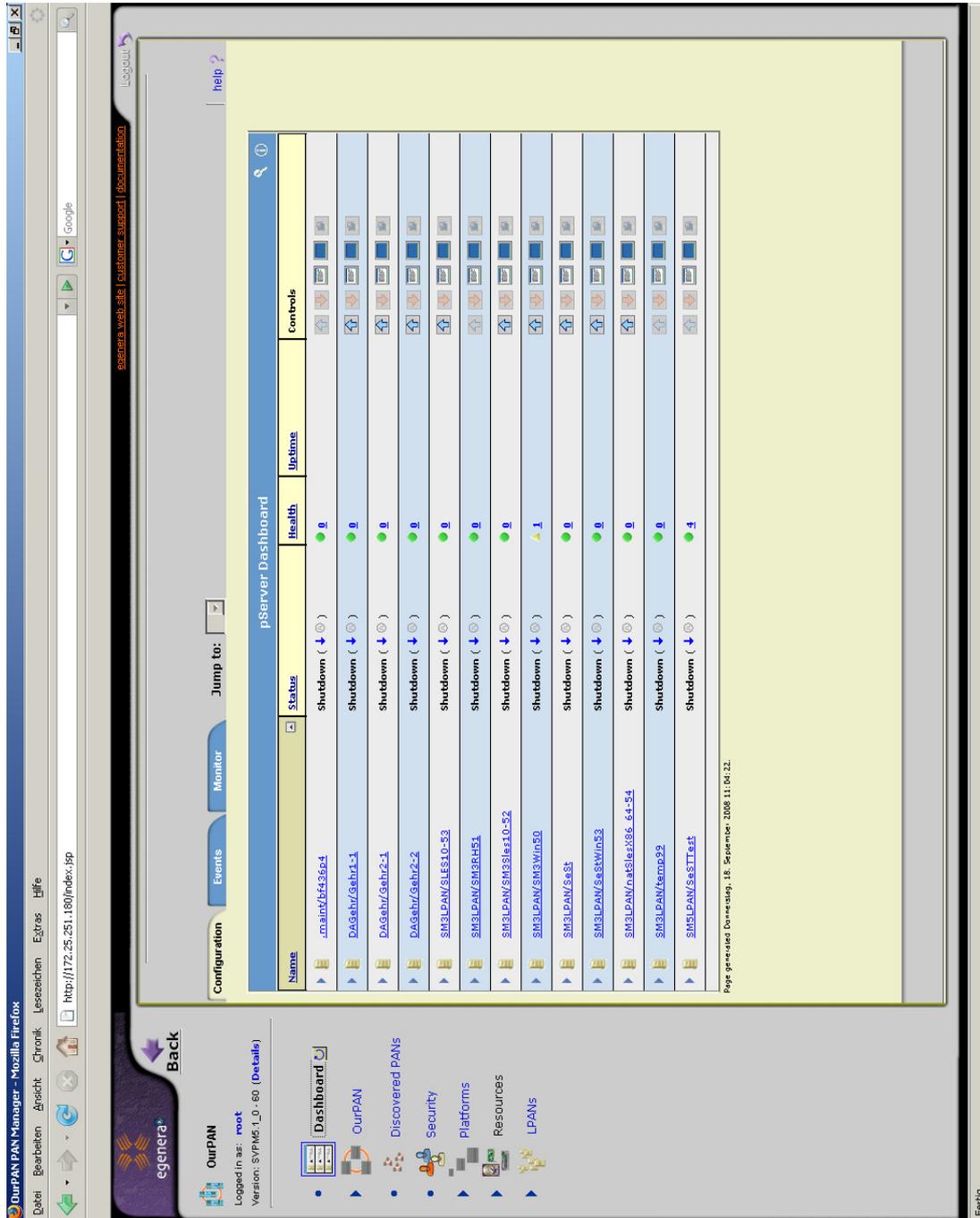


Abbildung 2.4: Screenshot des Pan Manager Dashboards

pServer gebootet oder heruntergefahren werden kann oder mit denen eine Verbindung zum Gastsystem eines pServers hergestellt werden kann (Konsole oder graphisch).

Unter dem Punkt *<Name des PAN>* werden Informationen zu der PAN Plattform (der Hardware auf der das PAN betrieben wird) und Einstellungsmöglichkeiten zu den Boot-, Root- und Media-Images angezeigt. Root- und Media-Images können dazu verwendet werden um pServer zu booten oder sie können in pServern als Speichermedien verwendet werden. Boot-Images übernehmen in etwa die Funktion des BIOS in herkömmlichen Systemen und ermöglichen das Booten von den angeschlossenen Medien. Weiterhin gibt es unter diesem Punkt die Möglichkeit Einstellungen zu Disaster Recovery, Domain Settings und Licenses zu tätigen. Disaster Recovery dient dazu, Backups des PAN oder von Images zu erstellen oder die Planung für automatische Backups einzustellen. Ein Backup des PAN enthält nur die Daten des PAN selbst, und keine Daten der angeschlossenen Medien. Die angeschlossenen Speichersysteme, auf der die virtualisierten Systeme arbeiten, müssen mit externen Mitteln gesichert werden. Unter Domain Settings lassen sich Einstellungen für externe SNMP Manager durchführen. Unter Licenses schließlich ist die Verwaltung von Lizenzen dieses PAN möglich.

Der Punkt *Discovered PANs* bietet eine Übersicht über weitere PANs, die sich im selben Management-Netz befinden. Der Nutzer bekommt die Möglichkeit sich über die Einträge hier direkt auf den anderen PANs anzumelden.

Unter *Security* lassen sich die User des PAN verwalten, es können User bestimmten Rollen, an die Berechtigungen geknüpft sind, zugewiesen werden und es ist möglich System User Gruppen anzulegen und diesen Gruppen User zuzuweisen.

Platforms bietet einen Überblick über den Hardwareaufbau des PAN. In einer Grafik werden die beiden cBlades und die pBlades mit dem jeweiligen Status angezeigt.

Die Ressourcen, die in PAN verwaltet werden, können unter dem Punkt *Resources* der Managementanwendung verwaltet werden. Diese Ressourcen werden später den LPANs zugeordnet und von ihnen benutzt. Die Ressourcen sind in folgende fünf Kategorien unterteilt, denen die entsprechenden einzelnen Ressourcen untergeordnet sind:

- Blades:
 - pBlades sind die wirklich physisch vorhandenen Blades. Sie können als ganzes einem LPAN zugewiesen werden oder logisch in vBlades unterteilt werden.
 - vBlades sind virtuelle Unterteilungen von pBlades. Bei der Erstellung wird festgelegt, wie viele Prozessoren und wie viel Speicher des pBlades dem vBlade zur Verfügung stehen.
- Pools:
 - Hierbei handelt es sich um globale Blade-Pools, die von jedem pServer, den es innerhalb der LPAN des PANs gibt, verwendet werden können. Den Pools können sowohl pBlades als auch vBlades zugeordnet werden.
- Disks:
 - SCSI-Disks haben LUNs, die im SAN für die Benutzung durch das PAN freigegeben sind und von PAN automatisch entdeckt werden. Hier kann die Partitionstabelle der Disks bearbeitet werden. Diese Disks stehen später den auf den pServern laufenden Betriebssystemen als Festspeicher zur Verfügung.

- Tapes:
 - SCSI-Tapes sind ebenfalls über SAN angeschlossene Geräte.
- Networking:
 - vSwitches sind virtuelle Switches, denen ein Uplink, also eine Ethernet-Verbindung nach außen, zugewiesen werden kann. Dieser Uplink wird über die beiden Ethernet-Ports der cBlades realisiert (siehe rEth). Wird kein Uplink angegeben, kann dieser vSwitch nur für PAN-Interne Kommunikation verwendet werden.
 - mrEth (mega redundant Ethernet) sind Verbindungen zwischen Frames die eine Blade Farm bilden.
 - rEth (redundant Ethernet)
 - * Interface 1 oder 2 (cBlade) sind die beiden Ethernet-NICs der beiden cBlades.
 - * Usage (vSwitch) - Gibt die Zuweisung der NICs an vSwitches an.
 - Ethernet Devices (cBlades, rEths)

Nachfolgend gibt es noch einen letzten Punkt *LPANs*. Für jedes LPAN können die einzelnen pServer verwaltet werden und es gibt für das LPAN globale Einstellungsmöglichkeiten für Domain Settings und High Availability (siehe im vorherigen Abschnitt 2.1.2).

2.2 VMware

Im folgenden wird der VMware ESX Server mit dem Management durch Virtual Center [VMwb] betrachtet.

ESX Server Der VMware ESX Server ist ein Produkt für die Virtualisierung von Servern und Netzen. Er besteht aus einem eigenen Kernel und einem angepassten Linux-System, der sogenannten Service-Konsole. Über die Service-Konsole werden nötige Dienste angeboten, während der Kernel den Hypervisor beinhaltet und für die Virtualisierung und Ressourcenverwaltung des Servers zuständig ist¹. Es ist auch möglich, einen ESX Server direkt mittels Webanwendung oder VI-Client (Virtual Infrastructure-Client) zu managen, jedoch stehen dann im Vergleich zu Virtual Center nur wenige Möglichkeiten zur Verfügung. Da hier das Management über Virtual Center betrachtet wird, kann das direkte Management vernachlässigt werden, da der ESX Server nach seiner Installation direkt dem Virtual Center bekannt gemacht wird, das dann die gesamte Steuerung übernimmt.

Virtual Center Virtual Center ist die Management-Plattform von VMware, mit deren Hilfe VMware Server (ein inzwischen frei verfügbares VMware Produkt zur Servervirtualisierung, früher bekannt als GSX-Server) und ESX-Server gemanagt werden können. Das Produkt umfasst die Komponenten, die im folgenden Abschnitt genannt werden.

2.2.1 Voraussetzungen

Wie in Abbildung 2.5 zu sehen, besteht eine Infrastruktur in dieser Konstellation hauptsächlich aus einem oder mehreren ESX Server-Hosts für die Virtualisierung und einem Virtual Cen-

¹Die Nachfolgerversion des ESX-Servers, der ESXi-Server besteht nur noch aus dem Kernel ohne die Server Konsole, wodurch Ressourcen auf dem Host, aber auch Verwaltungsaufwand eingespart wird.

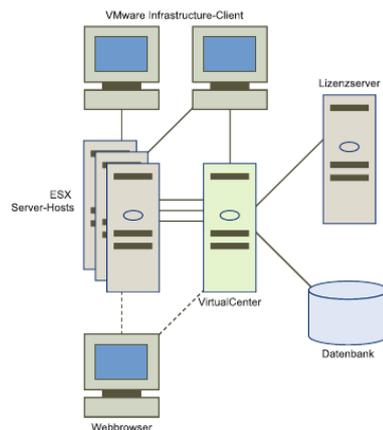


Abbildung 2.5: Basiskomponenten einer VMware-Infrastruktur (aus [VMw08a])

ter Server, der für das Management der ESX Server-Hosts zuständig ist. Der Virtual Center Server benötigt eine Datenbank zur Speicherung der Daten und einen Lizenzserver auf dem die Lizenzen der Infrastruktur verwaltet werden. Beide Komponenten können aber auch auf demselben System laufen wie der Virtual Center Server. Das System ist so konzipiert, dass im Falle eines Ausfalls des Management-Servers (also des Virtual Center-Servers) die Hosts mit den darauf laufenden virtuellen Maschinen weiter laufen. Die grundlegende Funktion der Infrastruktur ist durch einen Ausfall des Virtual Center-Servers nicht gefährdet. Für den Zugriff auf das Management stehen zwei Möglichkeiten zur Verfügung. Es kann über einen Webbrowser auf eine Webanwendung mit eingeschränkten Möglichkeiten zugegriffen werden, oder es kann der VI-Client (Virtual Infrastructure Client), der auf einem Windows-Rechner installiert werden kann, benutzt werden. Mit diesem Client kann Virtual Center in vollem Umfang benutzt werden.

2.2.2 Struktur

Im folgenden wird die logische Struktur von Virtual Center beschrieben. Die Grundlage für die Beschreibung ist die Oberfläche des VI-Clients.

Die logische Struktur, in der Server im VI-Client dargestellt werden, ist eine mögliche Darstellung physischer Strukturen. Als oberste Ebene eines Baumes gibt es Datacenter, die auch räumlich entfernte Orte darstellen können. Innerhalb der Datacenter können dann sogenannte Cluster gebildet werden, die eine logische Gruppierung darstellen. Diese Cluster beinhalten die ESX-Server, die durch Virtual Center verwaltet werden. Auf den ESX-Servern können dann Virtuelle Maschinen (VM) angelegt werden.

Ein weiteres Merkmal ist die Bildung von Ressourcen-Pools. Ressourcen-Pools können auf Clustern oder Servern gebildet werden. Dabei werden die in der jeweiligen Aggregation vorhandenen Ressourcen zusammengefasst und können von den VMs dieses Aggregates benutzt

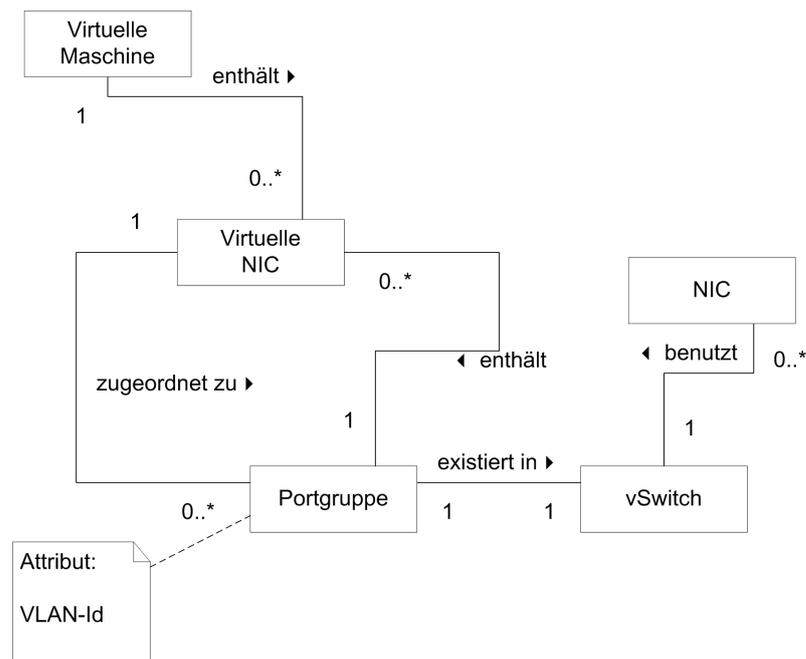


Abbildung 2.6: Das Netz-Management-Modell bei VMware

werden.

Für die Kommunikation der VMs können auch virtuelle Netze innerhalb eines ESX Server-Hosts eingerichtet werden. Ein Netz wird durch einen virtuellen Switch (vSwitch) repräsentiert, der an einen ESX-Server-Host gebunden ist. Ein Konzept bei den virtuellen Netzen ist die sogenannte Portgruppe, die eine Menge von Einstellungen für die Verbindung ist. Dazu gehören z.B. Bandbreitenbeschränkungen oder VLAN-Einstellungen. Diese Portgruppen sind an die „interne Seite“ des vSwitches, also den ESX-Host gekoppelt. Die physisch vorhandenen NICs des Hosts können an die „externe Seite“ des vSwitch angeschlossen werden. Werden mehrere NICs angeschlossen, bilden diese eine NIC-Gruppierung. Innerhalb dieser Gruppierung kann festgelegt werden, ob der Datenverkehr auf die NICs aufgeteilt wird oder, ob sie für einen Failover-Einsatz vorgesehen sind.

Ebenfalls auf der Ebene der ESX Server-Hosts werden die Zugänge zur Storage festgelegt. Die ESX-Server können auf Plattenspeicher zugreifen, der entweder lokal verfügbar ist oder es können externe Speicher über FC-SAN, iSCSI oder NAS verwendet werden.

Netz Management-Modell

Im obigen Abschnitt wurde schon erklärt, wie die Netze generell bei VMware aufgebaut sind. Nun wird genauer auf das dabei verwendete Managementmodell eingegangen. In Abbildung 2.6 ist zu sehen, dass das Modell aus den Teilen *virtuelle Maschine*, *virtuelle NIC*, *Portgruppe*, *vSwitch* und *NIC* besteht. Eine virtuelle Maschine hat analog zu einer physischen Maschine keine, eine oder mehrere virtuelle NIC. Eine virtuelle NIC wird beim Management mit VMware einer Portgruppe zugeordnet. Eine virtuelle NIC kann keiner oder bis zu mehreren Portgruppen zugeordnet sein. Eine Portgruppe kann keine bis mehrere VMs beinhalten. Die Portgruppe hat ein Attribut, *VLAN-Id*, das, falls gesetzt, die Zugehörigkeit einer

Portgruppe zu einem VLAN bestimmt. Eine Portgruppe ist genau einem vSwitch zugeordnet, während ein vSwitch keine bis mehrere Portgruppen beinhalten kann. Der vSwitch kann an vorhandene NICs des Hosts angeschlossen werden. Wird er an keine NIC angeschlossen, besteht nur ein virtuelles lokales Netz innerhalb des Hosts. Werden mehrere NICs angeschlossen, können Bandbreiten zusammengefasst werden oder NICs für den Failover-Fall ausgewählt sein. Die hier genannten Teile, beschreiben die Objekte, mit denen der Nutzer die Netz-Komponente beeinflussen kann.

2.2.3 Oberfläche

Der VI-Client bietet vier Ansichtskategorien an, bei denen jeweils unterschiedliche Ansichten der Infrastruktur und ihrer Komponenten angezeigt werden. Diese Ansichtskategorien heißen 'Bestandslisten' und es gibt die folgenden vier Ansichten:

Hosts & Cluster: Zeigt den logischen Aufbau (Data Center, Cluster, ESX-Hosts und Virtuelle Maschinen) an.

Virtuelle Maschinen & Vorlagen: Zeigt eine Liste der vorhandenen VMs und der Templates (Vorlagen) aus denen einfach VMs erstellt werden können. Ebenso werden die Pools und die zugeordneten VMs angezeigt.

Netzwerke: Zeigt die vorhandenen Netze an.

Datenspeicher: Zeigt die vorhandenen Datenspeicher an.

Bei jeder der vier Ansichten wird, wie auch in Abbildung 2.7 zu sehen ist, auf der linken Seite ein Baum mit den entsprechenden Elementen angezeigt. Je nach ausgewählten Element werden dann auf der rechten Seite der Anzeige Reiter mit Informationen und möglichen Aktionen zu den Elementen angezeigt.

Templates sind Images (Abbilder) von Virtuellen Maschinen, aus denen leicht VMs erstellt werden können. Diesen VMs müssen dann noch die Netz- und Datenspeicherkonfiguration übergeben werden. Danach ist eine VM mit Betriebssystem und installierten Anwendungen zum Betrieb bereit. Sollen virtual Appliances eingesetzt werden, können diese direkt als VMs auf den entsprechenden Hosts importiert werden.

2.3 Virtual Iron

Virtual Iron Extended Enterprise Edition ist ein Produkt der Firma Virtual Iron Software.

2.3.1 Voraussetzungen

Eine Virtual Iron Infrastruktur wird durch einen Management-Server gesteuert und besteht aus virtuellen Servern, angeschlossenem SAN und teils physisch vorhandenen, teils virtuellen Netzen. Der Management-Server mit dem Namen VI-Center ist für den Betrieb aller durch Virtual Iron verwendeten Teile zuständig bietet auch eine Java-GUI an. Sie wird über Java WebStart gestartet und kann gesamte Virtual Iron System steuern. Diese GUI ist von jedem Rechner mit installiertem JRE aus verfügbar, der Zugriff auf den Management-Server hat. Der Management-Server sollte mit einem unterstützten Betriebssystem (verschiedene

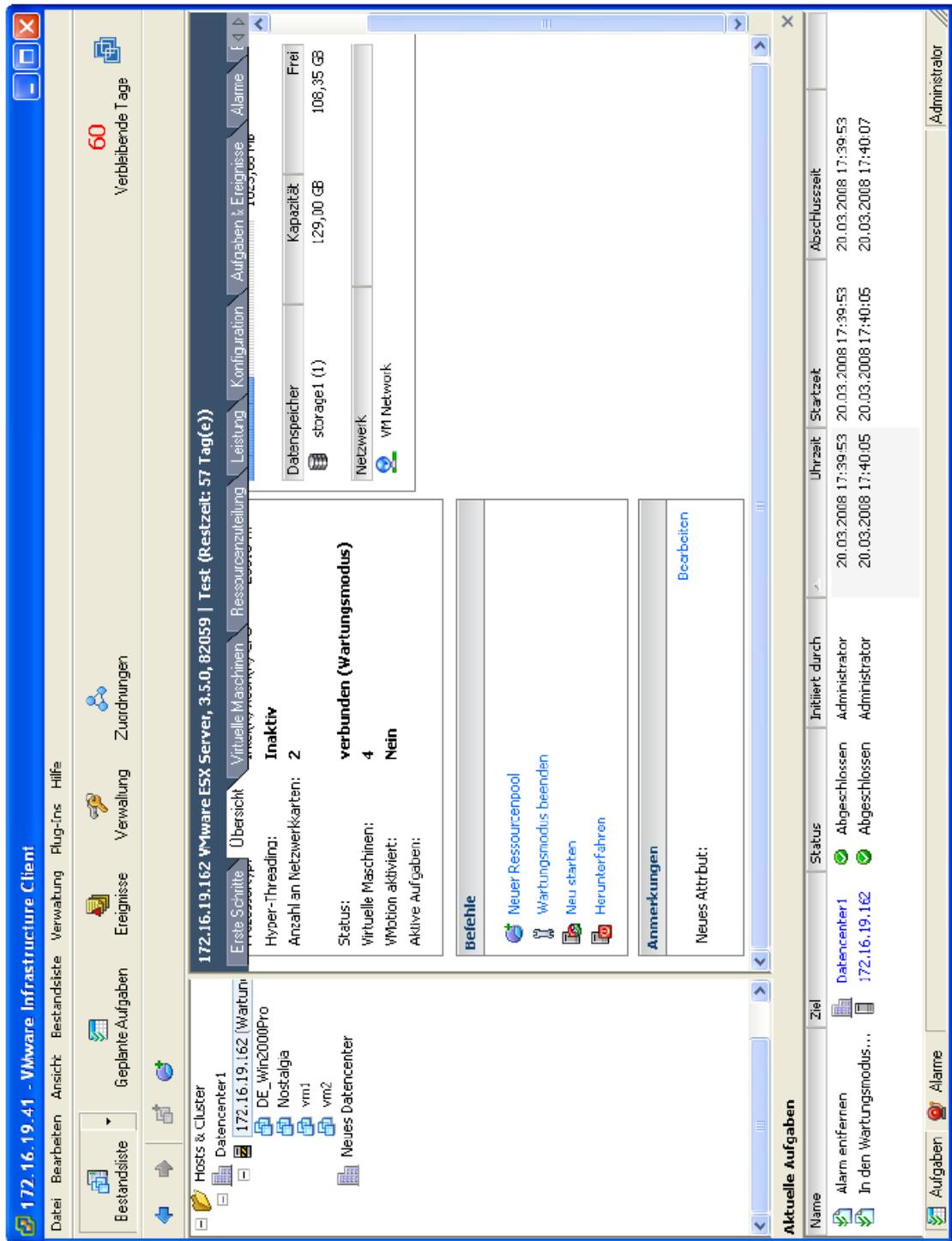


Abbildung 2.7: Der VI-Client

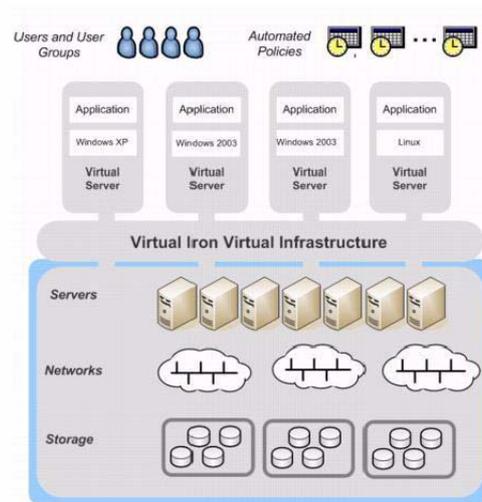


Abbildung 2.8: Schematischer Aufbau einer VI-Infrastruktur (aus[Vir08])

Windows Versionen oder unterschiedliche Linuxdistributionen) ausgestattet sein und über mindestens zwei NICs verfügen, da für den Betrieb von Virtual Iron ein gesondertes Management-Netz verwendet wird. Die einzelnen Hardware-Server sollten aus diesem Grund ebenso mindestens zwei NICs haben und müssen über einen Prozessor mit Virtualisierungsunterstützung verfügen. Weiterhin müssen sie über PXE (Preboot Execution Environment) booten können und sollten um den Komfort für die Administratoren zu erhöhen, über LAN zu starten sein.

2.3.2 Struktur

Die angeschlossenen Server müssen sowohl Anschluss an das separate Managementnetz haben als auch an etwaige weitere Netze, wie ein LAN und/oder ein SAN.

Eine Virtual Iron Infrastruktur ist die Zusammenfassung aller realen und virtuellen Komponenten eines 'Resource Centers' (siehe auch Abbildung 2.10). Das Resource Center wird in ein oder mehrere Virtual Data Center (VDC) gegliedert, denen ein oder mehrere physikalische Server (in der VI-Nomenklatur als *Nodes* bezeichnet) zugeordnet werden. Diesen physikalischen Nodes werden wieder Virtual Server (VS) untergeordnet. Auf den VS werden dann die Gastsysteme ausgeführt. Damit ist die Struktur innerhalb Virtual Iron schon beschrieben.

Vorhandener Festpeicher kann auf verschiedene Weisen bereitgestellt werden. Er kann als SAN über Fiber Channel oder iSCSI verfügbar gemacht werden oder als lokale Platte eines verwalteten Nodes. Es gibt zwei Möglichkeiten auf Storage zuzugreifen. Die eine Möglichkeit ist der 'direkte' Zugriff, wie beispielsweise Server auf eine verfügbare LUN eines SAN zugreift oder der Weg über logische Platten. Der Zugriff über logische Platten bietet einige Vorzüge wie die Möglichkeit der Unterteilung der Platten in mehrere Teile, die Fähigkeit Platten zu klonen oder VHDs (Virtual Hard Disk) zu importieren. Über die Verwendung von VHD können auch direkt Virtual Appliances genutzt werden. Weiterhin gibt es das Konzept der Disk-Gruppen, die als Container für logische Disks zu verstehen sind. Innerhalb der Disk-Gruppen werden dann die entsprechenden logischen Platten erstellt, die letztlich den VS als

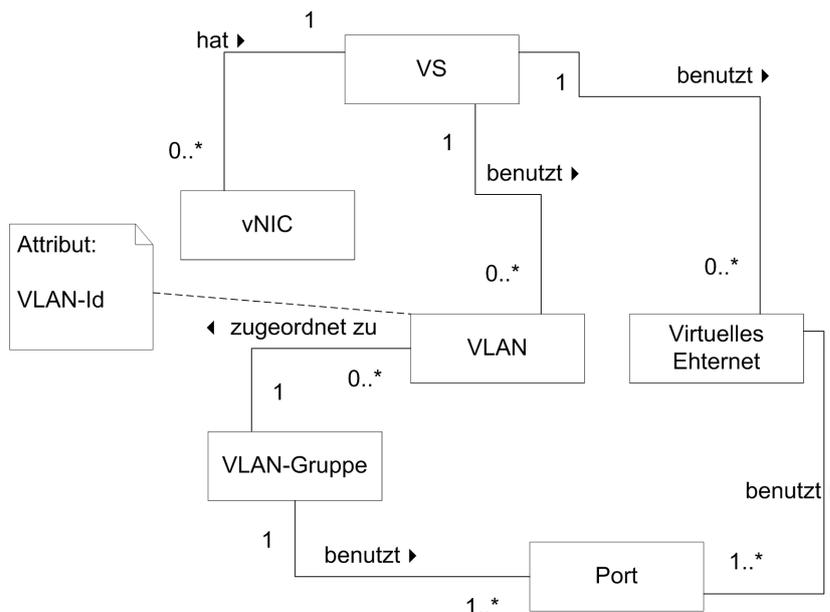


Abbildung 2.9: Das Netz-Management-Modell bei Virtual Iron

Speicher zugewiesen werden können.

Logische Netze lassen sich mit Virtual Iron einfach einrichten und verwalten. Diese können auch VLAN-Tagging durchführen und so externe VLANs erweitern.

Netz Management-Modell

Virtual Iron kennt folgende Objekte für das Netz-Management. Der *VS* bekommt keine, eine oder mehrere *VNIC* zugewiesen, die über eine virtuelle MAC verfügen. Ebenfalls wird ihm ein *Netz* zugewiesen. Dieses Netz kann, wie in Abbildung 2.9 dargestellt, entweder ein *virtuelles Ethernet* sein oder ein *VLAN*. Vom Management unterscheiden sich virtuelles Ethernet und VLAN nicht. Bei der Auswahl von Netzen können beide Arten ausgewählt werden. Ein VLAN hat noch die *VLAN-Id* als Attribut. Die VLANs werden in *VLAN-Groups* gruppiert. Die *Ports*, also die NICs der Nodes, werden entweder einem virtuellen Ethernet oder einer VLAN-Gruppe zugewiesen, wenn ein Uplink gewünscht wird. Ein VLAN bekommt die Ports über die VLAN-Group zugewiesen, während ein virtuelles Ethernet die Ports direkt zugeteilt bekommt.

2.3.3 Oberfläche

Der Aufbau des VI-Centers ist unterteilt in fünf Bereiche. Diese Bereiche sind *Resource Center*, *Hardware*, *Policies & Reports*, *Jobs* und *Users*. Bei Auswahl eines der Bereiche werden die weiteren Unterteilungen angezeigt. Dabei wird linksseitig eine Baumansicht mit den relevanten Objekten angezeigt und rechts finden sich entsprechend der Auswahl im Baum Reiterkarten mit Informationen oder möglichen Aktionen.

Das *Resource Center* (zu sehen in Abbildung 2.10) zeigt vorhandene Elemente der Infrastruktur in einer Baumansicht. Die angezeigten Elemente sind: das Resource Center selbst, die darin erstellten VDCs mit den ihnen zugeteilten Nodes. Zusätzlich werden in dem Baum

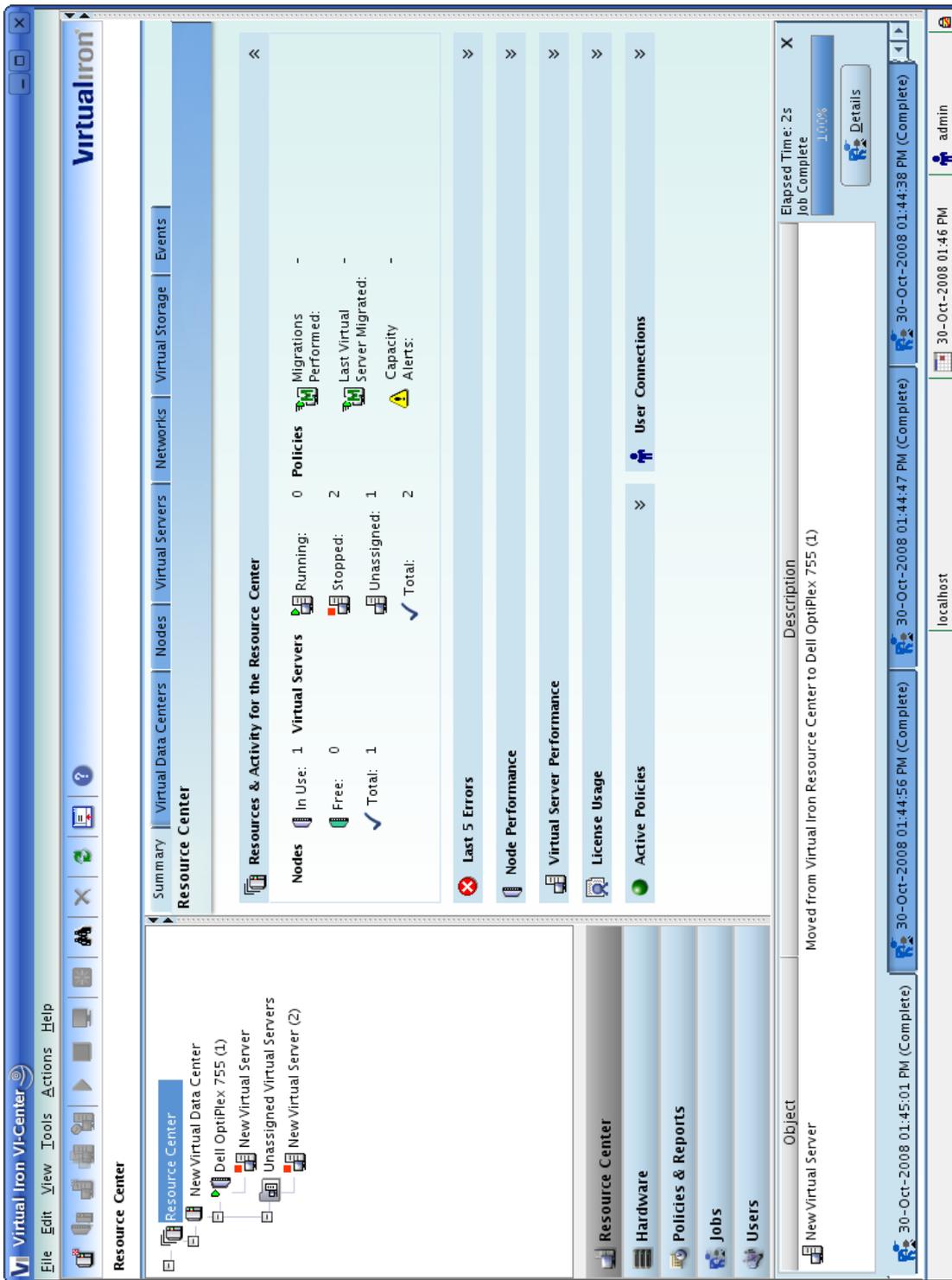


Abbildung 2.10: Screenshot des VI-Centers mit angezeigtem Resource Center

noch VS angezeigt, die den Nodes zugewiesen sind, aber auch nicht zugewiesene Nodes werden in jedem VDC unter dem Punkt 'Unassigned Virtual Servers' angezeigt. Die auf der rechten Seite angezeigten Registerkarten hängen von der Art des ausgewählten Knotens auf der linken Seite ab und bieten Aktionen und Informationen, die für das ausgewählte Bauelement relevant sind.

Der Punkt *Hardware* zeigt in der linken Baumansicht die verwaltete Hardware (*Managed Nodes*) an. Unterhalb der Nodes wird die dem Node zugehörige Hardware aufgelistet. Die einzelnen angezeigten Hardwarekomponenten sind nach der Art des Anschlusses (z.B. Ethernet, Fibre Channel, ...) gruppiert. Die Tabs auf der rechten Seite zeigen hier überwiegend nur Informationen über die ausgewählten Elemente der linken Seite.

Unter dem Punkt *Policies & Reports* werden Policies (Richtlinien) für das System und Reports aufgeführt. Die Policies sind in User und System Policies unterteilt. User Policies regeln Aktionen, die zu bestimmten Zeiten ausgeführt werden können. Es gibt standardmäßig nur drei User Policies zur Email-Benachrichtigung über bestimmte Events, zum automatischen Neustarten von VDCs und für das System-Backup. System Policies sind für das Verschieben von VS auf andere Nodes zuständig. Dies kann je nach Policy beim Ausfall eines Nodes passieren oder wenn ein Node eine bestimmte CPU-Last für eine festgelegte Zeit überschreitet (auf einen weniger ausgelasteten Node). In umgekehrter Form, wenn eine bestimmte CPU-Last für eine festgelegte Zeit unterschritten wird kann ein VS auf einen stärker ausgelasteten Node verschoben werden. Bei letzterem kann, wenn der letzte VS von einem Node weg migriert wurde, der Node heruntergefahren werden. Dieser Vorgang kann bei Bedarf auch rückgängig gemacht werden. Die Reports schließlich bieten die Möglichkeit über bestimmte Elemente der Infrastruktur oder Ereignisse Berichte anfertigen zu lassen, die über die entsprechende Registerkarte eingesehen werden können.

Der Bereich *Jobs* bietet eine Möglichkeit sich die im System angefallenen Jobs nach Datum und Uhrzeit sortiert anzusehen. Dabei werden Details wie Start- und Endzeit, die Dauer und der Eigentümer der Jobs und die einzelnen Schnitte, aus denen sie bestehen, sichtbar.

Unter dem letzten Punkt, ist eine einfache Nutzerverwaltung für Virtual Iron möglich. Hier können Nutzer erstellt und gelöscht, Passwörter können geändert werden und es besteht die Möglichkeit einer Integration eines LDAP zur Nutzerverwaltung.

2.4 VIOM

VIOM (ServerView Virtual-IO Manager) ist ein Produkt von Fujitsu-Siemens Computer, das I/O-Virtualisierung in BX 600 Frames²[Fujb] einsetzt. VIOM ist in die ServerView Suite von Fujitsu-Siemens eingebettet und bietet daher eine Möglichkeit vom zentralen Management-Server aus, die I/O-Virtualisierung zu verwalten. Der Vorteil der I/O-Virtualisierung, der bei VIOM zum Tragen kommt, ist, dass die Adressen eines Blade-Servers in einem Frame nicht mehr auf den Komponenten des Blades, also der NIC oder dem HBA, gespeichert werden. Dadurch kann z.B. bei einem Ausfall eines Blades dieses ersetzt werden, ohne dass weitere Schritte bei der Netz- oder Storage-Administration nötig würden. Wären die Adressen, also die MAC und die WWN, in den Komponenten des Blades gespeichert, müssten das angeschlossene LAN bzw. SAN so neu konfiguriert werden, dass dort die neuen Adressen bekannt

²BladeServer bieten die optimalen Hardwarevoraussetzungen, da ein MMB vorhanden ist, das Informationen über die vorhandenen Blades hat und auch die virtuellen Adressen für die Blades speichern kann. Weiterhin haben diese Frames ein IBP (Intelligent Blade Panel), das die nötige Pfadschaltung liefert.

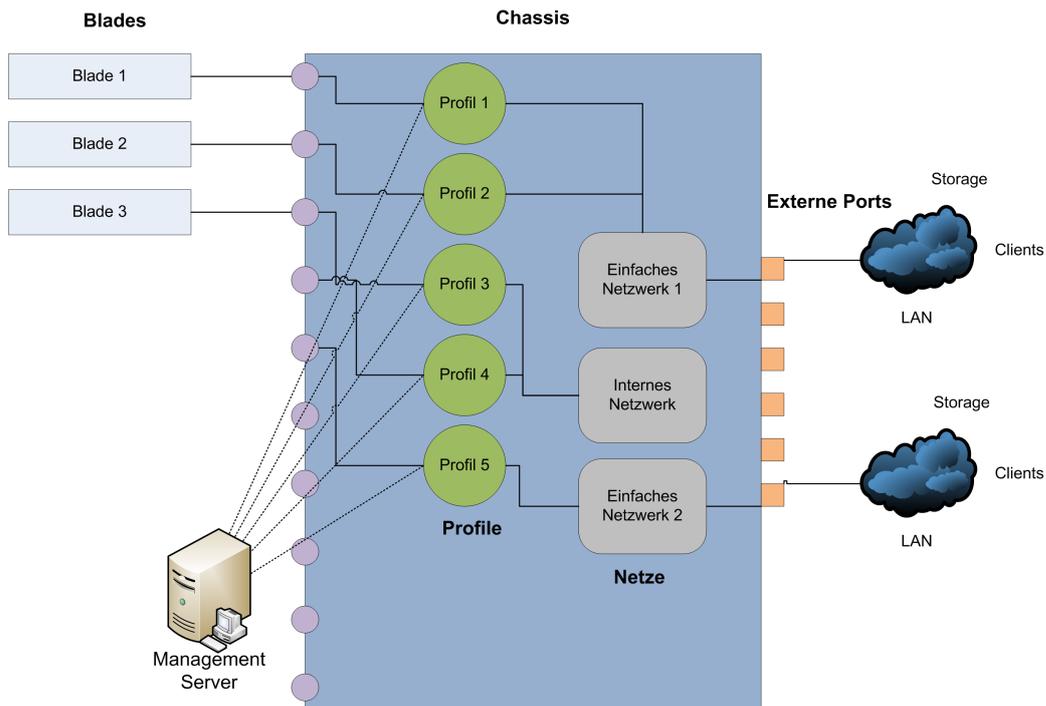


Abbildung 2.11: Schematische Darstellung des VIOM-Aufbaus

gemacht würden.

2.4.1 Voraussetzungen

Wie schon eingangs erwähnt, wird VIOM auf BX 600 Frames von FSC betrieben. Jedoch ist der vollständige Einsatz nur mit bestimmten Komponenten, bzw. mit bestimmten Versionen der Blades in dem Frame möglich. Im Besonderen wird hier ein Intelligent Blade Panel (IBP) eingesetzt, das das Switch-Blade bei der Verwendung mit PAN ersetzt. Das IBP selbst ist kein Switch, sondern ist mehr als ein Patch Panel zu verstehen, das dazu dient die Verbindungen der Blades zu den Ports festzulegen.

2.4.2 Struktur

Der wesentliche Punkt bei VIOM ist die Virtualisierung der Adressen eines Blades. Damit kann unter Verwendung von Netzwerkpfeilen und Profilen erreicht werden, dass ein Server von einem Slot in einen anderen umgezogen werden kann, ohne weitere Konfiguration des LAN oder des SAN nötig zu machen. Es kann genauso einfach ein Backup-Server definiert werden, der, falls er übernehmen muss, ohne weitere Konfiguration der Netze eingesetzt werden kann.

Der Begriff des Netzes bei VIOM beschreibt die verwendeten Uplinks. Das bedeutet, ein externer Port eines IBP wird einem Blade, genauer gesagt einem Slot, zugewiesen. Uplinks können entweder als aktive Uplinks oder als Backup definiert werden. Ein oder mehrere Uplinks werden in ein Uplink Set zusammengefasst. Sind mehrere aktive Uplinks in ein Uplink Set zusammengefasst, wird dieses als Link Aggregation Group (LAG) bezeichnet. Mit

diesem LAG ist es möglich über parallele Verbindungen die Übertragungsrate zu erhöhen.

Bei der Erstellung der Netzwerkpfade wird unterschieden zwischen drei Netz-Arten:

Interne Netze beschreiben die Verbindung von Blades innerhalb eines IBP ohne eine Verbindung nach außen.

„Einzelne“ Netze (single networks) definieren den Zugang in genau ein externes Netz. Sie sind VLAN transparent, das bedeutet ankommende oder ausgehende Pakete werden ungeachtet evtl. vorhandener VLAN-Tags zugestellt.

Netze mit VLAN-Ids beschreiben Netze, bei denen sich unter Umständen virtuelle Netze mit verschiedenen „Netz-Nummern“ (VLAN-Ids) ein Uplink Set teilen. Dabei kommen von den Blades Pakete ohne VLAN-Tag. Diese werden dann erst im Frame entsprechend der definierten Netze hinzugefügt und entsprechend weitergeleitet. Ankommende Pakete müssen passende VLAN-Tags haben, ansonsten werden sie nicht weitergeleitet.

Ein Profil dient dazu, Informationen für Verbindungen in externe Netze, für Adressen (MAC, WWN) und für Boot-Devices mit Parametern zu speichern. Die Profile sind völlig von Blades oder Frames losgelöst und werden auf dem zentralen Managementserver gespeichert. Sie können später Slots eines Frames zugewiesen werden, selbst wenn dieser noch nicht belegt ist. Auf diese Weise ist es möglich, angewandte Profile von einem Frame auf ein anderes umzuziehen, ohne weiteren Konfigurationsaufwand auszulösen.

Nun noch zu einigen Details die Arbeitsweise von VIOM betreffend. Die Profile sind, wie schon erwähnt, zunächst von der Hardware unabhängig auf dem Management-Server gespeichert. Werden die Profile einem Slot eines Frames zugewiesen, werden die entsprechenden Konfigurationsdaten des Profils in dem MMB des Frames gespeichert. Wird nun ein Blade gebootet, wird in einer Tabelle in dem MMB überprüft, ob für den entsprechenden Slot Daten gespeichert sind. Ist dies nicht der Fall bootet das Blade mit den Adressen (MAC und WWN), die auf der Hardware gespeichert sind. Sind für den Slot Daten gespeichert, werden diese Adressen anstatt der Hardwareseitig vergebenen verwendet. Durch die Speicherung der Daten in dem MMB eines Frames wird hauptsächlich eine gewisse Unabhängigkeit vom Management-Server geschaffen, denn selbst falls der VIOM-Manager nicht verfügbar ist, können die durch VIOM verwalteten Frames fehlerfrei funktionieren. Der gesamte Aufbau von VIOM ist schematisch in Abbildung 2.11 dargestellt. Dort ist nochmals der Zusammenhang von externen Ports (Uplinks), Netzen, Profilen und Slots (mit Blades) dargestellt.

Netz Management-Modell

Das Managementmodell bei VIOM ist in Abbildung 2.12 abgebildet. Darin gibt es einen *Server* (ein Blade), der in einem *Slot* des *Chassis* steckt. Das Chassis selbst hat 10 Slots, die mit Servern belegt sein können oder nicht. Ein *Profil* kann direkt Slots zugewiesen werden, unabhängig davon, ob der Slot mit einem Server belegt ist. Das Profil enthält 2 bis 6 *Ports*, die *Netzen* zugeordnet werden können. Ein Netz kann ein *Uplink-Set* benutzen, das aus einem oder mehreren *Uplinks* besteht. Soll ein Netz ein VLAN sein, kann die VLAN-Id im Netz gesetzt werden. Soll ein Netz nur ein lokales Netz sein, wird kein Uplink-Set dafür benötigt.

2.4.3 Oberfläche

Beim Aufruf von VIOM in der ServerView Suite wird zunächst einmal eine Standardansicht mit einer Serverliste auf der linken Seite und Versionsinformationen auf der rechten Seite

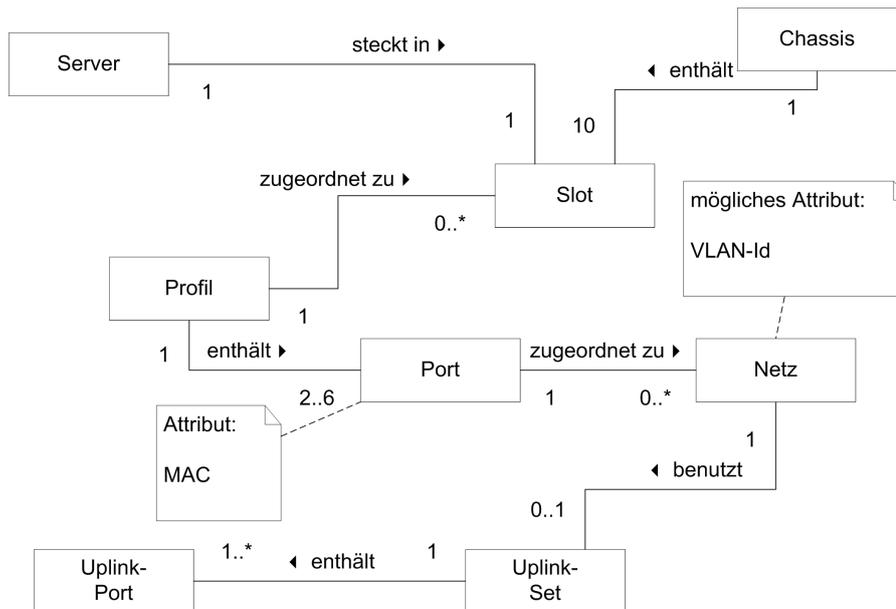


Abbildung 2.12: Das Netz-Management-Modell bei VIOM

angezeigt. Die Serverliste ist unterteilt in drei Bereiche, *all Server*, *VIOM manageable* und *VIOM managed*, also jeweils eine Übersicht über alle Server, die mit ServerView verwaltet werden, über die Server, die VIOM verwalten kann und die Server, die VIOM aktuell verwaltet. Unter den mit VIOM verwaltbaren Servern werden nur die aufgelistet, die die physikalischen Voraussetzungen für den Einsatz von VIOM erfüllen. Wird in der Liste für alle Server ein Eintrag ausgewählt, wird auf der rechten Seite in der einzigen aktiven Reiterkarte *Setup* eine graphische Darstellung mit einigen Technischen Daten des Systems angezeigt. Die graphischen Darstellungen zeigen die Vorder- und die Rückseite des Chassis. Es werden auch die jeweils vorhandenen Blades (sowohl die Rechen-Blades auf der Vorderseite, als auch die Kommunikations-Blades auf der Rückseite) angezeigt. Bei Auswahl eines eingesetzten Blades werden Die eingesetzten Blades können ausgewählt werden, worauf technische Details wie der verwendete Slot, der Produktname, die IP-Adresse, der Manage-Status (Managed oder nicht), der Fault-State und der State-Cause angezeigt werden. Ist ein System nicht durch VIOM managebar, so wird das durch ein Warn-Icon an den entsprechenden Blades verdeutlicht. Auf diese Weise werden jedoch nur BX 600 Frames angezeigt. Wenn VIOM das Management eines Frames übernimmt, verliert dieser zunächst die gesamte evtl. vorhandene Konnektivität. Unter der Reiterkarte *Setup* kann ein Chassis in die Verwaltung mit VIOM aufgenommen oder daraus entlassen werden. Hier können ebenfalls die gespeicherten Zugangsdaten verändert werden. Im Fall eines schwerwiegenden Fehlers ist es möglich über die Option 'Restore' die Daten der Management-Datenbank erneut in das IBP zu schreiben.

Mit dem Reiter *Chassis Configuration* wird eine schematische Ansicht der Konfiguration des Frames angezeigt. Dabei werden sowohl die Slots mit den sich darin befindlichen Blades angezeigt, der Name des Profils, das dem Blade zugeordnet ist, sowie die entsprechende Verbindung der Uplink Sets.

Die Registerkarte *Ext. LAN Connections* zeigt zwei Reiterkarten an. Die erste, *Graphic* zeigt eine schematische Darstellung der angeschlossenen IBPs und ermöglicht das Erstellen

und Bearbeiten von Netz-Pfaden auf den IBPs. Die Reiterkarte *Details* zeigt in einer Tabelle die Definitionen der vorhandenen Netze. Die Schritte zur Erstellung und Bearbeitung lassen sich auch in dieser Ansicht durchführen.

Mit dem Reiter *Server Blade Configuration* können Daten über die einzelnen Slots und den ihnen zugewiesenen Profilen eingesehen werden. In dieser Ansicht ist auch das Booten oder Herunterfahren von Blades möglich. Es besteht hier auch die Möglichkeit Profile direkt anzulegen und sie anschließend zuzuweisen.

Unter dem Punkt *Profiles* auf der linken Seite lassen sich Server Profile anlegen und verwalten. Diese Ansicht bietet eine komplette Auflistung aller vorhandenen Profile.

Ein wichtiger Punkt der bei VIOM auffällt, ist das Log-Meldungen, die für die Überwachung des Systems oder zur Fehlersuche nötig sind, nur über das Windows-System Log verfügbar sind.

2.5 Zusammenfassung

In diesem Kapitel wurden die vier Virtualisierungslösungen, die in dieser Arbeit getestet und deren Virtualisierungs-Management-Modelle überprüft werden, vorgestellt. Es wurden für jedes Produkt die technischen Voraussetzungen, die logische Struktur einer damit implementierten Infrastruktur und die Management-Oberfläche beschrieben. Leider war im Gegensatz zu den anderen Modellen für VMware ESX und Virtual Center keine Testumgebung vorhanden. Dadurch fällt hier die Beschreibung etwas weniger detailliert aus. Ebenso konnte die Umsetzung der Szenarien nur theoretisch „auf dem Papier“ durchgeführt werden. Martin Roll und Christoph Biardzki standen jedoch zur Verfügung, um die VMware-Themen zu besprechen.

3 Szenarien und Anforderungen

Dieses Kapitel beschreibt die Szenarien, die in dieser Arbeit verwendet werden, um die existierenden Modelle, die in Kapitel 2 beschrieben wurden, bezüglich ihres Virtualisierungs-Management-Modells zu evaluieren. Jedes Szenario stellt einen Teil einer Infrastruktur dar, die in der beschriebenen oder in ähnlicher Form in real existierenden Infrastrukturen auftreten können. Die Szenarien wurden so ausgewählt, dass sie sich in verschiedenen Punkten voneinander unterscheiden. Dadurch ist gewährleistet, dass eine möglichst große Zahl von reell existierenden oder möglichen Umgebungen und die damit verbundene breit gefächerten Anforderungen, abgedeckt werden. So wird sichergestellt, dass das Modell, das im Verlauf dieser Arbeit entwickelt wird, für ein weites Spektrum an Einsatzmöglichkeiten geeignet ist und sich nicht nur auf wenige oder sehr spezielle Anforderungen anwenden lässt. Zunächst werden in Abschnitt 3.1 die vier Szenarien beschrieben. Dabei wird darauf eingegangen, welche Umgebung sich für den Nutzer darstellt und wie sich das Szenario charakterisieren lässt. Nach der Beschreibung der Szenarien werden in Abschnitt 3.2 die Anforderungen an das Virtualisierungs-Management-Modell aufgestellt.

3.1 Beschreibung der Szenarien

Nun werden die Szenarien definiert, wobei in der Beschreibung abstrakt geschildert wird, wie die Infrastruktur aufgebaut ist. Dabei geht es darum, was das Szenario funktional leisten muss und nicht um die wirkliche Umsetzung des Infrastruktur-Teils, den das Szenario darstellt. Es wird beschrieben, was für den Nutzer eines solchen Systems „sichtbar“ ist und welche infrastrukturellen Voraussetzungen dafür notwendig sind. Auf den konkreten Aufbau, ob direkt auf realer Hardware oder virtuell, wird später in Kapitel 4 eingegangen.

3.1.1 Szenario 1a

Dieses Szenario lässt sich zum Beispiel in einem kleinen Unternehmen finden, das seine eigene IT-Infrastruktur betreibt. Es gibt dort fünf Nutzer, die an ihren Arbeitsplätzen über den Browser ihres PCs an einer zentralen Geschäftsanwendung für die Auftragsbearbeitung arbeiten. Diese Anwendung ist, wie in Abbildung 3.1 zu sehen, nach der 3-Schichten-Architektur aufgebaut und benötigt einen Web-, einen Application- und einen Datenbank-Server. Es kann noch weitere allgemeine angebotene Dienste geben, von denen exemplarisch aber nur Email angegeben ist. Da es mehrere Arbeitsplätze gibt, müssen diese mit dem zentralen Server für die Geschäftsanwendung verbunden, also in irgendeiner Form vernetzt, sein. Ebenso ist die Speicherung der Daten notwendig, so dass auch Storage verfügbar sein muss. Nachts, wenn die Geschäftsanwendung nicht durch die Nutzer benutzt wird, soll anstatt der Auftragsbearbeitung die Rechnungserstellung laufen. Das lässt sich durch einen Wechsel der Geschäftsanwendung bewerkstelligen, der automatisch durchgeführt wird. Am Morgen wird dann wieder zur Anwendung für die Auftragsbearbeitung umgestellt.

3 Szenarien und Anforderungen

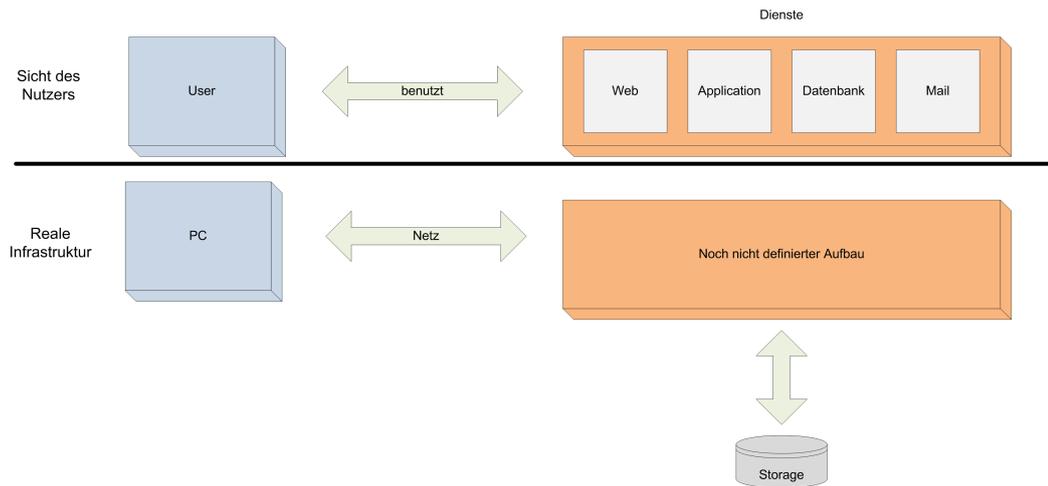


Abbildung 3.1: Szenario 1a

Ein weiteres Merkmal dieses Szenarios ist die Art und Weise in der die Administration durchgeführt wird. In dem Unternehmen gibt es Mitarbeiter, die sich um den Aufbau und den Betrieb der IT-Infrastruktur kümmern. Diese Mitarbeiter sind jedoch keine Fachkräfte im Bereich der Administration, sondern nur im Umgang mit Computern versierte Benutzer. Hieraus ergibt sich, dass bestimmte Aufgaben, sei es in der Planung und Umsetzung oder bei der Identifikation und Behebung von Problemen und Fehlern, durch diese Kräfte nicht umfassend gelöst werden können. Da das Unternehmen, um Kosten zu sparen, keinen Servicevertrag mit einem Anbieter hat, müssen in Fällen, in denen der eigene „Laien-Administrator“ nicht weiter helfen kann, die Dienste von Firmen in Anspruch genommen werden, die diese Probleme beheben können.

Das Szenario lässt sich wie folgt charakterisieren.

- Kleines Unternehmen mit eigener Infrastruktur
- Nutzer arbeiten mit Ihren Daten auf einem zentralen Server
- Wechsel der Geschäftsanwendung in der Nacht (geplante Dynamik)
- Mitarbeiter betreut die Infrastruktur (nicht-professioneller Administrator)

3.1.2 Szenario 1b

Dieses Szenario hat gemeinsame Komponenten mit dem vorherigen Szenario. Es handelt sich hier um ein Unternehmen, das zu seinem Stammhaus noch vier weitere Filialen/Standorte hat. In jeder dieser Niederlassungen ist dieselbe Infrastruktur vorhanden wie in Szenario 1a. Das heißt, es gibt pro Niederlassung fünf Mitarbeiter, die an ihren PCs auf der Geschäftsanwendung ihrer Niederlassung arbeiten. Die Daten werden an jedem Standort auf vorhandenen Datenspeichern gespeichert. Neben den Geschäftsanwendungen werden in den Standorten weitere Dienste angeboten, von denen in diesem, wie im vorigen Szenario Email als Beispiel angeführt wird. Der Aufbau dieses Szenarios ist in Abbildung 3.2 dargestellt. Die einzelnen Geschäftsanwendungen synchronisieren sich mit der in der Zentrale laufenden Instanz. Der

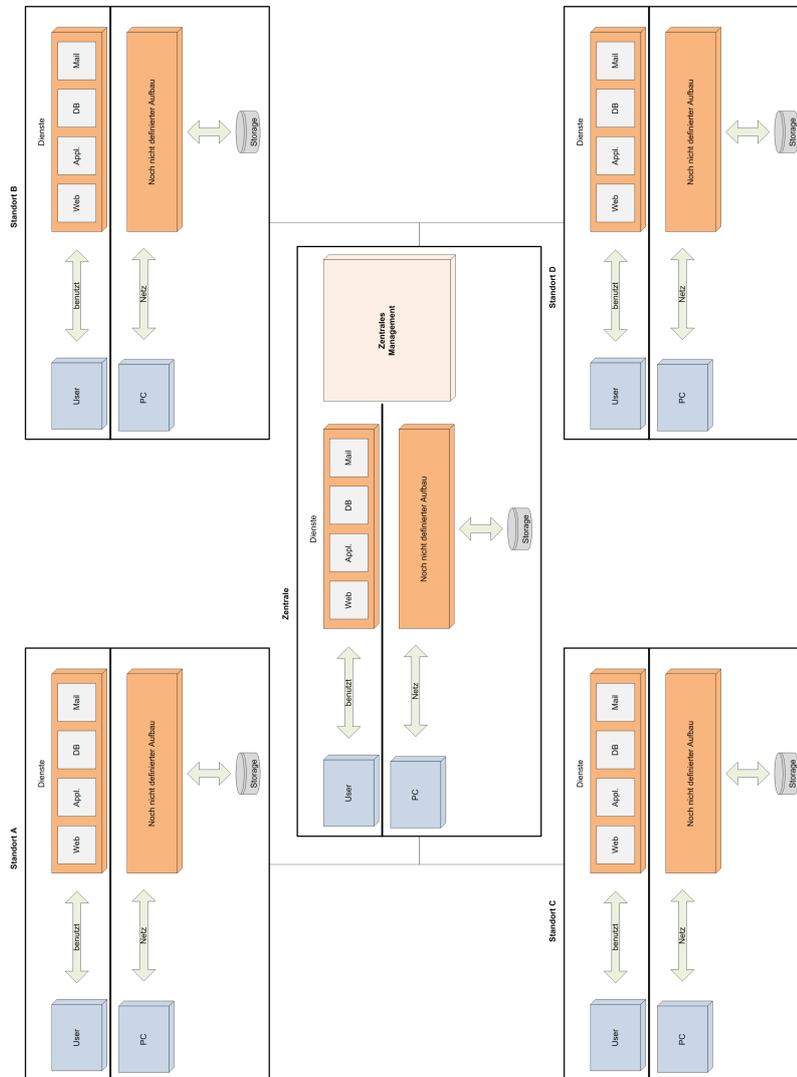


Abbildung 3.2: Szenario 1b

3 Szenarien und Anforderungen

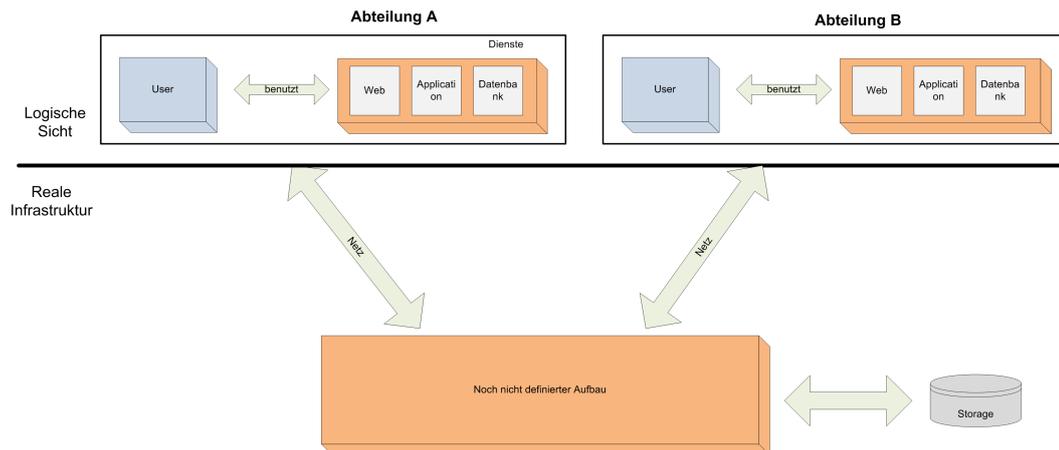


Abbildung 3.3: Szenario 2a

Wechsel der laufenden Anwendung wie in Szenario 1a bei Nacht ist hier nicht vorgesehen. Dadurch handelt es sich hier um eine statische Infrastruktur.

Das Management der Infrastrukturen der einzelnen Standorte wird hier aber nicht wie im ersten Fall vor Ort durchgeführt, sondern es gibt in der Zentrale einen professionellen Administrator, der alle Teil-Infrastrukturen remote verwaltet. Nur wenn das Arbeiten remote nicht möglich ist, z.B. durch Fehler, die das Personal vor Ort nicht beheben kann, muss der Administrator in dem entsprechenden Standort anwesend sein, um direkt dort zu arbeiten.

Im Folgenden wird zusammengefasst, was dieses Szenario charakterisiert:

- Mittleres Unternehmen mit eigener Infrastruktur in jedem Standort
- Benutzer arbeiten auf Infrastruktur und Daten in ihrem Standort
- Datenabgleich der Standorte mit der Zentrale
- Statische Infrastruktur
- Management der IT-Infrastruktur durch professionellen Administrator in der Zentrale
 - In der Zentrale findet das Management vor Ort statt
 - Die entfernten Standorte werden remote gemanagt

3.1.3 Szenario 2a

Dieses Szenario findet sich als Teil einer Infrastruktur eines großen Unternehmens, das ein eigenes Rechenzentrum betreibt. Der Teil davon, der hier betrachtet wird, sind, wie in Abbildung 3.3 dargestellt, zwei Abteilungen, die mit derselben Geschäftsanwendung, aber mit unterschiedlichen Daten arbeiten. Der Zugriff auf die Daten soll exklusiv nur für die eine Abteilung möglich sein. Dieses Szenario stellt z.B. auch ein typisches Outsourcing-Szenario dar, bei dem Kunden Dienste einkaufen, die von einem Rechenzentrum bereitgestellt werden. Mit diesem Hintergrund ist es besonders einsichtig, warum eine strikte Trennung der einzelnen Bereiche notwendig ist. Jede Abteilung hat zehn PC-Arbeitsplätze, die über das interne Netz mit den im Rechenzentrum betriebenen Servern verbunden sind. Wie auch in

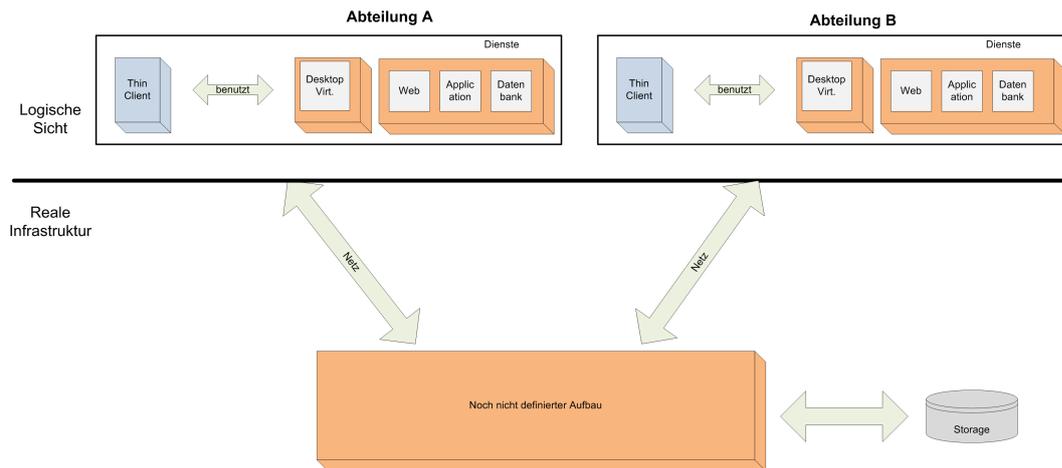


Abbildung 3.4: Szenario 2b

den beiden vorangegangenen Szenarien ist hier die Geschäftsanwendung wieder nach dem 3-Schichten-Prinzip mit einem Web-, einem Application- und einem Datenbankserver aufgebaut. Diese Server bieten sowohl die Möglichkeit zum dynamischen Failover, das bedeutet im Falle eines Fehlers auf der Hardware startet der Server automatisch auf einer anderen physikalischen Maschine. Ebenso wird dynamische Migration unterstützt, bei der ein Server im Fall einer zu starken Auslastung der System-Ressourcen auf eine weniger ausgelastete Hardware umzieht. Um eine wirkliche Trennung der beiden Abteilungen zu erreichen, hat jede der Abteilungen ein eigenes Netz zum Zugriff auf die Server. Dieser Netzzugang kann auch über VLAN erfolgen. Neben den Hardware-Servern ist hier noch ein Netz sowie die Möglichkeit zur Speicherung der Daten nötig. Es gibt also ein lokales Netz, über das die Clients der Abteilungen mit den Servern kommunizieren und den Zugang zu Storage, wo die entsprechenden Daten gespeichert werden. Die Administration der Infrastruktur erfolgt hier durch die im Rechenzentrum beschäftigten Administratoren. Dadurch sind professionelle Kräfte vorhanden, die, falls das nötig werden sollte, auch sofort Zugang zu der Hardware haben.

Dieses Szenario lässt sich wie folgt charakterisieren:

- Teil einer IT-Infrastruktur eines großen Unternehmens
- Zwei Abteilungen arbeiten mit der selben Anwendung
- Strikte Trennung der Abteilungen
- Beide Abteilungen arbeiten mit exklusiv für sie verfügbaren Daten
- Administration durch Administratoren des Firmen-Rechenzentrums
- Automatische Dynamik mit Failover und lastabhängiger Migration

3.1.4 Szenario 2b

Dieses Szenario hat grundsätzlich denselben Aufbau wie das eben beschriebene Szenario 2a (siehe Abschnitt 3.1.3) und ist auch in der selben Umgebung angesiedelt. Der wesentliche

3 Szenarien und Anforderungen

Unterschied ist, wie in Abbildung 3.4 zu sehen, dass die Client-PCs in den Abteilungen durch Thin-Clients ersetzt werden, die Desktopvirtualisierung einsetzen. Dadurch wird ein neuer Aspekt der Virtualisierung hinzugefügt und das Management der Desktops wird stark verändert. Ansonsten ist der Aufbau derselbe wie in Szenario 2a. Die Clients arbeiten an der Geschäftsanwendung, die durch drei Server bereitgestellt wird. Die Kommunikation erfolgt über getrennte Netze, so dass keine Abteilung auf die Daten der anderen zugreifen kann. Die Speicherung der Daten erfolgt auf angeschlossenen Storage-Möglichkeiten.

Dieses Szenario lässt sich wie folgt charakterisieren:

- Teil einer IT-Infrastruktur eines großen Unternehmens
- Zwei Abteilungen arbeiten mit der selben Anwendung
- Strikte Trennung der Abteilungen
- Beide Abteilungen arbeiten mit exklusiv für sie verfügbaren Daten
- Desktops in den Abteilungen sind virtualisiert und werden durch das Rechenzentrum bereitgestellt.
- Administration durch Administratoren des Firmen-Rechenzentrums
- Automatische Dynamik mit Failover und lastabhängiger Migration

3.1.5 Charakterisierung der Szenarien

Eine Charakterisierung ist in Tabelle 3.1 in Form einer Matrix zu sehen, in der einige Eckdaten zum Vergleich eingetragen sind. Dabei ist unter *Komplexität* die Komplexität der Infrastruktur und auch die Größe eines Szenarios gemeint. Mit *Ort der Administration* wird beschrieben, ob das Szenario lokal oder remote gemanagt wird. Welche fachliche Qualifikation der jeweilige Administrator hat wird mit *Qualifikation* beschrieben. *Dynamik* beschreibt das dynamische Verhalten eines Szenarios, also ob sich die Infrastruktur anpasst oder verändert oder ob ein statischer Aufbau vorliegt. Dynamik kann automatisch eintreten, um auf Gegebenheiten (z.B. Vergrößerung der Rechenleistung eines Servers bei Lastspitzen) zu reagieren oder geplant (z.B. Konsolidierung dreier Server auf einer Hardware um 21 Uhr) eingesetzt werden.

Szen.	Komplexität	Ort der Administration	Qualifikation	Dynamik
1a	Gering	Lokal	Nicht-prof. Admin	Gering, geplant
1b	Mittel	Remote und Lokal	Prof. Admin	Statisch
2a	Hoch	Lokal	Prof. Admin	Hoch, automatisch
2b	Hoch	Lokal	Prof. Admin	Hoch, automatisch

Tabelle 3.1: Übersicht über die Szenarien

3.2 Anforderungen

Die Modelle der betrachteten Produkte sollen zum Erlangen eines Überblicks den Stand der Technik dienen. Sie sollen deshalb auch mit Hilfe von Anforderung bewertet werden,

die hier beschrieben werden. Weiterhin sind dies die Anforderungen, die das zu erstellende Modell erfüllen muss. Dabei ist die übliche Unterteilung in funktionale und nichtfunktionale Anforderungen eingehalten worden. Generell wird in den Anforderungen, sofern nötig, die Einteilung und Klassifikation der Nutzer aus Abschnitt 3.1 in professionelle und nicht-professionelle Nutzer (siehe auch Tabelle 3.1) beibehalten. Bewerten lassen sich die Anforderungen jeweils mit einer Ordinalskala die von schlecht nach gut aufsteigend mit den Werten *nicht möglich*, *teilweise möglich* und *vollständig möglich* versehen ist. Ist für eine Anforderung die Bewertung mit *teilweise möglich* nicht sinnvoll, da die Anforderung nur erfüllt oder nicht erfüllt werden kann, so wird dort nur mit den beiden Extremwerten bewertet.

3.2.1 Aufstellung der Anforderungen

Die Anforderungen ergeben sich einerseits aus der Aufgabenstellung (siehe Abschnitt 1.1) und andererseits aus den Gegebenheiten der Szenarien. Zunächst muss es mit dem Virtualisierungs-Management-Modell möglich sein, virtuelle Infrastrukturen aufzubauen. Das beinhaltet die *Erstellung* der virtuellen Komponenten und deren Verbindung an die physische Umgebung. Der Aufbau und die Grundkonfiguration der Virtualisierungslösung wird hier ausgenommen, da es sich dabei bei jedem Produkt um individuelle Aufgaben handelt, die noch durch keine einheitliche Management-Plattform übernommen werden können. Beim Aufbau wird schon mit dem *physischen Management* und den evtl. vorhandenen Management-Domänen interagiert. Diese Interaktionen werden auch in der Betriebsphase der Infrastruktur nötig sein, um Anpassungen durchzuführen oder auf Probleme im *Betrieb* reagieren zu können. Auch innerhalb der virtuellen Infrastruktur fallen im laufenden Betrieb eine Vielzahl von Aufgaben an. Dazu gehören unter anderem Veränderungen der Infrastruktur oder ihrer Komponenten, Softwareupdates und die Erstellung von Backups. Das Virtualisierungs-Management-Modell soll Vorteile der Virtualisierung unterstützen, wie die schnelle Bereitstellung neuer virtueller Maschinen oder eine möglichst optimale Ausnutzung physischer Ressourcen. Ein Hilfsmittel dazu stellt *Automation* von Abläufen dar. Eine komplexe Infrastruktur wird für gewöhnlich nicht nur von einer einzigen Person betreut, daher ist es notwendig die Nutzer mit *Rollen und Rechten* auszustatten. In den Szenarien 2a und 2b (siehe die Abschnitte 3.1.3, 3.1.4) werden Teile der Infrastruktur beschrieben, die voneinander unabhängig verwaltet und betrieben werden müssen. Eine Änderung in einem Teil darf keine Auswirkung auf den anderen Teil haben. Aus diesem Grund ist die *Mandantenfähigkeit* des Modells nötig. Damit das Managementmodell nicht unnötig komplex wird, ist es nötig, das Management *transparent* darzustellen. Das bedeutet, das Modell, mit dem ein Nutzer arbeitet, ist ein anderes, als die Management-Plattform intern für ihre Arbeit nutzt. Die internen Vorgänge und Strukturen sind also für den Nutzer transparent. Die Aufgabenstellung fordert ebenso, dass auch Personen, die keine professionellen IT-Administratoren sind, mit dem Modell arbeiten können sollen. Das erfordert zunächst eine adäquate *Darstellung der Technik* für diesen Anwenderkreis, da es hier sinnvoll ist, Details vor dem Nutzer zu verstecken, um die Komplexität, die für nicht-professionelle Administratoren sehr hoch ist, zu verringern. Generell ist für die *Benutzbarkeit* wichtig, dass das Modell übersichtlich und verständlich ist. Das erleichtert den Umgang damit sowie die Erlernbarkeit. Das Modell muss auch, wie in den Szenarien zu sehen ist, mit kleinen und großen Infrastrukturen funktionieren. Ebenso muss es mit einer starken Veränderung der Größe der Infrastruktur zurechtkommen. Daher ist die *Skalierbarkeit* wichtig. Weiterhin soll das Modell auch in Zukunft einsetzbar sein, das bedeutet es muss möglich sein das Virtualisierungs-Management-Modell zu erweitern und

damit veränderten Anforderungen anzupassen.

Die in diesem Abschnitt *kursiv* dargestellten Begriffe stellen die Anforderungen an ein Virtualisierungs-Management-Modell dar und werden im Folgenden genau definiert.

3.2.2 Funktionale Anforderungen

A1 - Aufbau Es muss möglich sein, eine virtuelle Infrastruktur aufzubauen und in die bestehende physikalische Infrastruktur einzubinden. Dabei ist nur die Erstellung der Infrastruktur und die Anbindung an die bestehende Infrastruktur innerhalb der Virtualisierungslösung gemeint. Die Inbetriebnahme der erforderlichen Hard- und Software ist nicht Gegenstand dieser Anforderung. Konkret müssen folgende Schritte möglich sein:

Anlegen von virtuellen Komponenten

- Virtuelle Netze (Bandbreite, VLAN-Zugehörigkeit, internes Netz(nur innerhalb der virtuellen Infrastruktur), externes Netz(Anschluss an LAN))
- Virtuelle Maschinen (CPU-Leistung, RAM, Speicherplatz)
- Virtuelle Maschine aus Vorlage erstellen
- Speicherplatz für virtuelle Maschinen

Erstellen von Vorlagen (Templates)

- Vorlagen für virtuelle Maschinen erstellen

Bewertet wird diese Anforderung je nachdem, ob ein Modell diese Aufgaben erfüllen kann oder nicht. Eine teilweise Erfüllung (das bedeutet, wenn nicht alle Punkte möglich sind) wird als solche bewertet.

A2 - Betrieb Im Betrieb einer Infrastruktur fällt eine große Anzahl an nötigen Tätigkeiten über einen langen Zeitraum hin an. Um eine virtuelle Infrastruktur dauerhaft betreiben zu können, ist es notwendig, dass das Virtualisierungs-Management-Modell diese Tätigkeiten unterstützt. Diese Liste wurde erstellt und im Gespräch mit Christoph Biardzki auf Vollständigkeit überprüft.

Starten

- Virtuelle Maschinen
- Hosts (Virtualisierungsplattformen)

Stoppen

- Virtuelle Maschinen
- Hosts (Virtualisierungsplattformen)

Bearbeiten virtueller Komponenten

- Parameter virtuelle Maschine (CPU-Leistung, RAM, Speicherplatz)
- Migrieren virtuelle Maschine
- Virtuelle Netze (Bandbreite, VLAN-Zugehörigkeit, internes, externes Netz)
- Storage (auch Migration des Speichers der virtuellen Maschinen)
- Entfernen virtuelle Maschine

Veränderung der Hardwarestruktur

- Hinzufügen neuer Hosts
- Hinzufügen neuer Netzverbindungen
- Hinzufügen von Storage
- Entfernen von Hosts
- Entfernen von Netzverbindungen
- Entfernen von Storage

Diese Schritte ziehen evtl. eine Bearbeitung der virtuellen Komponenten nach sich.

Update

- Update Virtualisierungslösung
- Update Gastssysteme
- Update Tools¹(falls vorhanden)

Backup

- Backup Virtualisierung
- Backup Gastssystem
 - Von „innen“ (auf Betriebssystemebene)
 - Von „außen“ (Snapshot der virtuellen Maschine oder Kopie des Speicherplatzes einer virtuellen Maschine)
- Wiederherstellen von Backups im Notfall (Granularität (gesamte Platte, einzelne Datei) abhängig von der Art des Backups)

Das Backup von „innen“ wird vermutlich weniger vom Administrator der Infrastruktur ausgeführt, als vom Administrator des jeweiligen Servers. Da diese Rollen aber z.B. in Szenario 1a oder auch 1b von einer Person erfüllt werden, ist diese Option hier mit aufgeführt.

¹„Tools“ ist Software, die von dem Hersteller der Virtualisierungslösung bereitgestellt wird und in den Gastsystemen installiert werden sollte, um ein besseres Zusammenarbeiten der Gastssysteme mit der Virtualisierungslösung zu ermöglichen.

Überwachung (Monitoring, QoS) der Infrastruktur

- Hosts
- Virtuelle Maschinen
- Virtuelle Netze
- Speicherplatz der virtuellen Maschinen

Fehlermanagement

- Fehler lokalisieren
- Fehler beheben
 - Hardware
 - Software
 - * Innerhalb der Gastsysteme
 - * In der Virtualisierungslösung

Nutzer und Rollen

- Anlegen
- Bearbeiten (Namen, Rollen, ...)
- Löschen
- Bestehende Nutzer aus Verzeichnisdienst einbinden

Bearbeiten von Vorlagen

- Vorlagen für virtuelle Maschinen bearbeiten
- Vorlagen löschen

Bewertet wird diese Anforderung je nachdem, ob ein Modell diese Aufgaben erfüllen kann oder nicht. Eine teilweise Erfüllung (das bedeutet, wenn nicht alle Punkte möglich sind) wird als solche bewertet.

A3 - Schnittstelle zum physischen Management Neben den Tätigkeiten aus A1 und A2, die innerhalb des Virtualisierungs-Management-Modells anfallen, gibt es noch Aufgaben, die außerhalb des Modells selbst, in den jeweiligen Management-Domänen selbst erledigt werden müssen. Darunter fällt das Management des externen LAN, der Storage, der Desktops und der Server(-Betriebssysteme).

Die Grenzen des Virtualisierungs-Management-Modells stellen den Übergang zwischen dem Management virtueller und physischer Komponenten dar. Eine Veränderung in der physischen Infrastruktur kann Veränderungen in der virtuellen Infrastruktur nötig machen und umgekehrt. Dies erfordert einen Informationsfluss zwischen dem Management der physischen und der virtuellen Komponenten. Diese Grenze und der erforderliche Informationsfluss stellt eine Fehlerquelle dar, da Änderungen in einem Bereich weitere Anpassungen in anderen Bereichen erforderlich machen. Gerade für einfache Infrastrukturen wäre ein automatisches Anpassen von Konfigurationen wünschenswert, jedoch

müsste diese Funktionalität von einer Management-Plattform übernommen werden, auf die das Virtualisierungs-Management-Modell aufsetzt. Gerade in Rechenzentren ist eine solche automatische Änderung der Einstellungen oft nicht gewünscht, da dabei evtl. über Management-Domänen hinweg Änderungen propagiert werden müssen, die von den verantwortlichen Personen erst überprüft werden müssen. Weiterhin wäre es sicher wünschenswert, wenn die gesamte IT-Infrastruktur mit allen physischen und virtuellen Komponenten mittels eines Management-Tools verwaltet werden könnte. Es muss aber eine Management-Plattform geben, die dies leisten kann. Eine solche Funktionalität ist nicht Teil des Virtualisierungs-Management-Modells und geht über die Aufgabenstellung dieser Arbeit hinaus. Eine andere Möglichkeit wäre, den Management-Domänen Zugang und die entsprechenden Rechte zu dem Virtualisierungs-Management-Modell zu gewähren. Damit könnten die einzelnen Management-Domänen auch die virtuellen Objekte, die logisch gesehen in ihren Aufgabenbereich gehören, verwalten. Diese Möglichkeit lässt sich über das Rollen- und Rechtekonzept realisieren.

Bewertet wird diese Anforderung je nachdem, ob ein Modell diese Aufgaben erfüllen kann oder nicht. Eine teilweise Erfüllung (das bedeutet, wenn nicht alle Punkte möglich sind) wird als solche bewertet.

A4 - Automation Das Stichwort Automation gibt es in diesem Kontext zunächst in zwei Bedeutungen. Automation für den professionellen Nutzer bedeutet hauptsächlich das automatische Ausführen von Aufgaben, die der Nutzer ansonsten von Hand erledigen müsste. Für den nicht-professionellen Nutzer bedeutet Automation die Ausführung von nötigen Aktionen „im Verborgenen“ wobei durch den Nutzer eine Aktion ausgelöst wird, die aus mehreren Einzelaufgaben besteht. Der Nutzer hat jedoch kein Wissen über diese Teilaufgaben und könnte ohne diese Automation die Infrastruktur nicht ohne Probleme verwalten.

- Teilweise automatische Erstellung von virtuellen Maschinen durch Verwendung von Vorlagen. Dabei werden die nötigen Parameter, die die Maschine identifizieren angegeben (z.B. RAM- und CPU-Zuteilung, ...) und mit den festgelegten Parametern der Vorlagen (verwendetes Gastbetriebssystem) kombiniert. Daraus wird automatisch eine virtuelle Maschine mit den gewünschten Parametern erstellt.
- Automatische Erstellung von Backups

Ebenso ist die Dynamik, die in den Szenarien beschrieben wurde, ein Teil der Automation. Geplante Veränderungen in der Infrastruktur, die automatisch stattfinden oder auch automatische Anpassungen an Gegebenheiten innerhalb der Infrastruktur, wie automatische Migration von virtuellen Maschinen zum Lastausgleich oder im Failover-Fall, zählen ebenso dazu.

- Automatische Migration einer virtuellen Maschine bei zu hoher CPU-Last auf einen weniger ausgelasteten Host.
- Automatisches anschalten eines Hosts, wenn er zur Migration oder zum Neustart einer virtuellen Maschine benötigt wird.
- Automatische Migration einer virtuellen Maschine bei zu geringer CPU-Last auf einen weniger ausgelasteten Host. Nachdem von einem Host so die letzte virtuelle Maschine entfernt wurde, kann dieser abgeschaltet werden.

- Automatisches Abschalten und Starten von virtuellen Maschinen zu festgelegten Zeiten.
- Automatische Migration auf andere Hardware, falls die virtuelle Maschine auf der aktuellen nicht mehr ausgeführt werden kann (z.B. durch Defekt der Hardware).

Eine weitere Art von Automation wäre die automatische Reaktion auf Ereignisse, die durch Monitoring festgestellt werden und sich nicht auf das dynamische Verhalten der Infrastruktur wie eben beschrieben beziehen.

- Automatische Aktion auf Ereignisse durch das Monitoring, z.B. Information des Administrators durch Email.

Bewertet wird diese Anforderung je nachdem, ob ein Modell sie erfüllen kann oder nicht.

A5 - Mandantenfähigkeit Verschiedene organisatorische Einheiten (Mandanten, z.B. unterschiedliche Administratoren der Server der unterschiedlichen Abteilungen aus Szenario 2a) müssen in der Lage sein ihre Arbeit ohne Beeinträchtigung anderer Mandanten auszuführen und dürfen selbst auch nicht durch andere beeinträchtigt werden. Die Zuteilung von Nutzern zu Mandanten wird dabei durch das Rollen- und Rechtekonzept (A6) realisiert. Bewertet wird diese Anforderung je nachdem, ob ein Modell sie erfüllen kann oder nicht.

A6 - Rollen- und Rechtekonzept Um Nutzer des Modells mit Berechtigungen auszustatten können ihnen Rollen zugewiesen werden. Diese Rollen sind dann an Berechtigungen für bestimmte Objekte gebunden. Ein Nutzer kann auch mehrere Rollen haben. Zuständigkeitsbereiche lassen sich auch über Rollen abbilden. So kann es beispielsweise eine Rolle für Netz-, eine für Server- und eine für Storage-Administratoren geben. Analog dazu lassen sich nur lesende Rollen zum Monitoring einführen. Die Nutzerverwaltung die für dieses Konzept nötig ist, kann alternativ durch einen Verzeichnisdienst außerhalb der Virtualisierungslösung realisiert sein. Bewertet wird diese Anforderung je nachdem, ob ein Modell sie erfüllen kann oder nicht.

A7 - Transparenz der Virtualisierungslösung Transparenz beschreibt, dass das Virtualisierungs-Management-Modell Details der Technik abstrahiert darstellt. Das dem Management zugrundeliegende, in der Regel recht komplexe Informationsmodell muss auf ein weniger komplexes Managementmodell abgebildet werden. Diese Abstraktion dient hauptsächlich dazu, dass das Managementmodell eines Produkts nicht direkt das jeweilige Informationsmodell widerspiegelt, wodurch für den Nutzer Transparenz erzielt wird, da er nicht mit dem internen Modell konfrontiert wird. So lässt sich Unabhängigkeit in der Präsentation des Managements erzielen, da das Virtualisierungs-Management-Modell in den benutzten Objekten und Konzepten nicht von Technik und Implementierung eines Produktes abhängt. Ist diese Anforderung nicht erfüllt, zeigt das Managementmodell die Technik der Lösung ohne Abstraktion an.

3.2.3 Nichtfunktionale Anforderungen

A8 - Darstellung der Technik Der Detailgrad der Darstellung der zugrundeliegenden Technik soll dem Anwender angemessen sein. Ein nicht-professioneller Anwender soll eine

weniger tiefe Darstellung erhalten, also weniger Informationen und Aktionen angeboten bekommen, als ein professioneller Anwender, der für die Ausschöpfung aller Möglichkeiten Zugang zu allen Informationen und Aktionen braucht. Das bezieht sich auch auf Meldungen, z.B. Fehlermeldungen oder Monitoring-Informationen, die dem Nutzer gezeigt werden. Auch diese müssen soweit angepasst sein, dass die Darstellung den Anforderungen des jeweiligen Nutzers entsprechen. Das bedeutet eine Fehlermeldung informiert über die Ursache des Fehlers auf der Detailebene, auf der der Nutzer arbeitet und bietet, falls möglich, eine Lösung an. Für den Fall des nicht-professionellen Anwenders ist eine nicht-detaillierte Sicht auf die Komponenten der Infrastruktur wie folgt als sinnvoll zu erachten:

Server Eine Darstellung einer virtuellen Maschine soll CPU-Leistung, RAM, die Zugehörigkeit zu einem Netz, die Größe der Festplatte und das zu verwendende Gastbetriebssystem beinhalten. Bei Erstellung einer virtuellen Maschine wird dann automatisch eine solche mit den angegebenen Parametern aus einer Vorlage erzeugt, die bei der Inbetriebnahme der Infrastruktur durch den Hersteller oder eine Servicefirma erstellt wird.

Netz Ein Netz soll nur durch sein Vorhandensein dargestellt werden. Virtuelle Maschinen sollen zwar die Möglichkeit haben daran angeschlossen zu werden, aber mehr Möglichkeiten als das Anlegen und das Löschen eines Netzes werden nicht benötigt. Die Realisierung der Netze wird über virtuelle Switches und VLANs durchgeführt, die vom System automatisch konfiguriert werden. Ein Netz aus Sicht des Nutzers ist dabei ein VLAN.

Die Komponenten *Server* und *Netz* sind dabei virtuelle Objekte. *Storage* wird hier nicht mit aufgeführt, da die Festplatte eines Servers schon in dessen Beschreibung enthalten ist. Damit arbeitet der nicht-professionelle Nutzer mit Konzepten der Hardware-Welt, von denen angenommen wird, dass er sie kennt und versteht, da er, wie in Szenario 1a beschrieben, eine kleine IT-Infrastruktur betreut.

Dieser Punkt beschreibt allgemein gesagt, wie alle Aspekte der Anforderungen aus A1 und A2 für den jeweiligen Nutzertyp angeboten werden. Der professionelle Nutzer hat die detaillierte Sicht auf der Ebene, wie sie in den zwei Anforderungen (A1 und A2) beschrieben sind. Der nicht-professionelle Nutzer bekommt eine vereinfachte, wenig detaillierte Sicht der Infrastruktur geboten, wie sie in dieser Anforderung beschrieben ist. Bewertet wird diese Anforderung je nachdem, ob ein Modell sie erfüllt, oder nicht.

Es gibt noch weitere, jedoch allgemeinere nichtfunktionale Anforderungen an ein Virtualisierungs-Management-Modell. Die folgenden Anforderungen sind zwar auch Anforderungen an das Modell, jedoch sind sie nur schwer messbar. Eine angemessene Bewertung dieser Anforderungen würde z.B. aufwändige Nutzerstudien notwendig machen, die den Rahmen dieser Arbeit sprengen würden. Deswegen werden sie angeführt, aber bei der Bewertung der bestehenden Modelle nicht beachtet.

Das Modell soll eine möglichst gute *Benutzbarkeit (Usability)* aufweisen. Das bedeutet unter anderem, es soll eine übersichtliche Darstellung anbieten, die leicht verständlich und leicht zu erlernen ist. Die Arbeit mit dem Modell soll effizient sein, das bedeutet, die Aufgaben, die ein Nutzer gewöhnlich ausführt, sollen schnell durchführbar sein. Eine andere Anforderung ist die *Skalierbarkeit*. Das bedeutet, das Modell soll sowohl für kleine (z.B. Szenario 1a), als auch für große Infrastrukturen (z.B. hunderte virtueller Maschinen und virtueller Netze)

einsetzbar sein. Eine weitere nichtfunktionale Anforderung ist die *Erweiterbarkeit* des Virtualisierungs-Management-Modells. Es soll möglich sein, neue Techniken oder Konzepte in das Modell aufzunehmen. Dadurch soll erreicht werden, dass das Modell auch durch neue Entwicklungen nicht veraltet und auf lange Sicht einsetzbar bleibt.

Weitere nichtfunktionale Anforderungen werden hier nicht aufgestellt, da sie für das Virtualisierungs-Management-Modell, das entwickelt wird nicht gelten, weil es sich um ein abstraktes Modell ohne Implementierung handelt. Daher fallen häufige ([Stö05, S. 132f]) Anforderungen wie Übertragbarkeit auf andere Plattformen (Portability), Interoperabilität, Leistungsverhalten, Antwortzeiten, Fehlerrate, etc. weg. Eine ausführliche Sammlung weiterer nichtfunktionaler Anforderungen findet sich bei [Wika].

3.3 Zusammenfassung

In diesem Kapitel wurden die Szenarien, die mit den bestehenden Modellen umgesetzt werden sollen um diese zu testen, beschrieben. Dabei wurde beschrieben was die Infrastrukturen der Szenarien zu leisten haben und wie ihr physikalischer Rahmen auszusehen hat. Anschließend wurden die Anforderungen an ein Virtualisierungs-Management-Modell aufgestellt und beschrieben.

4 Umsetzung der Szenarien in den Modellen

In diesem Kapitel wird untersucht, wie die in Kapitel 3 beschriebenen Szenarien mittels der in Kapitel 2 vorgestellten Modelle umsetzbar sind. Damit die abstrakten Beschreibungen der Szenarien zunächst noch konkreter werden, wird neben den virtuellen Umsetzungen auch noch eine „klassische“ Umsetzung direkt auf Hardware beschrieben. Diese direkte Implementierung steht dann zum Vergleich mit den virtualisierten Implementierungen zur Verfügung. Bei den Beschreibungen der Umsetzung wird erläutert, welche Schritte nötig sind und in welcher Form sich die Gegebenheiten der Szenarien nachbilden lassen, bzw. ob es Probleme bei der Umsetzung gibt. Dabei ist die Grundkonfiguration der Virtualisierungslösungen schon vorausgesetzt. Es wird also von einem einsatzfähigen Virtualisierungssystem ausgegangen. Diese Einschränkung wird gemacht, da die Installation einer Virtualisierungslösung in aller Regel über zusätzliche Tools geschieht und insofern nichts mit dem Management der Infrastruktur, also des Modells des Produkts, zu tun hat. Die Umsetzung der Szenarien mit den zu testenden Modellen liefert Informationen darüber, ob und wie gut, oder wie einfach sich die Szenarien umsetzen lassen, oder ob sich Szenarien oder einzelne Aspekte davon nicht umsetzen lassen. Dieses Vorgehen dient einerseits dazu, dass eine Basis geschaffen wird, aufgrund derer sich die unterschiedlichen Modelle vergleichen lassen. Andererseits werden so weitere Informationen gesammelt, welche Modelle welche Fähigkeiten haben. Diese Informationen können später bei der Erstellung eines generischen Modells berücksichtigt werden, um ein möglichst brauchbares Modell zu erschaffen. Nach der Beschreibung der Umsetzung wird die jeweilige Realisierung anhand der Anforderungen aus Abschnitt 3.2 bewertet.

Es wird in den Abschnitten 4.1 bis 4.4 jedes Szenario mit den fünf Modellen (die vier Modelle aus Kapitel 2 plus die klassische Variante) umgesetzt. Die Beschreibung der Umsetzung beinhaltet eine Beschreibung der Struktur der Infrastruktur, des zugrundeliegenden Informationsmodells im Vergleich mit dem vorliegenden Managementmodell, eine Auflistung der Tätigkeiten, die in dem Szenario mit diesem Modell anfallen, sowie einer Zusammenfassung und einer Bewertung anhand der Anforderungen. Jedoch wird diese gesamte Beschreibung mit dem Augenmerk auf die Netze durchgeführt und der Vergleich der Informations- und der Managementmodelle beschränkt sich ausschließlich auf diesen Punkt. Bei der Bewertung wird die Erfüllung mit *gut (+)*, *ausreichend (o)* oder *schlecht (-)* bewertet, je nach dem, ob ein Modell für das Szenario geeignet ist. Es wird hier abweichend von der Bewertung aus Abschnitt 3.2 bewertet, da für jedes Szenario überprüft werden soll, welches Modell sich wie gut dafür eignet und das ist mit der dort beschriebenen Bewertung nicht sinnvoll. Nachdem die Szenarien fertig umgesetzt sind, folgt in Abschnitt 4.5 eine generelle Bewertung der Modelle. Hierbei wird die in Abschnitt 3.2 beschriebene Bewertung mit *erfüllt*, *teilweise erfüllt* und *nicht erfüllt* durchgeführt, da hier das gesamte Modell bewertet wird und nicht wie tauglich ein Modell für ein Szenario ist.

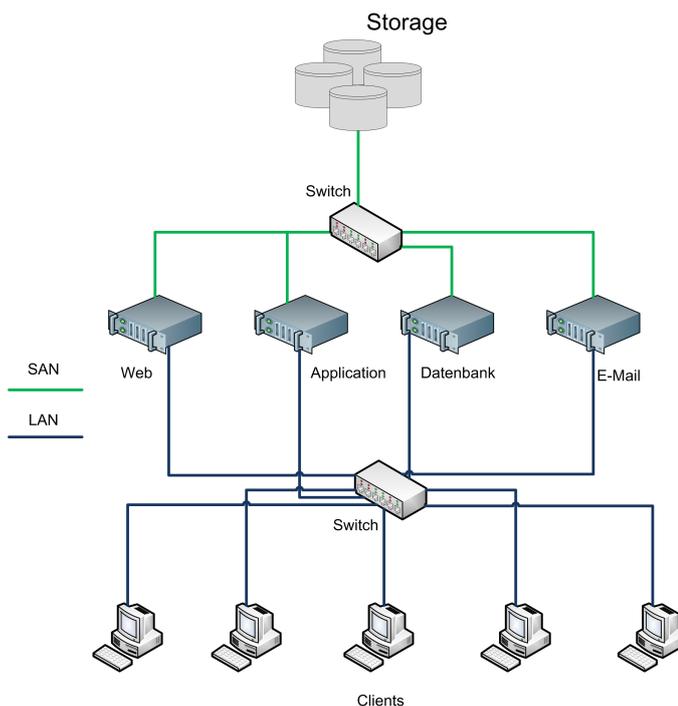


Abbildung 4.1: Szenario 1a Ohne Virtualisierung

4.1 Szenario 1a

Dieses Szenario wurde in Abschnitt 3.1.1 beschrieben. Es handelt sich um eine kleine Infrastruktur in einem kleinen Unternehmen. Im folgenden wird dargestellt wie sich das Szenario mit den einzelnen Techniken und ohne Virtualisierung modellieren lässt.

4.1.1 Ohne Virtualisierung

Für die Nachbildung dieses Szenarios ohne Virtualisierung werden vier Hardware-Server benötigt. Das Datennetz zwischen den Client-PCs der Anwender und den Servern wird über ein lokales Ethernet realisiert. Für das Netz ist ein Switch nötig, der die Rechner des Netzes miteinander verbindet. Für den Anschluss der Storage wird ein SAN auf Basis von FC (Fibre Channel) eingesetzt. Nachdem die nötige Hardware zusammengefasst ist, wird der Aufbau der Infrastruktur, der in Abbildung 4.1 zu sehen ist, beschrieben. Auf jedem der Server wird ein Betriebssystem installiert und jeweils einer der benötigten Software-Server. In jedem Betriebssystem muss noch der Zugang zum Netz und der Anschluss der Storage konfiguriert werden. Es wird also auf einem Server ein Webserver installiert, auf dem nächsten ein Applicationserver, auf dem dritten ein Datenbankserver und auf dem letzten die Software für einen Emailserver. Damit wären die Dienste, die in dem Szenario benötigt werden, zur Verfügung gestellt. Der Wechsel der Geschäftsanwendung bei Nacht wird durch ein Skript gesteuert, das auf dem Server, auf dem der Applicationserver installiert ist, liegt und zu festgelegten Zeiten ausgeführt wird. Dieses Skript fährt eine Konfiguration des Applicationsservers herunter und startet eine andere. Die Konfigurationen sind jeweils so, dass die Erste die tagsüber verwendete Auftragsbearbeitung und die Zweite die Anwendung für die Rech-

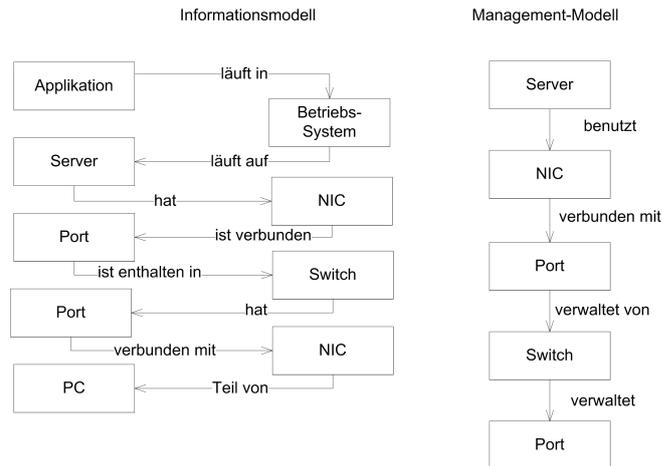


Abbildung 4.2: Informations- und Managementmodell ohne Virtualisierung für Szenario 1a

nungserstellung bereitstellt. Alle Rechner werden über den Switch miteinander verbunden. Das Management dieser Infrastruktur wird in einer sehr einfachen Form durchgeführt. Es gibt keine Managementserver oder professionellen Managementplattformen. Der Mitarbeiter, der die Infrastruktur verwaltet, arbeitet zur Verwaltung der Desktops entweder remote oder direkt auf den Rechnern. Zur Verwaltung der Server greift er über das Netz auf die Server zu. Nur in besonderen Fällen, wie der Installation des Betriebssystems der Server, oder bei Fehlern, die eine Administration über das Netz verhindern, greift er direkt auf die Server zu. Der Ethernet-Switch wird genau wie der FC-Switch über die integrierte Managementoberfläche verwaltet.

Modelle

In Abbildung 4.2 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung ohne Virtualisierung vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Das Informationsmodell umfasst die Elemente angefangen bei den Applikationen, die in Betriebssystemen laufen, über den physischen Server, der über die physische NIC den Netzverkehr verarbeitet. Die NIC ist über einen Port mit einem Switch verbunden, der über einen anderen Port mit der NIC eines PCs verbunden ist. Das Managementmodell ohne Virtualisierung hat im Bezug auf Netze dieselben Komponenten wie das Informationsmodell. Hier gibt es den Server, der die NIC benutzt. Die NIC ist mit einem Port des Switches verbunden. Am Switch befindet sich noch einen weiteren Port, der zu verwalten ist. Es findet eine direkte 1:1 Abbildung zwischen dem Managementmodell und dem Informationsmodell statt.

Arbeitsschritte

- Konfiguration
 - Netz
 - Storage

- Server Starten
- Softwareinstallation
 - Betriebssystem
 - Anwendungen
- Betrieb
 - Logs überprüfen
 - Fehler beheben

Zusammenfassung

Das Management dieses Aufbaus erfordert viele einzelne Schritte, da es keinen zentralen Management-Server gibt. Für jede Aktion muss eine Verbindung oder ein Zugang zu dem entsprechenden System hergestellt werden, das heißt, es gibt viele sich wiederholende Schritte, die bei jedem System notwendig sind. Das Management der Server ist auf das Management der Betriebssysteme und der Applikationen beschränkt. Beim Management der Desktops wird der jeweilige Rechner über die Administrationsmöglichkeiten des Betriebssystems verwaltet. Das Management der Switches wird über in den Geräten integrierte Managementmöglichkeiten durchgeführt. Die Netzkonfiguration erfolgt durch Einstellungen an den einzelnen Systemen sowie an den Switches. Es wird für jedes Teil der Infrastruktur ein gesondertes Management durchgeführt. Dieses Vorgehen ist sehr aufwändig und fehleranfällig. Bei auftretenden Fehlern ist es notwendig, den Fehler zu suchen, die Ursache zu finden und diese zu beheben. Es existieren keine Mechanismen, die den Administrator dabei unterstützen.

Bewertung

- A1 - Aufbau** Die Erstellung einer virtuellen Infrastruktur ohne Virtualisierung ist nicht möglich.
- A2 - Betrieb** Der Betrieb einer virtuellen Infrastruktur ohne Virtualisierung ist nicht möglich.
- A3 - Schnittstelle zum physischen Management** Da es nur das physische Management und kein Virtualisierungs-Management-Modell gibt, existiert keine Schnittstelle zum physischen Management.
- A4 - Automation** Es steht keine Automation zur Verfügung.
- A5 - Mandantenfähigkeit** Das System ist nicht mandantenfähig, was sich aber in diesem Szenario nicht nachteilig auswirkt.
- A6 - Rollen- und Rechtekonzept** Einzelne Tools bieten eigene Möglichkeiten zur Nutzerverwaltung. Es gibt jedoch keine integrierte Lösung mit Rollen und Rechten. Für das Szenario ist das ausreichend, aber unkomfortabel.
- A7 - Transparenz der Virtualisierungslösung** Das Managementmodell entspricht dem Informationsmodell. Das Netz-Management wird nicht transparent gestaltet.
- A8 - Darstellung der Technik** Die Darstellung der Technik ist in den Tools eine direkte Abbildung der verwendeten Technik. Deshalb ist es für das Szenario schlecht geeignet.

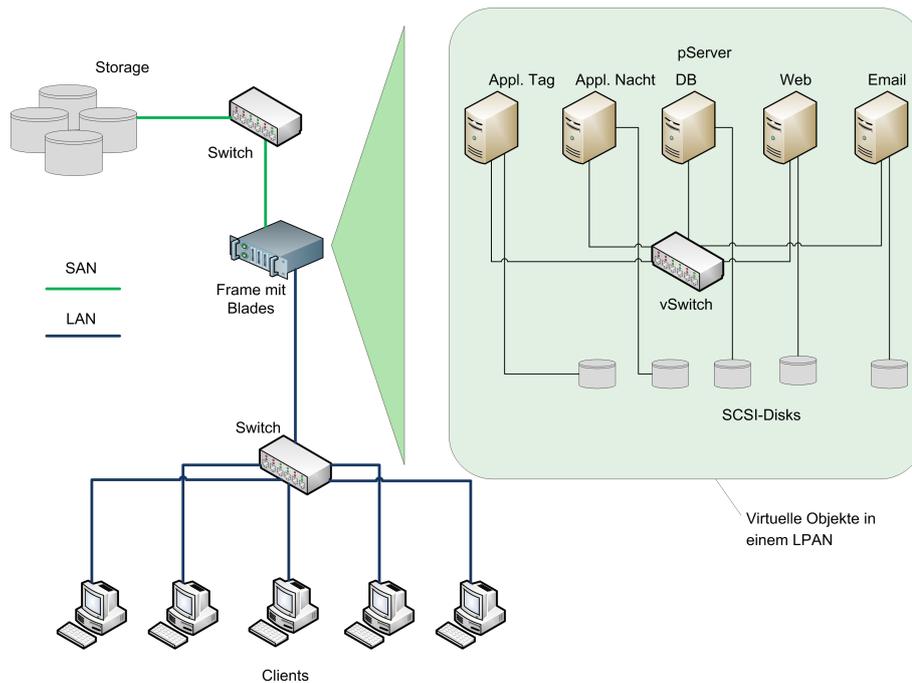


Abbildung 4.3: Szenario 1a mit PAN

4.1.2 PAN

Um dieses Szenario in PAN umzusetzen, reicht ein LPAN¹ aus. In diesem LPAN existieren fünf pServer. Einer davon stellt den Webserver bereit. Zwei weitere stellen zwei Applicationserver bereit, von denen einer tagsüber, der andere in der Nacht laufen sollen. Die beiden verbleibenden pServer sind für den Datenbank- und den Emailserver gedacht. Benötigte Ressourcen sind ein pBlade, auf dem fünf vBlades eingerichtet sind, fünf SCSI-Disks für die Speicherung der Betriebssysteme und Anwendungen, die über SAN verfügbar sind und ein vSwitch, der über ein rEth einen Uplink in das angeschlossene Netz hat. Zunächst muss ein LPAN erstellt werden, dem die nötigen Ressourcen (vBlades, Disks und vSwitch) zugeteilt werden. Als nächstes werden fünf pServer angelegt. Anschließend werden in der Ansicht des pServers die entsprechenden Ressourcen dem jeweiligen pServer zugewiesen. Die Zuteilung wird wie folgt durchgeführt: Ein pServer erhält jeweils ein vBlade als Primär-Blade und eine Festplatte zugewiesen. Beide Ressourcen-Typen werden den pServern dabei exklusiv zugewiesen. Die pServer bekommen über ihre vEth den vSwitches zugewiesen, über den sie per rEth mit dem physischen Switch verbunden werden. Auf den unterschiedlichen Festplatten wird dasselbe Betriebssystem installiert und auf den beiden Tag/Nacht-Disks gleich konfiguriert. Der einzige Unterschied sind die Anwendungen, die den Wechsel des Software-Stacks in diesem Szenario notwendig machen. Eine Disk enthält die eine Menge von Anwendungen, die andere Disk die andere Menge von Anwendungen. Auf diese Weise kann der Wechsel des Software-Stacks durch das alternierende Booten der beiden pServern erreicht werden. Auf den weiteren Festplatten wird entsprechend die nötige Software installiert und konfiguriert. Als Boot-Image der pServer kann das standardmäßig vorhandene EVBS benutzt werden,

¹Für eine Erklärung der hier gebrauchten PAN-spezifischen Namen und Bezeichnungen siehe Kapitel 2.1

4 Umsetzung der Szenarien in den Modellen

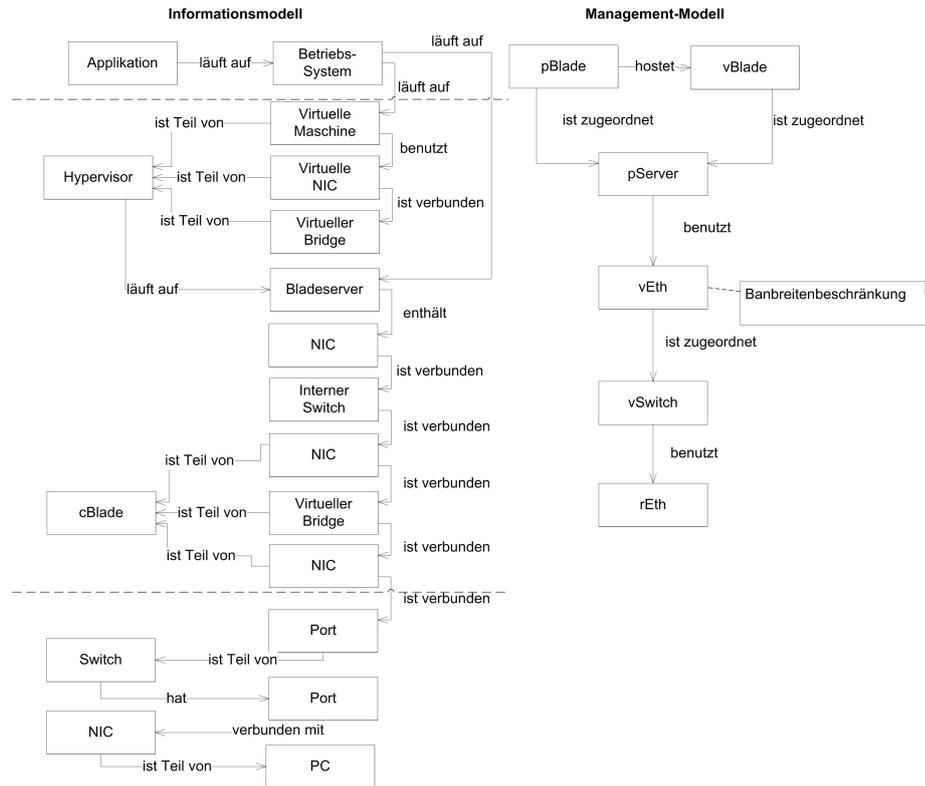


Abbildung 4.4: Informations- und Managementmodell bei PAN für Szenario 1a

das von allen angeschlossenen Medien booten kann, sofern diese bootfähig sind. In Abbildung 4.3 ist der Aufbau abgebildet. Ein automatischer, z.B. zeitlich vorgegebener Wechsel der pServer, ist bei PAN an sich nicht möglich. Jedoch ist es möglich, den Wechsel über ein Skript per CLI durchzuführen. Dieses Skript müsste von einem externen System aus ausgeführt werden (evtl. ließe sich das auch als cron-Job auf den cBlades ausführen, auf denen eine Linuxinstallation läuft). Das Management erfolgt entweder von einem Rechner aus, der über das Netz mit dem PAN verbunden ist, oder direkt am Frame über einen KVM-Switch (Keyboard, Video, Mouse).

Modelle

In Abbildung 4.4 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit PAN vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Im Informationsmodell sind die folgenden Elemente enthalten: Eine Applikation läuft auf einem Betriebssystem, das auf einer virtuellen Maschine oder direkt auf dem Bladeserver läuft. Ob das Betriebssystem auf einer virtuellen Maschine oder auf der Hardware betrieben wird, ist abhängig von der Art des pServers (siehe weiter unten in diesem Abschnitt bei der Beschreibung der Abbildung vom Managementmodell auf das Informationsmodell). Die virtuelle Maschine benutzt eine virtuelle NIC, die mit einer virtuellen Bridge verbunden ist. Die drei virtuellen Komponenten werden durch den Hypervisor verwaltet. Der Hypervisor läuft wiederum auf einem Bladeserver, der über seine NIC

den internen Switch benutzt. Über den internen Switch findet die Kommunikation mit dem cBlade statt. Dabei läuft Datenverkehr vom internen Switch über eine NIC des cBlades. Diese ist wiederum mit einer virtuellen Bridge verbunden, die über eine weitere NIC die Verbindung nach außen anbietet. Diese NIC ist mit dem Port eines Switches verbunden, der über einen weiteren Port mit der NIC eines PCs verbunden ist. Es werden nur die Teile des Informationsmodells von PAN gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. PAN kann zwar auch Applikationen auf Linux-Gastsystemen verwalten, aber da hier speziell auf das Netz-Management eingegangen wird, ist dieser Teil ausgenommen. Das Managementmodell von PAN wurde schon in Abschnitt 2.1.2 erläutert. An dieser Stelle soll darauf eingegangen werden, wie das Managementmodell auf das Informationsmodell abgebildet wird. Die Abbildung des pServers ist abhängig von der Art des Blades, auf dem er gebootet ist. Die Abbildung ist eine andere, je nachdem, ob der pServer auf einem pBlade oder einem vBlade gebootet ist. Ist er auf einem pBlade gebootet, wird er auf einen Bladeserver abgebildet. In diesem Fall ist die vEth die NIC des Bladeservers. Ist der pServer auf einem vBlade gebootet, wird er auf eine virtuelle Maschine abgebildet und seine vEth auf die virtuelle NIC. In beiden Fällen kann an der vEth eine Bandbreitenbeschränkung eingerichtet werden. Ein vSwitch wird auf den internen Switch sowie die interne NIC des cBlades abgebildet. Die rEth wird auf die virtuelle Bridge des cBlades und deren externe NIC abgebildet.

Arbeitsschritte

- LPAN anlegen
- vSwitch anlegen und konfigurieren
- LPAN Ressourcen zuteilen
- pServer erstellen und konfigurieren (Verwendung des vSwitch)
- pServer starten
- Betriebssysteme und Applikationen installieren und konfigurieren
- Ereignisse auf Fehler prüfen
- Fehler lokalisieren und beheben

Zusammenfassung

Der Aufbau der GUI des PAN-Managers wurde schon in Abschnitt 2.1.3 beschrieben. Sie bietet damit eine recht übersichtliche Möglichkeit zur Verwaltung eines PAN an. Ein wesentlicher Vorteil ist, dass fast das gesamte Management der Infrastruktur über ein Tool erledigt werden kann. Es gibt nur wenige Aufgaben, die nicht über den PAN-Manager erledigt werden können. So muss das Management der auf den pServern installierten Betriebssysteme und der darin installierten Anwendungen über Mittel durchgeführt werden, die von ihnen selbst bereitgestellt werden. PAN bietet zwar die Möglichkeit, in Linuxsystemen installierte Anwendungen zu steuern (Starten, Beenden), aber die restliche Verwaltung muss extern durchgeführt werden. Eine andere Aufgabe, die mit PAN nicht erledigt werden kann, ist das Backup der pServer oder der angeschlossenen Medien allgemein. Der in PAN integrierte

Backup-Mechanismus kann nur das PAN selbst, also die Daten über die Infrastruktur und nicht die Daten in der Infrastruktur sichern. Dafür müssen externe Lösungen verwendet werden. Bei der Verwaltung der externen Hardware (Switches, Storage Arrays) muss ebenfalls auf die Managementlösung der Geräte zurückgegriffen werden.

Bewertung

- A1 - Aufbau** Mit PAN können die nötigen virtuellen Netze und virtuellen Maschinen mit Festplatten aus dem SAN erstellt werden.
- A2 - Betrieb** PAN beherrscht das Management der virtuellen Infrastruktur mit Ausnahme der in Abschnitt 4.5.2 aufgeführten Punkte.
- A3 - Schnittstelle zum physischen Management** Eine Schnittstelle zum physischen Management ist nicht vorhanden.
- A4 - Automation** Automation ist nur für das automatische Failover für einzelne pServer vorhanden. Das nötige Abschalten und Starten von pServern muss über externe Skripten durchgeführt werden.
- A5 - Mandantenfähigkeit** Das System ist mandantenfähig. Diese Fähigkeit wird in diesem Szenario aber nicht ausgenutzt.
- A6 - Rollen- und Rechtekonzept** Die Rollen und Rechte, die bei PAN vergeben werden können, sind für dieses Szenario nicht von Bedeutung, da nur ein Nutzer als Administrator tätig ist.
- A7 - Transparenz der Virtualisierungslösung** PAN ist als Virtualisierung für den Nutzer im Netz-Management transparent. Insbesondere wird ein interner Switch im Frame transparent gemanagt.
- A8 - Darstellung der Technik** Die Darstellung des Systems ist eine Präsentation des komplexen logischen Modells von PAN. Daher ist sie für dieses Szenario nicht geeignet.

4.1.3 VMware

Für dieses Szenario benötigt man einen Hardware Server als ESX Server Host, sowie einen Server für den Virtual Center Server. Zunächst wird ein Data Center angelegt, dem der ESX Server hinzugefügt wird. Auf dem ESX Server wird ein Netz an einem vSwitch angelegt, das als Uplink eine physikalische NIC des Hosts bekommt. Nun wird für die fünf nötigen Server jeweils eine virtuelle Festplatte auf dem Datastore angelegt. Als nächstes werden fünf virtuelle Maschinen angelegt und mit dem Netz und den entsprechenden virtuellen Festplatten verbunden. Im Anschluss können die VMs gestartet und die Betriebssysteme installiert werden. Der beschriebene Aufbau ist schematisch in Abbildung 4.5 zu sehen.

Der zeitgesteuerte Wechsel des Applicationsservers lässt sich mit VMware auf zwei Arten realisieren. Einerseits gibt es die Möglichkeit 'Scheduled Tasks', also zeitlich geplante Aufgaben, anzulegen, die dann das Starten und Stoppen der entsprechenden Maschine übernehmen. Andererseits ist es, wie bei den anderen Produkten auch hier möglich, den Wechsel über Skripte zu steuern, die zu den festgelegten Zeiten auszuführen sind.

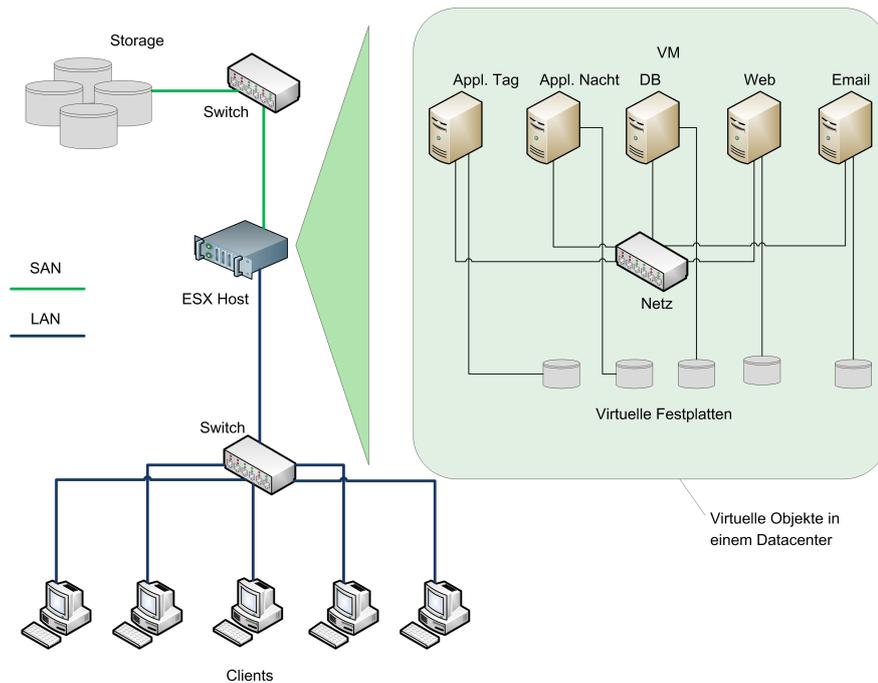


Abbildung 4.5: Szenario 1a mit VMware

Modelle

In Abbildung 4.6 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit VMware vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management der Netze in VMware arbeitet. Es werden nur die Teile des Informationsmodells von VMware gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. Das Informationsmodell umfasst die Applikationen, die in Betriebssystemen laufen, die virtuellen Maschinen, die über eine virtuelle NIC an einem virtuellen Port an einen virtuellen Switch angeschlossen sind. Dieser virtuelle Switch leitet Netzverkehr über den verwaltenden Hypervisor an den physischen Host, der ihn an die physische NIC übergibt. Die NIC ist über einen Port mit einem externen Switch verbunden, der über einen weiteren Port die Verbindung zur NIC eines PCs herstellt. Bei der Abbildung des Managementmodells auf das Informationsmodell wird wie folgt vorgegangen: Die virtuelle Maschine des Managementmodells wird auf die virtuelle Maschine des Informationsmodells abgebildet. Analog wird mit der virtuellen NIC vorgegangen. Die Portgruppe wird auf virtuelle Ports abgebildet und der vSwitch auf den virtuellen Switch. Die NIC schließlich wird auf die NIC des Hosts abgebildet.

Arbeitsschritte

- Data Center anlegen
- vSwitch anlegen
- Portgruppe anlegen
- Storage definieren

4 Umsetzung der Szenarien in den Modellen

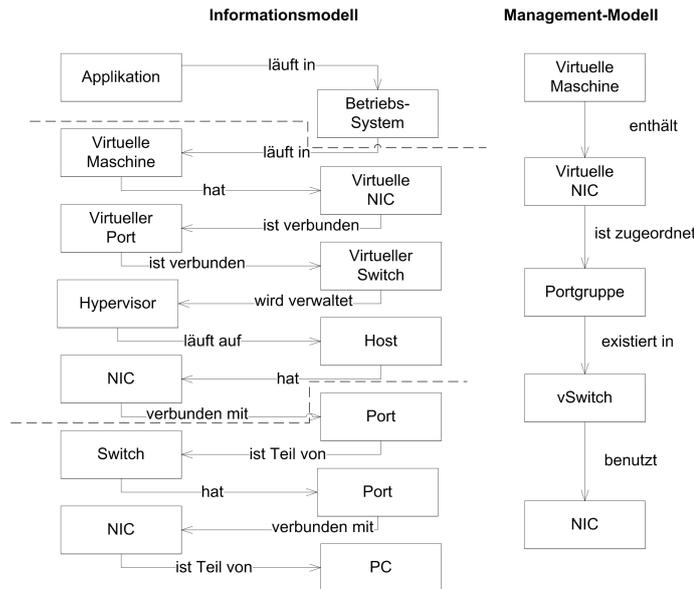


Abbildung 4.6: Informations- und Managementmodell von Szenario 1a mit VMware

- ESX Server Host zuweisen
- Virtuelle Maschine erstellen
- Virtuelle Maschine Portgruppe zuweisen
- Virtuelle Maschine booten
- Logs auf Fehler überprüfen
- Fehler lokalisieren und beheben

Zusammenfassung

Mit dem Virtual Center steht eine Management-Plattform bereit, mit der alle Aufgaben, die die virtualisierte Infrastruktur betreffen, zu erledigen sind. Man kann die gesamte virtuelle Infrastruktur aus Servern und Netzen steuern. Es gibt auch die Möglichkeit, über ein Zusatzprodukt ein zentral gesteuertes Backup der Hosts und der VMs durchzuführen. Einzig die Bereiche, die nicht direkt die Virtualisierung betreffen, also in diesem Fall die Server-, Netz-, Storage- und Desktopadministration können nicht über Virtual Center gesteuert werden. Hier bleiben die üblichen Schnittpunkte bestehen, die auch meist durch Grenzen organisatorischer Aufgabenbereiche existieren.

Besonders positiv fällt auf, dass es möglich ist, virtuelle Maschinen zeitlich geplant zu starten und zu stoppen, wodurch sich der Wechsel der Anwendungen in diesem Szenario realisieren lässt.

Bewertung

A1 - Aufbau Die Erstellung von virtuellen Maschinen, die Definition von virtuellen Festplatten und virtuellen Netzen sind durchführbar. Darüber hinaus können Vorlagen zur

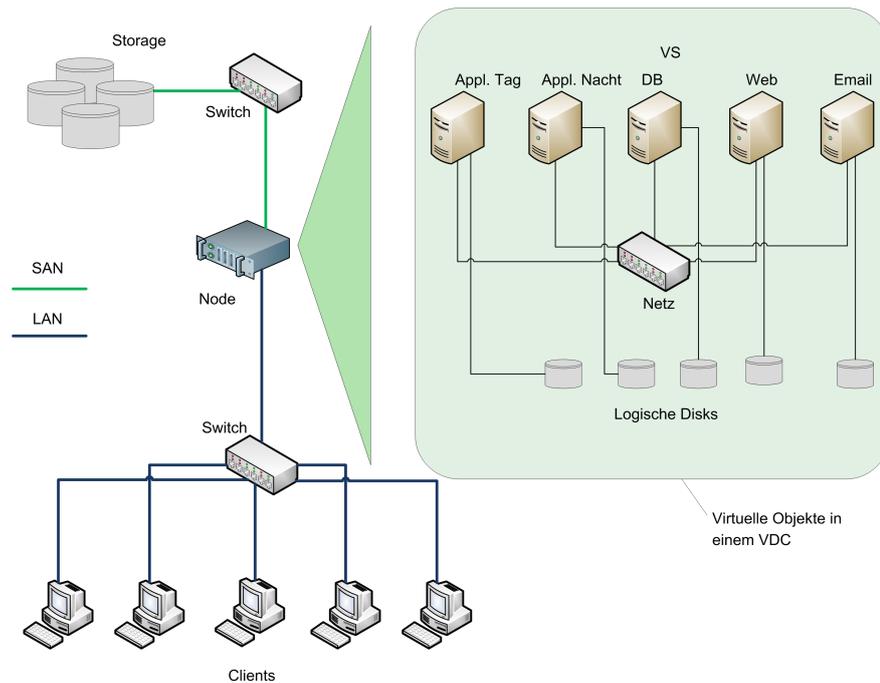


Abbildung 4.7: Szenario 1a mit VI

Erstellung virtueller Maschinen verwendet werden.

- A2 - Betrieb** Mit den Einschränkungen aus Abschnitt 4.5.3 kann die Infrastruktur betrieben werden.
- A3 - Schnittstelle zum physischen Management** Es gibt keine Schnittstelle zum physischen Management.
- A4 - Automation** Automation kann bei der Erstellung der virtuellen Maschinen mit Vorlagen eingesetzt werden. Das Starten und Stoppen der virtuellen Maschinen kann ebenfalls mit Virtual Center durchgeführt werden.
- A5 - Mandantenfähigkeit** Dieses Szenario benötigt keine Mandantenfähigkeit.
- A6 - Rollen- und Rechtekonzept** Für das Szenario sind keine Rollen und Rechte nötig.
- A7 - Transparenz der Virtualisierungslösung** Das Managementmodell schafft Transparenz in der Verwendung. Es wird mit vereinfachten Konzepten gearbeitet, die die Arbeit erleichtern.
- A8 - Darstellung der Technik** Die Darstellung ist eine Repräsentation des logischen Modells und für dieses Szenario nicht gut geeignet.

4.1.4 Virtual Iron

Eine schematische Darstellung des gesamten Aufbaus ist in Abbildung 4.7 zu sehen. Zunächst wird ein Netz eingerichtet, über das der Anschluss an das LAN erfolgt. Anschließend wird ein

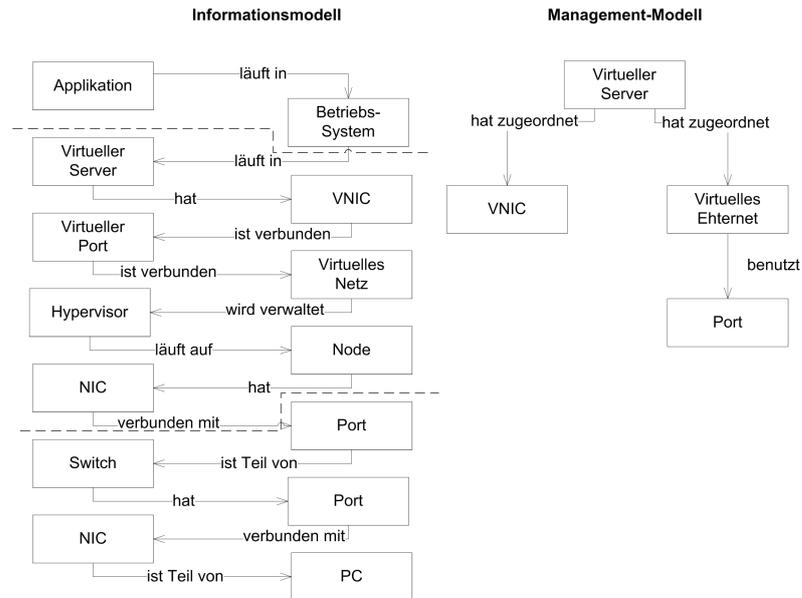


Abbildung 4.8: Informations- und Managementmodell bei Virtual Iron für Szenario 1a

Virtual Data Center (VDC) für dieses Szenario angelegt. Diesem VDC wird der vorhandene Node zugewiesen. In dem ausgewählten VDC werden dann die nötigen logischen Platten angelegt. Dazu wird eine Disk Group erstellt, innerhalb derer die logischen Partitionen angelegt werden. Es werden für dieses Szenario fünf logische Partitionen angelegt, für jeden der fünf benötigten Server eine. Anschließend wird noch für jeden der benötigten Server ein VS auf dem Node erstellt. Dabei wird die entsprechende logische Disk und das entsprechende Netz mit der entsprechenden VNIC angegeben. Es muss auch noch angegeben werden, welches der unterstützten Betriebssysteme auf dem Server laufen wird und von welchem Medium gebootet werden soll. Anschließend wird ausgewählt wieviel Prozessorleistung und RAM der VS bekommt. Danach können die VS gestartet und die entsprechenden Betriebssysteme installiert werden. Nach der Installation kann es nochmals nötig werden, das Boot-Gerät eines VS neu zu bestimmen.

Auch Virtual Iron besitzt keinen Mechanismus zum zeitgesteuerten Starten oder Herunterfahren eines VS, wie es für den Wechsel der Anwendung in diesem Szenario benötigt wird, auch wenn es die Möglichkeit über eine Policy bietet ein oder mehrere VDC zu rebooten. Jedoch kann auch hier über ein externes Skript dieses Ziel erreicht werden. Das Skript kann dann z.B. von dem Management-Server aus über einen cron-Job zeitgesteuert ausgeführt werden.

Modelle

In Abbildung 4.8 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit Virtual Iron vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Es werden nur die Teile des Informationsmodells von Virtual Iron gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. Das Informationsmodell besteht aus den Komponenten Applikationen, Betriebssystem, virtueller

Server, VNIC, virtueller Port, virtuelles Netz, Hypervisor, Node, NIC, Port, Switch, Port, NIC und PC. Diese Komponenten benutzen jeweils die auf sie folgende. Das Managementmodell von Virtual Iron wurde in Abschnitt 2.3.2 erläutert. Die Elemente des Managementmodells werden folgendermaßen auf das Informationsmodell abgebildet: Der Virtuelle Server wird auf die virtuelle Maschine des Informationsmodells abgebildet. Die virtuelle NIC wird analog dazu auf die virtuelle NIC abgebildet. Das virtuelle Netz wird auf das virtuelle Netz des Informationsmodells abgebildet. Der Port des Managementmodells wird auf die NIC des Informationsmodells abgebildet. Im Managementmodell gibt es keine direkte Verbindung zwischen der virtuellen NIC und dem Port, eine solche wird aber über den virtuellen Server hergestellt. Im Informationsmodell besteht jedoch eine mittelbare Beziehung der korrespondierenden Komponenten, wodurch auch hier die Verbindung hergestellt wird.

Arbeitsschritte

- VNICs anlegen
- Netz anlegen
- Virtual Data Center anlegen
- Node zuweisen
- Logische Platten erstellen
- Virtual Server erstellen (dabei VNIC und Netz zuweisen)
- Virtual Server booten
- Logs auf Fehler überprüfen

Zusammenfassung

Die Aufgaben, die innerhalb des VI-Centers ausgeführt werden können, sind übersichtlich und thematisch gut gruppiert durchzuführen. Egal, ob ein Server erstellt oder eine Festplatte angelegt werden soll, der Nutzer hat fast immer direkte Wege, um zu seinem Ziel zu kommen. Es ist auch möglich, sehr viele Aufgaben innerhalb des VI-Centers durchzuführen. Es gibt die Möglichkeit die Nodes zu steuern und Storage zu verwalten. Leider ist es nicht direkt möglich, ein Backup der Platteninhalte anzulegen. Die Backup-Funktion von Virtual Iron ermöglicht das Anlegen mehrerer Backups der Infrastruktur, also der Daten, die mit dem VI-Center verwaltet werden. Ein Backup der Platten der Server ist nicht direkt, sondern nur über den Umweg der Erstellung eines Snapshots möglich. Die Verwaltung der Betriebssysteme ist über eine Virtuelle Server Konsole möglich. Die Administration des LAN ist nicht möglich und auch die Administration des SAN kann nur soweit durchgeführt werden, wie es die Erstellung der logischen Disks betrifft. Alle weiteren administrativen Schritte das SAN betreffend müssen mit externen Möglichkeiten durchgeführt werden. Auch die Desktop-Rechner der Mitarbeiter müssen wieder extra gemanagt werden.

Bewertung

- A1 - Aufbau** Die virtuelle Infrastruktur kann vollständig angelegt werden.
- A2 - Betrieb** Der Betrieb der Infrastruktur ist mit den Einschränkungen aus Abschnitt 4.5.4 möglich.
- A3 - Schnittstelle zum physischen Management** Es gibt keine Schnittstelle zum physischen Management.
- A4 - Automation** Automation ist für die Erstellung von virtuellen Servern mittels Vorlagen eingeschränkt möglich. Das automatische Starten und Stoppen ist jedoch nicht möglich.
- A5 - Mandantenfähigkeit** VI ist nur bedingt mandantenfähig, aber das ist für dieses Szenario auch nicht nötig.
- A6 - Rollen- und Rechtekonzept** Virtual Iron hat kein Rechte- und Rollenkonzept; das ist aber für das Szenario auch nicht nötig.
- A7 - Transparenz der Virtualisierungslösung** Das Netz-Management ist bei Virtual Iron für den Nutzer transparent. Es wird ein virtuelles Netz verwendet, dessen Umsetzung für den Nutzer nicht ersichtlich ist.
- A8 - Darstellung der Technik** Die Darstellung der Technik spiegelt das logische Konzept von VI wieder und ist für das Szenario deswegen nicht geeignet.

4.1.5 VIOM

Für die Umsetzung dieses Szenarios mit VIOM muss ein Frame mit fünf Blades eingesetzt werden. Es wird an dieser Stelle vorausgesetzt, dass das entsprechende Frame schon mit VIOM gemanagt wird, also dass es unter dem Punkt 'VIOM Managed' im VIOM Manager aufgeführt ist. Für die Verbindung nach außen muss zunächst ein Netzwerk (also ein Uplink Set) angelegt werden, über das die Blades mit dem lokalen Netz kommunizieren können. Es wäre möglich, für jedes Blade ein einzelnes Netzwerk anzulegen, so dass auch eine physikalische Verbindung für jedes Blade in das LAN notwendig wird. Aus Gründen der Einfachheit und Übersichtlichkeit wird nur ein einziges Netzwerk für das gesamte Frame angelegt, da nicht zu erwarten ist, dass es zu Engpässen in der Netzkapazität kommt. Es wird auf dem ersten IBP (das auf der rechten Seite angezeigt wird!) ein neues Netzwerk vom Typ 'Single Network'² erstellt und die Ports ausgewählt, die mit dem LAN verbunden sind. Als nächstes müssen die Profile angelegt werden. Dabei wird pro Profil das Netzwerk ausgewählt, mit dem das Profil verbunden werden soll. Hier können auch die Werte für das SAN (WWPN (World Wide Port Name und LUN des Ziels) eingetragen werden. Es muss für jedes Blade ein eigenes Profil erstellt werden, da hier gleich die Zuordnung zu den Boot-Images der Server durchgeführt wird. Nun wird noch die Zuordnung der Profile zu den Blades durchgeführt. Abbildung 4.9 zeigt schematisch den Aufbau des Szenarios.

VIOM bietet an sich keine Möglichkeit zeitgesteuert ein Blade herunterzufahren oder ein anderes zu starten. Man kann sich hier behelfen, indem man, wie bei PAN auch, ein Skript zeitgesteuert ausführt, das ein Blade per CLI herunterfährt und ein anderes bootet. Die

²Für eine Beschreibung der einzelnen Optionen siehe Abschnitt 2.4.3

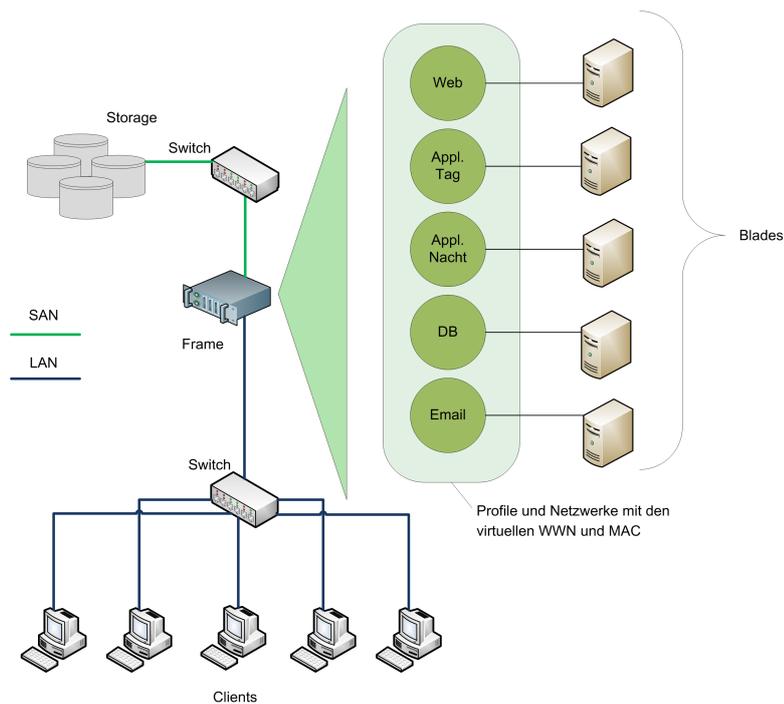


Abbildung 4.9: Szenario 1a Mit VIOM

ServerView Suite, in die VIOM integriert ist, bietet auch die Möglichkeit, Blades zeitgesteuert zu starten und zu stoppen. Jedoch ist dies nicht direkt ein Teil des VIOM-Managements.

Die weiteren Teile der Infrastruktur wie SAN, LAN, Client-Desktops, lassen sich nicht über VIOM steuern. Es kann also nur ein recht kleiner Teil des Szenarios nachgebildet werden.

Modelle

In Abbildung 4.10 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit VIOM vorhanden sind. Es werden nur die Teile des Informationsmodells von VIOM gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. VIOM kennt im Informationsmodell die Applikationen, das Betriebssystem, das Blade mit einer NIC, der Slot, in dem das Blade montiert ist, der Port des Slots, das Chassis, dessen Teil der Slot ist, das IBP, das Teil des Chassis ist, die darin enthaltenen Uplink-Ports, der Port am externen Switch, der Switch selbst, ein weiterer Port und die NIC des PCs und der PC selbst. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Nun wird die Abbildung der Elemente des Managementmodells auf die des Informationsmodells beschrieben. Das Chassis wird auf das Chassis und ein Server auf ein Blade abgebildet. Der Slot wird direkt auf einen Slot abgebildet. Das Profil wird auf eine Menge der Ports eines Slots im Informationsmodell abgebildet. Ein Port des Managementmodells wird auf einen Port eines Slots im Informationsmodell abgebildet. Nun wird ein Uplink-Set auf eine Menge von Ports des IBP abgebildet. Ein Netz ist eine Menge bestehend aus Ports der Slots (also der Abbildung eines Profils) und Ports des IBP (der Abbildung eines Uplink-Sets). Ein einzelner Uplink-Port wird auf einen Port des IBP abgebildet.

4 Umsetzung der Szenarien in den Modellen

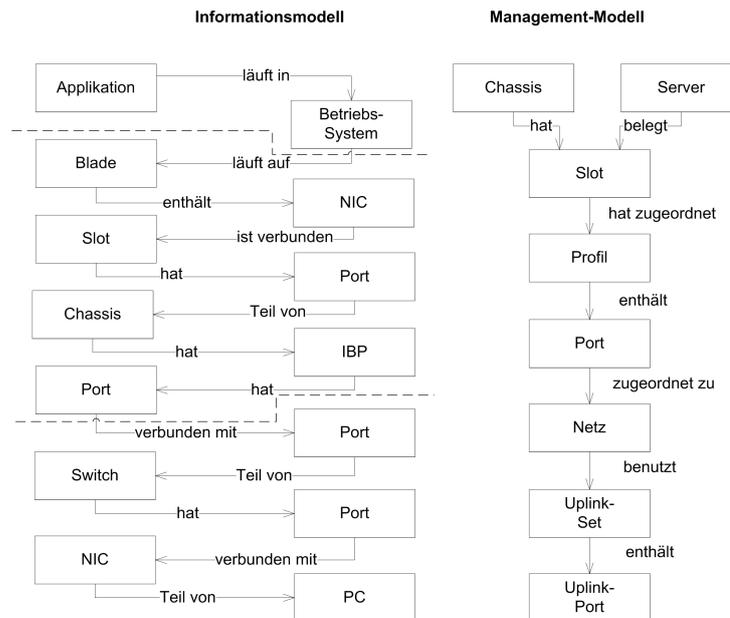


Abbildung 4.10: Informations- und Management-Modell bei VIOM für Szenario 1a

Arbeitsschritte

- Anlegen und Konfigurieren eines Netzes
- Anlegen und Konfigurieren der Profile
- Zuweisen der Profile an Slots
- Booten der Blades
- Neuzeuweisen eines Profils an einen anderen Slot im Fehlerfall

Zusammenfassung

Der VIOM Manager selbst bietet eine gute Möglichkeit, ein Frame mit I/O-Virtualisierung zu managen. Leider ist VIOM dadurch nur ein kleiner Teil des gesamten Szenarios und bietet keine Möglichkeiten für anderweitige Administrationsaufgaben. Dafür muss entweder die ServerView Suite, von der VIOM ein Teil ist, eingesetzt werden oder es muss auf andere Möglichkeiten zurück gegriffen werden.

Bewertung

- A1 - Aufbau** Das Erstellen der Infrastruktur ist möglich, jedoch nur mit physischen Komponenten und virtuellen Adressen und Pfadschaltungen.
- A2 - Betrieb** Der Betrieb der Infrastruktur ist im Rahmen der in Abschnitt 4.5.5 genannten Möglichkeiten durchführbar.

- A3 - Schnittstelle zum physischen Management** VIOM bietet keine Schnittstelle zu Teilen der externen Infrastruktur außerhalb des Frames. Jedoch kann die ServerView Suite, in die VIOM eingebettet ist, diese Aufgabe erfüllen.
- A4 - Automation** Automation ist nicht direkt, sondern nur über externe Skripten oder die ServerView Suite möglich.
- A5 - Mandantenfähigkeit** Das System ist nur eingeschränkt mandantenfähig, was aber auch nicht für das System nötig ist.
- A6 - Rollen- und Rechtekonzept** VIOM bietet kein Rollen- und Rechtekonzept.
- A7 - Transparenz der Virtualisierungslösung** Das Netz-Management von VIOM findet transparent statt.
- A8 - Darstellung der Technik** Die Darstellung der Technik spiegelt direkt VIOMs logische Struktur wieder und ist für das Szenario nicht geeignet.

4.1.6 Bewertung für das Szenario 1a

Modell	A1	A2	A3	A4	A5	A6	A7	A8
ohne Virt.	-	-	-	-	-	-	-	-
PAN	+	o	-	-	o	o	+	-
VMware	+	o	-	+	o	o	+	-
Virtual Iron	+	o	-	-	o	-	+	-
VIOM	o	o	-	-	o	-	+	-

+ : gut o : ausreichend - : schlecht

Tabelle 4.1: Bewertung der Virtualisierungs-Management-Modelle für Szenario 1a

In Tabelle 4.1 ist dargestellt, wie die einzelnen Virtualisierungs-Managementmodelle für die Gegebenheiten des Szenarios bewertet werden. Die Umsetzung ohne Virtualisierung fällt in allen Punkten durch. Alle anderen haben Probleme bei einer angemessenen Darstellung der Technik und der Schnittstelle zum physischen Management. Insgesamt schneidet VMware am besten ab, da es die nötige Dynamik des Szenarios von Haus aus unterstützt, während die anderen Modelle damit Schwierigkeiten haben.

4.2 Szenario 1b

Dieses Szenario stellt eine Erweiterung des Szenarios 1a dar. Dabei gibt es mehrere Infrastrukturen wie in Szenario 1a, die räumlich verteilt in Standorten des Unternehmens sind. Die einzelnen Standorte haben autark funktionierende Infrastrukturen, die ihre Daten mit der Zentrale abgleichen. Das Management der verteilten Infrastrukturen wird von der Zentrale aus durch einen professionellen Administrator durchgeführt. Eine genauere Beschreibung des Szenarios findet sich in Abschnitt 3.1.2. Im folgenden wird erläutert, wie sich dieses Szenario mit und ohne die Virtualisierungslösungen, die in dieser Arbeit betrachtet werden, in die Realität umsetzen lässt.

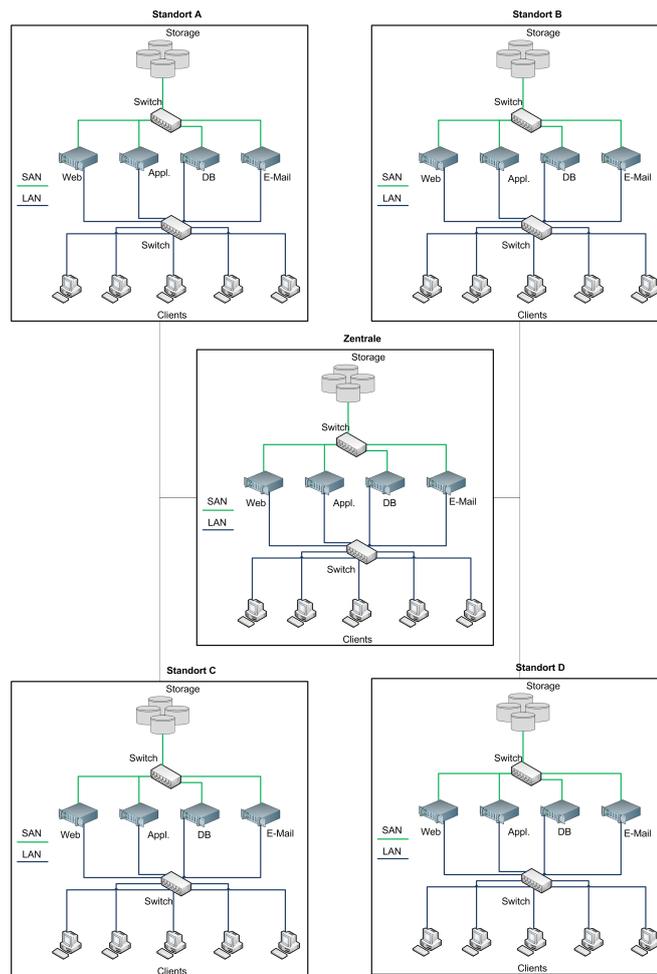


Abbildung 4.11: Szenario 1b Ohne Virtualisierung

4.2.1 Ohne Virtualisierung

Der Aufbau der einzelnen Systeme in den Standorten ist identisch mit dem, der in Abschnitt 4.1.1 beschrieben wurde. Anders als in Szenario 1a sind die einzelnen Standorte mit der Zentrale verbunden und werden von dort aus gemanagt (siehe Abbildung 4.11). Um die Verbindung eines Standortes nach außen zu realisieren, muss noch ein Router eingesetzt werden. Ein weiterer Unterschied ist, dass der Wechsel der Geschäftsanwendung nicht stattfindet. Der Administrator hat seinen Arbeitsplatz in der Zentrale und verbindet sich über ein VPN mit den einzelnen Standorten, um diese über das Netz zu managen.

Modelle

In Abbildung 4.12 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung ohne Virtualisierung vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Das Informationsmodell umfasst die Elemente angefangen bei den Applikationen, die in Betriebssystemen laufen, über den physischen Server,

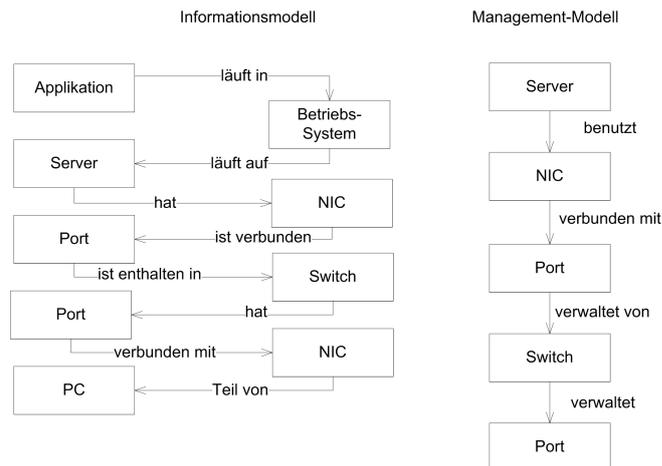


Abbildung 4.12: Informations- und Managementmodell ohne Virtualisierung für Szenario 1b

der über die physische NIC den Netzverkehr verarbeitet. Die NIC ist über einen Port mit einem Switch verbunden, der über einen anderen Port mit der NIC eines PCs verbunden ist. Das Managementmodell ohne Virtualisierung hat im Bezug auf Netze dieselben Komponenten wie das Informationsmodell. Hier gibt es den Server, der die NIC benutzt. Die NIC ist mit einem Port des Switches verbunden. Der Switch hat noch einen weiteren Port. Es findet eine direkte 1:1 Abbildung zwischen dem Managementmodell und dem Informationsmodell statt.

Arbeitsschritte

- Konfiguration
 - Netz
 - Storage
- Server Starten
- Softwareinstallation
 - Betriebssystem
 - Anwendungen
- Betrieb
 - Logs überprüfen
 - Fehler beheben

Zusammenfassung

Das Management in diesem Fall stellt sich analog zu dem von Szenario 1a dar, wie es in Abschnitt 4.1.1 beschrieben ist. Um die Verbindung eines Standortes nach außen durchzuführen, ist in jedem Standort noch ein Router nötig, der ebenfalls über die mitgelieferte Managementschnittstelle verwaltet wird. Die wesentliche Änderung in diesem Szenario ist,

dass der Zugriff auf die einzelnen Standorte remote erfolgt. Daraus folgt, dass ein Ausfall der Konnektivität eines Standortes zur Folge hat, dass der Administrator nicht mehr darauf zugreifen kann, da das Management in-band erfolgt. In einem solchen Fall muss er sich entweder selbst zu dem Standort begeben, um den Fehler zu beheben oder er kann jemanden aus dem Standort so instruieren, dass das Problem behoben wird. Ansonsten sind es aus Sicht des Administrators in jedem Standort exakt die selben Voraussetzungen wie bei Szenario 1a.

Bewertung

- A1 - Aufbau** Es ist nicht möglich ohne Virtualisierung eine virtuelle Infrastruktur zu erstellen.
- A2 - Betrieb** Ohne Virtualisierung kann keine virtuelle Infrastruktur betrieben werden.
- A3 - Schnittstelle zum physischen Management** Das gesamte Management wird über das physische Management durchgeführt. Es gibt keine Schnittstelle zu einem Virtualisierungs-Management-Modell.
- A4 - Automation** Dynamik wird in diesem Szenario nicht benötigt. Andere Formen der Automation werden ebenfalls nicht angeboten.
- A5 - Mandantenfähigkeit** Das System muss für das Szenario nicht mandantenfähig sein.
- A6 - Rollen- und Rechtekonzept** Es gibt keine integrierte Nutzerverwaltung mit Rollen und Rechten. Eine solche wird aber für das Szenario nicht benötigt.
- A7 - Transparenz der Virtualisierungslösung** Das Managementmodell entspricht dem Informationsmodell. Das Netz-Management wird nicht transparent gestaltet.
- A8 - Darstellung der Technik** Die Darstellung der Technik ist ausschließlich eine direkte Abbildung der Technik und damit für das Szenario angemessen.

4.2.2 PAN

Für dieses Szenario muss in jedem der räumlich verteilten Standorte ein eigenes PAN eingerichtet werden. Das bedeutet, es muss zunächst ein Frame konfiguriert und darauf ein PAN mit allen nötigen Einstellungen eingerichtet werden. Dann wird dort ein LPAN erstellt, das weitestgehend dem Aufbau des LPAN in Szenario 1a (siehe Abschnitt 4.1.2) entspricht. Da in diesem Fall kein automatischer Wechsel der Geschäftsanwendung nötig ist, kommt das LPAN mit nur vier pServern für Web-, Application-, Datenbank- und Emailserver aus. Der weitere Aufbau bleibt derselbe wie in Abschnitt 4.1.2 beschrieben. Das Management der Systeme der einzelnen Standorte erfolgt von einer zentralen Stelle aus. Dabei kann per Browser auf die Management-Webanwendung zugegriffen werden, die auf den jeweiligen Systemen laufen. Ein Zusammenschluss der einzelnen PANs ist dabei nicht möglich. Es muss also jedes PAN einzeln verwaltet werden. Jedoch kann die fertiggestellte Konfiguration eines Standortes gespeichert und auf die anderen Systeme übertragen werden. Der gesamte Aufbau ist schematisch in Abbildung 4.13 dargestellt.

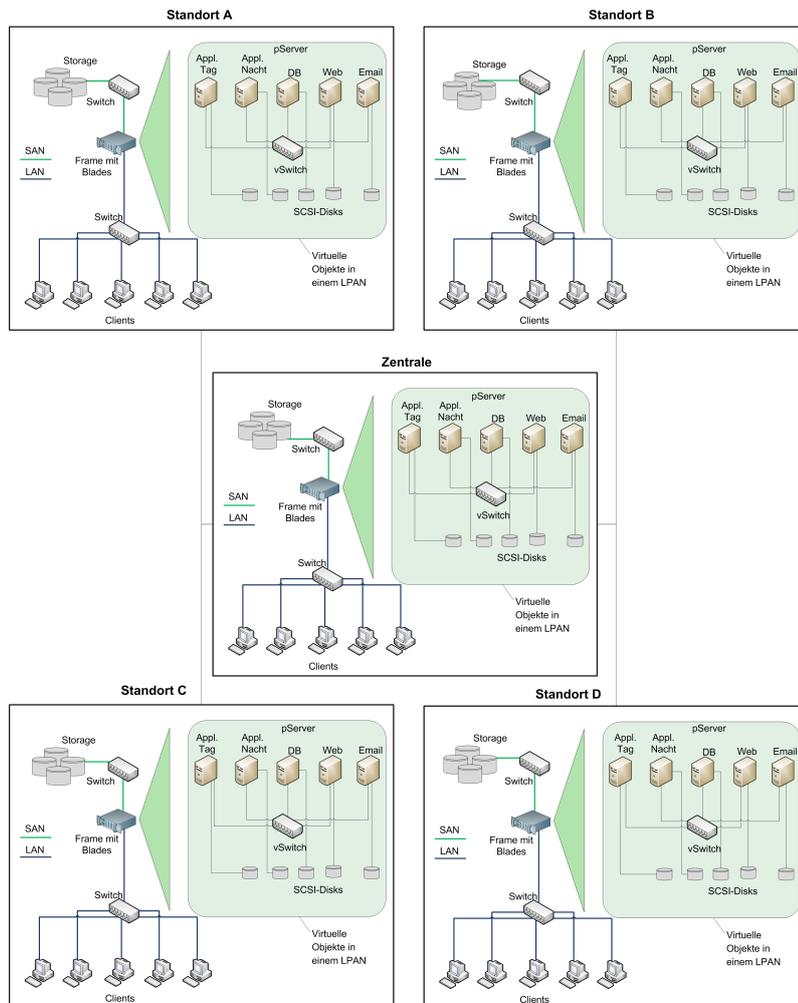


Abbildung 4.13: Szenario 1b mit PAN

4 Umsetzung der Szenarien in den Modellen

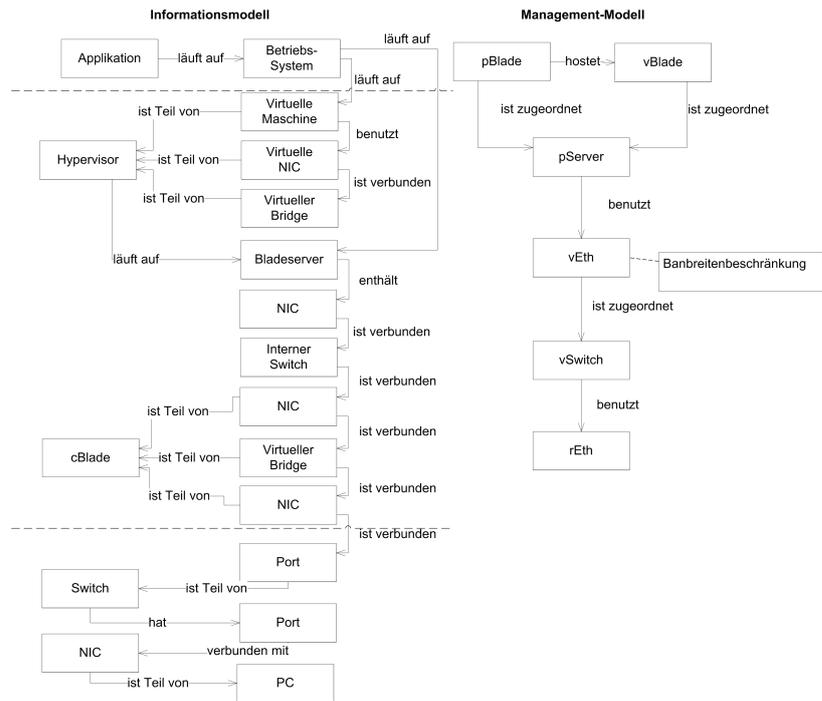


Abbildung 4.14: Informations- und Managementmodell bei PAN für Szenario 1b

Modelle

In Abbildung 4.14 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit PAN vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Im Informationsmodell sind die folgenden Elemente enthalten: Eine Applikation läuft auf einem Betriebssystem, das auf einer virtuellen Maschine oder direkt auf dem Bladeserver läuft. Ob das Betriebssystem auf einer virtuellen Maschine oder auf der Hardware betrieben wird, ist abhängig von der Art des pServers (siehe weiter unten in diesem Abschnitt bei der Beschreibung der Abbildung vom Managementmodell auf das Informationsmodell). Die virtuelle Maschine benutzt eine virtuelle NIC, die mit einer virtuellen Bridge verbunden ist. Die drei virtuellen Komponenten werden durch den Hypervisor verwaltet. Der Hypervisor läuft wiederum auf einem Bladeserver, der über seine NIC den internen Switch benutzt. Über den internen Switch findet die Kommunikation mit dem cBlade statt. Dabei läuft Datenverkehr vom internen Switch über eine NIC des cBlades. Diese ist wiederum mit einer virtuellen Bridge verbunden, die über eine weitere NIC die Verbindung nach außen anbietet. Diese NIC ist mit dem Port eines Switches verbunden, der über einen weiteren Port mit der NIC eines PCs verbunden ist. Es werden nur die Teile des Informationsmodells von PAN gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. PAN kann zwar auch Applikationen auf Linux Gastsystemen verwalten, aber da hier speziell auf das Netz-Management eingegangen wird, ist dieser Teil ausgenommen. Das Managementmodell von PAN wurde schon in Abschnitt 2.1.2 erläutert. An dieser Stelle soll darauf eingegangen werden, wie das Managementmodell auf das Informationsmodell abgebildet wird. Die Abbildung des pServers ist abhängig von der Art des Blades, auf dem

er gebootet ist. Die Abbildung ist eine andere je nachdem, ob der pServer auf einem pBlade oder einem vBlade gebootet ist. Ist er auf einem pBlade gebootet, wird er auf einen Bladeserver abgebildet. In diesem Fall ist die vEth die NIC des Bladeservers. Ist der pServer auf einem vBlade gebootet, wird er auf die Virtuelle Maschine abgebildet und seine vEth auf die virtuelle NIC. In beiden Fällen kann an der vEth eine Bandbreitenbeschränkung eingerichtet werden. Ein vSwitch wird abgebildet auf den internen Switch sowie die interne NIC des cBlades. Die rEth wird auf die virtuelle Bridge des cBlades und deren externe NIC abgebildet.

Arbeitsschritte

- LPAN anlegen
- vSwitch anlegen und konfigurieren
- LPAN Ressourcen zuteilen
- pServer erstellen und konfigurieren (Verwendung des vSwitch)
- pServer starten
- Betriebssysteme und Applikationen installieren und konfigurieren
- Ereignisse auf Fehler prüfen
- Fehler lokalisieren und beheben

Zusammenfassung

Wie auch im vorherigen Szenario ist hier die in PAN integrierte Management-Anwendung, der PAN-Manager, eine große Erleichterung. Die gesamte Hardware-Infrastruktur lässt sich damit verwalten und es wird nur für die Verwaltung externer Geräte wie z.B. Switches, die eine Anbindung des PAN an das lokale Netz realisieren, eine externe Lösung benötigt. Ebenso ist das Management der Betriebssysteme und Anwendungen und das Management der Backups nicht über den PAN-Manager möglich. Die Steuerung der einzelnen Standorte stellt jedoch keine große Hürde dar. Durch Zugriff auf das lokale Netz der Standorte hat der Administrator die Möglichkeit, das lokale PAN zu verwalten.

Bewertung

A1 - Aufbau Der Aufbau der Infrastrukturen ist möglich.

A2 - Betrieb Der Betrieb ist mit den Einschränkungen aus Abschnitt 4.5.2 möglich.

A3 - Schnittstelle zum physischen Management PAN stellt keine Schnittstelle zum physischen Management bereit.

A4 - Automation Für das Szenario ist keine Dynamik nötig. PAN bietet nur Automation für den Failover-Fall.

A5 - Mandantenfähigkeit Das Szenario erfordert keine Mandantenfähigkeit.

4 Umsetzung der Szenarien in den Modellen

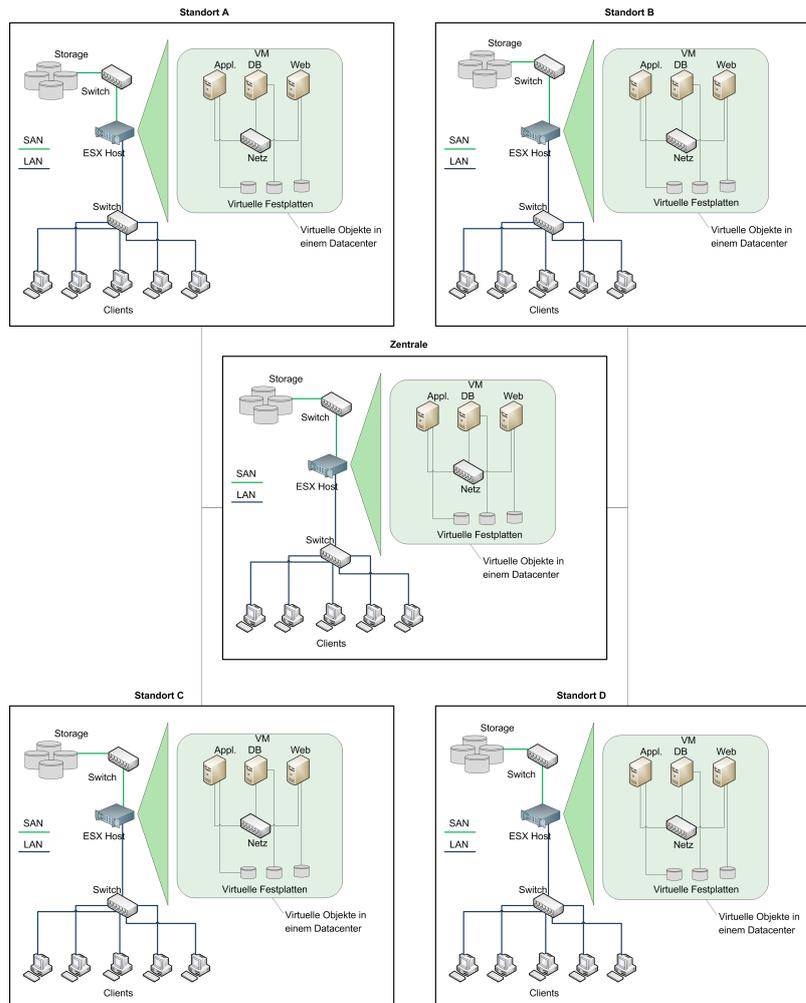


Abbildung 4.15: Szenario 1b mit VMware

A6 - Rollen- und Rechtekonzept Ein Rollen- und Rechtesystem ist für das Szenario nicht nötig.

A7 - Transparenz der Virtualisierungslösung PAN ist als Virtualisierung für den Nutzer im Netzmanagement transparent. Insbesondere wird ein interner Frame transparent verwaltet.

A8 - Darstellung der Technik Die Darstellung des logischen Konzepts von PAN ist für das Szenario angemessen.

4.2.3 VMware

In jedem der fünf Standorte ist, wie in Abbildung 4.15 zu sehen, jeweils ein Server vorhanden, auf dem der ESX-Server installiert wird. In der Zentrale ist zusätzlich noch die Hardware für den Virtual Center Server mit der installierten Software vorhanden. Für jeden der Standorte wird ein Data Center eingerichtet, denen die entsprechenden ESX Server zugeordnet werden.

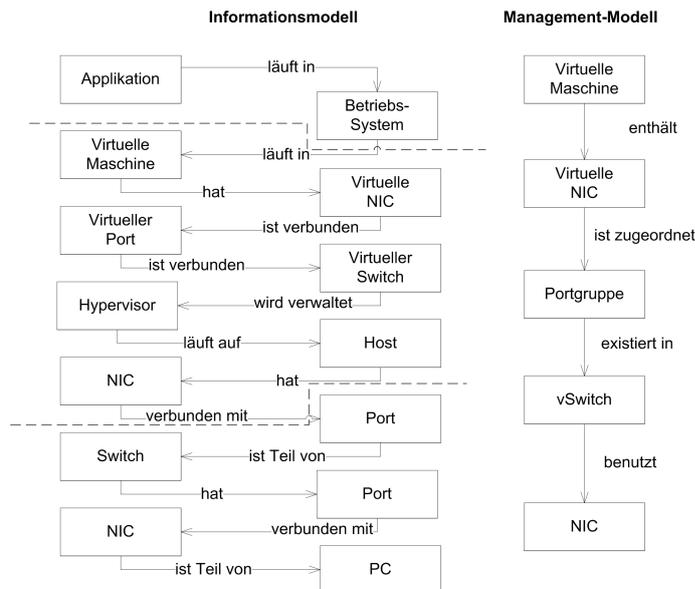


Abbildung 4.16: Informations- und Managementmodell von Szenario 1b mit VMware

Danach kann mit der Einrichtung der Strukturen der einzelnen Standorte begonnen werden, die analog zu der aus Szenario 1a abläuft (siehe Abschnitt 4.1.3), jedoch sind in diesem Szenario nur vier virtuelle Festplatten und vier virtuelle Maschinen nötig. Dazu werden die nötigen Netze und Festplatten angelegt und die Virtuellen Maschinen erstellt. Das gesamte Management der einzelnen Systeme wird über den, in der Zentrale vorhandenen, Virtual Center Server durchgeführt.

Modelle

In Abbildung 4.16 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit VMware vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management der Netze in VMware arbeitet. Es werden nur die Teile des Informationsmodells von VMware gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. Das Informationsmodell umfasst die Applikationen, die in Betriebssystemen laufen, über die virtuellen Maschinen, die über eine virtuelle NIC an einem virtuellen Port an einen virtuellen Switch angeschlossen sind. Dieser virtuelle Switch leitet Netzverkehr über den verwaltenden Hypervisor an den physischen Host, der ihn an die physische NIC übergibt. Die NIC ist über eine Port mit einem externen Switch verbunden, der über einen weiteren Port die Verbindung zur NIC eines PCs herstellt. Bei der Abbildung des Managementmodell auf das Informationsmodell wird wie folgt vorgegangen: Die virtuelle Maschine des Managementmodell wird auf die virtuelle Maschine des Informationsmodell abgebildet. Analog wird mit der virtuellen NIC vorgegangen. Die Portgruppe wird auf virtuelle Ports abgebildet und der vSwitch auf den virtuellen Switch. Die NIC schließlich wird auf die NIC des Hosts abgebildet.

Arbeitsschritte

- Data Center anlegen

4 Umsetzung der Szenarien in den Modellen

- vSwitch anlegen
- Portgruppe anlegen
- Storage definieren
- ESX Server Host zuweisen
- Virtuelle Maschine erstellen
- Virtuelle Maschine Portgruppe zuweisen
- Virtuelle Maschine booten
- Logs auf Fehler überprüfen
- Fehler lokalisieren und beheben

Zusammenfassung

Wie auch im vorhergehenden Szenario lassen sich alle Aufgaben, die die virtuelle Infrastruktur allein betreffen, mit Virtual Center erledigen. Teile der gesamten Infrastruktur, die nicht virtualisiert sind, also Desktops und Netze, müssen allerdings auch hier mit den entsprechenden Management-Tools verwaltet werden. Der zentrale Management-Server in Gestalt des Virtual Center-Servers kann hier das Management entscheidend vereinfachen. Zum Beispiel lassen sich in allen Standorten VMs aus den selben Vorlagen erstellen, so dass die Installation des Betriebssystems und der Anwendungen im Gegensatz zum herkömmlichen Aufbau drastisch vereinfacht wird.

Bewertung

- A1 - Aufbau** Die Infrastrukturen lassen sich mit allen Anforderungen erstellen.
- A2 - Betrieb** Mit den Beschränkungen aus Abschnitt 4.5.3 lässt sich die Infrastruktur betreiben.
- A3 - Schnittstelle zum physischen Management** Virtual Center bietet keine Schnittstelle zum physischen Management.
- A4 - Automation** Da das Szenario statisch ist, wird Automation nur in Teilen benötigt. Hier kann Virtual Center volle Unterstützung geben.
- A5 - Mandantenfähigkeit** Das Szenario erfordert keine Mandantenfähigkeit.
- A6 - Rollen- und Rechtenkonzept** Durch das Szenario ist kein Rechte- und Rollensystem notwendig.
- A7 - Transparenz der Virtualisierungslösung** Das Managementmodell schafft Transparenz in der Verwendung. Es wird mit Konzepten gearbeitet, die die Arbeit erleichtern.
- A8 - Darstellung der Technik** Die Darstellung der Technik als Widerspiegelung des logischen Modells ist für das Szenario angemessen.

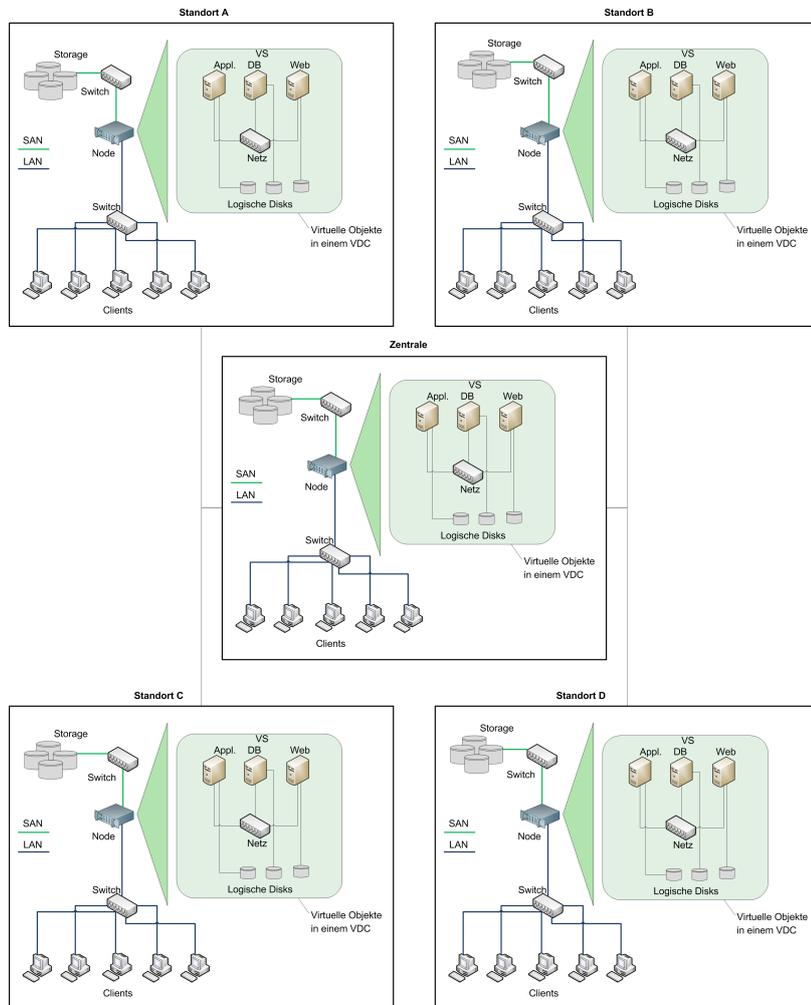


Abbildung 4.17: Szenario 1b mit VI

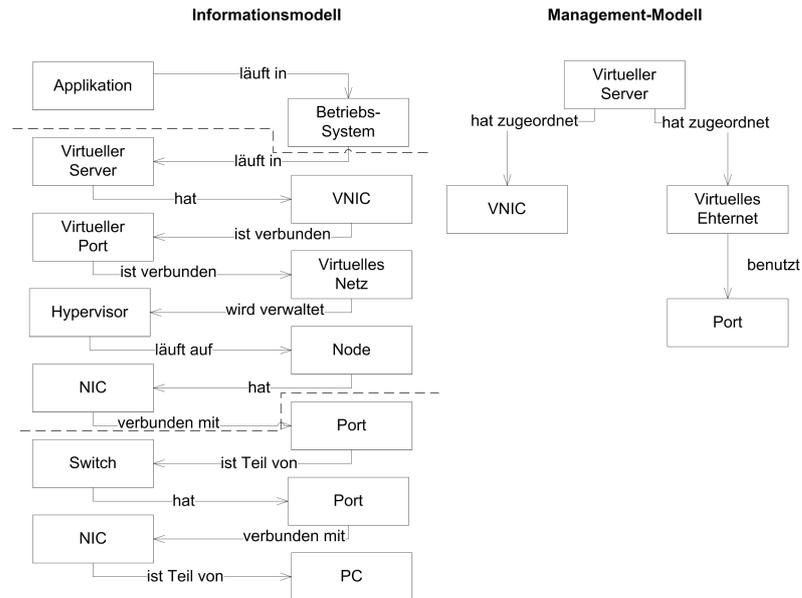


Abbildung 4.18: Informations- und Managementmodell bei Virtual Iron für Szenario 1b

4.2.4 Virtual Iron

Wie in Abbildung 4.17 zu sehen ist, sind die Infrastrukturen in jedem Standort wieder identisch und wie folgt aufgebaut: Es gibt einen Management-Server, einen Node, ein Virtual Data Center und vier virtuelle Server. Zusätzlich gibt es jeweils ein SAN, auf dem pro VS eine logische Platte angelegt wird. Als letztes Element ist ein Netz nötig, das die Verbindung in das angeschlossene LAN realisiert. Der Administrator kann sich dann von der Zentrale aus auf die einzelnen Management-Server verbinden und die Infrastrukturen steuern. Jedoch muss er auch in diesem Fall die anderen Teile, die sich nicht über das VI-Center steuern lassen, mit anderen Tools remote managen können.

Modelle

In Abbildung 4.18 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit Virtual Iron vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Es werden nur die Teile des Informationsmodells von Virtual Iron gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. Das Informationsmodell besteht aus den Komponenten Applikationen, Betriebssystem, virtueller Server, VNIC, virtueller Port, virtuelles Netz, Hypervisor, Node, NIC, Port, Switch, Port, NIC und PC. Diese Komponenten benutzen jeweils die auf sie folgende. Das Managementmodell von Virtual Iron wurde in Abschnitt 2.3.2 erläutert. Die Elemente des Managementmodells werden folgendermaßen auf das Informationsmodell abgebildet: Der Virtuelle Server wird auf die virtuelle Maschine des Informationsmodells abgebildet. Die virtuelle NIC wird analog dazu auf die virtuelle NIC abgebildet. Das virtuelle Netz wird auf das virtuelle Netz des Informationsmodells abgebildet. Der Port des Managementmodells wird auf die NIC des Informationsmodells abgebildet. Im Managementmodell gibt es keine direkte Verbindung

zwischen der virtuellen NIC und dem Port; eine solche wird aber über den virtuellen Server hergestellt. Im Informationsmodell besteht jedoch eine mittelbare Beziehung der korrespondierenden Komponenten, wodurch auch hier die Verbindung hergestellt wird.

Arbeitsschritte

- VNICs anlegen
- Netz anlegen
- Virtual Data Center anlegen
- Node zuweisen
- Logische Platten erstellen
- Virtual Server erstellen (dabei VNIC und Netz zuweisen)
- Virtual Server booten
- Logs auf Fehler überprüfen

Zusammenfassung

Für das Remote Management ist Virtual Iron nur teilweise gut ausgerüstet. Für den Zugriff auf die Infrastruktur eines Standortes muss jeweils auf den dort vorhandenen Management-Server zugegriffen werden. Zusätzlich sind auch hier weitere Managementmöglichkeiten z.B. für die Netze und die Desktops nötig.

Bewertung

- A1 - Aufbau** Die virtuelle Infrastruktur lässt sich aufbauen.
- A2 - Betrieb** Mit Einschränkung der in Abschnitt 4.5.4 genannten Punkte ist der Betrieb einer Infrastruktur möglich.
- A3 - Schnittstelle zum physischen Management** Virtual Iron bietet keine Schnittstelle für das physische Management an.
- A4 - Automation** Virtual Iron beherrscht zwar Automation, diese ist aber für das Szenario nicht erforderlich.
- A5 - Mandantenfähigkeit** Mandantenfähigkeit ist begrenzt gegeben, aber auch nicht notwendig.
- A6 - Rollen- und Rechtekonzept** Ein Rollen- und Rechtesystem wird für das Szenario nicht gebraucht und ist auch nicht vorhanden.
- A7 - Transparenz der Virtualisierungslösung** Das Netz-Management ist bei Virtual Iron für den Nutzer transparent.
- A8 - Darstellung der Technik** Die Darstellung der Technik durch Virtual Iron ist dem Szenario angemessen.

4 Umsetzung der Szenarien in den Modellen

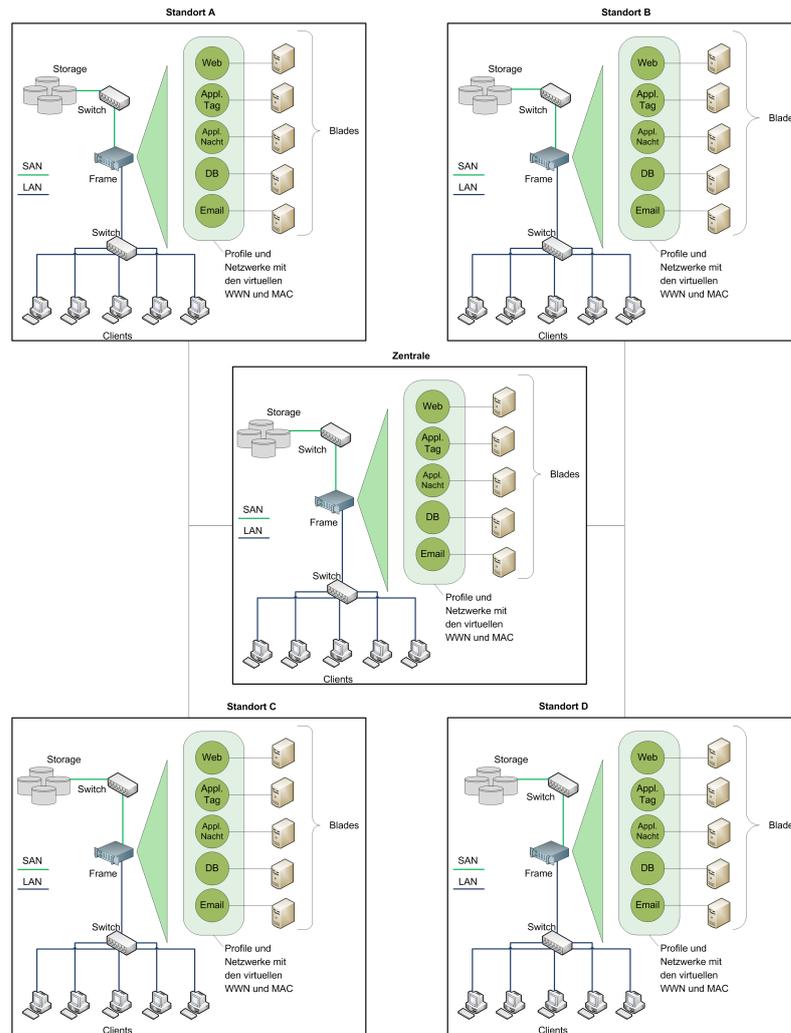


Abbildung 4.19: Szenario 1b Mit VIOM

4.2.5 VIOM

Der Einsatz von VIOM in diesem Szenario stellt sich vom Hardware-Aufbau genauso dar, wie der in Abschnitt 4.1.5 und ist schematisch in Abbildung 4.19 dargestellt. Anders als in Szenario 1a wird in diesem Fall ein Blade weniger und damit ein Profil weniger benötigt, da der Wechsel der Anwendung bei Nacht weg fällt. Um die entfernten Systeme remote managen zu können, ist in der Zentrale ein Management-Server mit VIOM nötig. Dieser Management-Server kann direkt die Frames in den Standorten verwalten. Dieser Umstand macht es dem Administrator recht leicht, die Server aller Standorte zu verwalten. Jedoch nur in dem Rahmen, der mit VIOM möglich ist. Ein Vorteil der Profile macht sich hier bemerkbar. Es können auf allen Systemen dieselben Profile verwendet werden, solange auf jedem System das verwendete Netzwerk den gleichen Namen trägt. Ein Profil für jeden Server-Typ muss nur einmal angelegt werden und kann in jedem Frame zugewiesen werden.

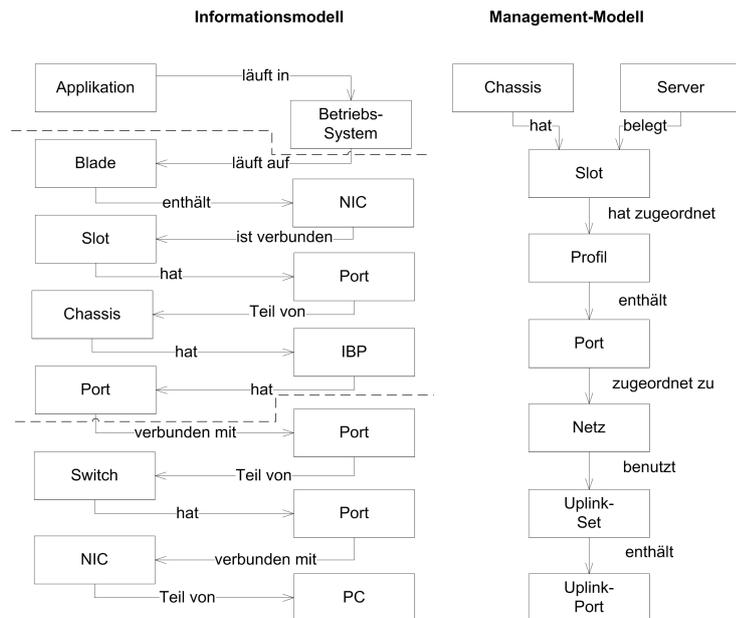


Abbildung 4.20: Informations- und Managementmodell bei VIOM für Szenario 1b

Modelle

In Abbildung 4.20 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit VIOM vorhanden sind. Es werden nur die Teile des Informationsmodells von VIOM gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. VIOM kennt im Informationsmodell die Applikationen, das Betriebssystem, das Blade mit einer NIC, der Slot, in dem das Blade montiert ist, der Port des Slots, das Chassis, dessen Teil der Slot ist, das IBP, das Teil des Chassis ist, die darin enthaltenen Uplink-Ports, der Port am externen Switch, der Switch selbst, ein weiterer Port, die NIC des PCs und der PC selbst. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Nun wird die Abbildung der Elemente des Managementmodells auf die des Informationsmodells beschrieben. Das Chassis wird auf das Chassis und ein Server auf ein Blade abgebildet. Der Slot wird direkt auf einen Slot abgebildet. Das Profil wird auf eine Menge der Ports eines Slots im Informationsmodell abgebildet. Ein Port des Managementmodells wird auf einen Port eines Slots im Informationsmodell abgebildet. Nun wird ein Uplink-Set auf eine Menge von Ports des IBP abgebildet. Ein Netz ist eine Menge bestehend aus Ports der Slots (also der Abbildung eines Profils) und Ports des IBP (der Abbildung eines Uplink-Sets). Ein einzelner Uplink-Port wird auf einen Port des IBP abgebildet.

Arbeitsschritte

- Anlegen und Konfigurieren eines Netzes
- Anlegen und Konfigurieren der Profile
- Zuweisen der Profile an Slots

4 Umsetzung der Szenarien in den Modellen

- Booten der Blades
- Neuzuweisen eines Profils an einen anderen Slot im Fehlerfall

Zusammenfassung

Wie auch im vorangegangenen Szenario sind die Möglichkeiten zum Management dieses Szenarios unzureichend. Es müssen sehr viele Teile der Infrastruktur extern verwaltet werden. Jedoch bietet die Einbettung in die ServerView Suite einen sehr großen Vorteil. Dadurch, dass alle Systeme durch nur einen Management-Server steuerbar sind, ist hier die Verwaltung sehr vereinfacht. Diese Vereinfachung wird durch die Profile, die unabhängig von der Hardware zu handhaben sind, noch weiter verbessert. Hier liegt eine eindeutige Stärke von VIOM.

Bewertung

- A1 - Aufbau** Die Infrastruktur lässt sich mit den Einschränkungen von VIOM aufbauen.
- A2 - Betrieb** Der Betrieb ist mit den generellen Einschränkungen möglich.
- A3 - Schnittstelle zum physischen Management** VIOM bietet keine Schnittstelle für das Management der physischen Infrastruktur außerhalb des eigenen Frames.
- A4 - Automation** Automation ist nicht nötig und nicht vorhanden.
- A5 - Mandantenfähigkeit** Das Szenario erfordert keine Mandantenfähigkeit, eine solche wird aber auch nur eingeschränkt bereitgestellt.
- A6 - Rollen- und Rechtekonzept** Rollen und Rechte sind für das Szenario nicht nötig, und werden auch nicht angeboten.
- A7 - Transparenz der Virtualisierungslösung** Das Netz-Management von VIOM findet transparent statt.
- A8 - Darstellung der Technik** Die Darstellung der Technik ist für einen professionellen Administrator angemessen.

4.2.6 Bewertung für das Szenario 1b

Modell	A1	A2	A3	A4	A5	A6	A7	A8
ohne Virt.	-	-	-	o	o	o	-	+
PAN	+	o	-	o	o	o	+	+
VMware	+	o	-	o	o	o	+	+
Virtual Iron	+	o	-	o	o	o	+	+
VIOM	o	o	-	o	o	o	+	+

+: gut o: neutral -: schlecht

Tabelle 4.2: Bewertung der Virtualisierungs-Management-Modelle für Szenario 1b

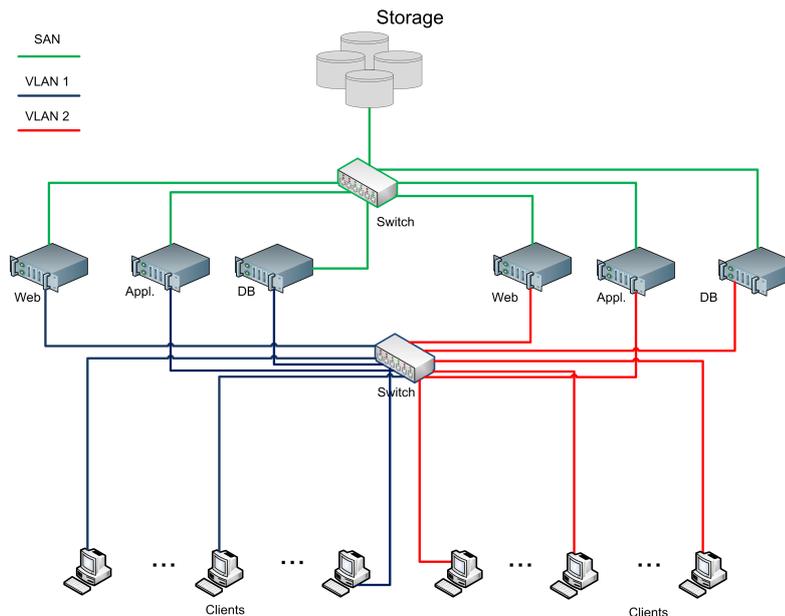


Abbildung 4.21: Szenario 2a ohne Virtualisierung

In Tabelle 4.2 ist dargestellt, wie die einzelnen Virtualisierungs-Management-Modelle für dieses Szenario bewertet werden. Für dieses Szenario werden PAN, VMware und Virtual Iron alle gleich gut bewertet. VIOM ist nur in der Bewertung der Anforderung A1 schlechter. Ansonsten haben alle Modelle, bis auf das Vorgehen ohne Virtualisierung, dieselbe Bewertung.

4.3 Szenario 2a

Dieser Abschnitt zeigt auf, wie die Modellierung des Szenarios 2a (siehe Abschnitt 3.1.3) mit den vorhandenen Modellen durchgeführt werden kann. Dieses Szenario ist in einem großen Unternehmen mit eigenem Rechenzentrum angesiedelt. In dem Unternehmen gibt es zwei Abteilungen, die zwar dieselbe Geschäftsanwendung nutzen, aber nur exklusiven Zugang zu ihren Daten haben sollen.

4.3.1 Ohne Virtualisierung

Für die Umsetzung dieses Szenarios werden sechs Server benötigt, um die Anwendung für die beiden Abteilungen anbieten zu können. Für die Realisierung des Netzes wird ein VLAN-tauglicher Ethernet-Switch benötigt und ein FC-Switch mit angeschlossenen Speichern für das SAN. Die jeweils zehn PCs der Abteilungen kommunizieren mit den für sie zuständigen Servern über ein VLAN. Der Zugang zu den jeweiligen Servern über das SAN wird über die Freigabe der jeweiligen Adressen der Server geregelt. Auf den Servern wird jeweils ein Betriebssystem mit den nötigen Anwendungen installiert. Der gesamte Aufbau ist schematisch in Abbildung 4.21 dargestellt.

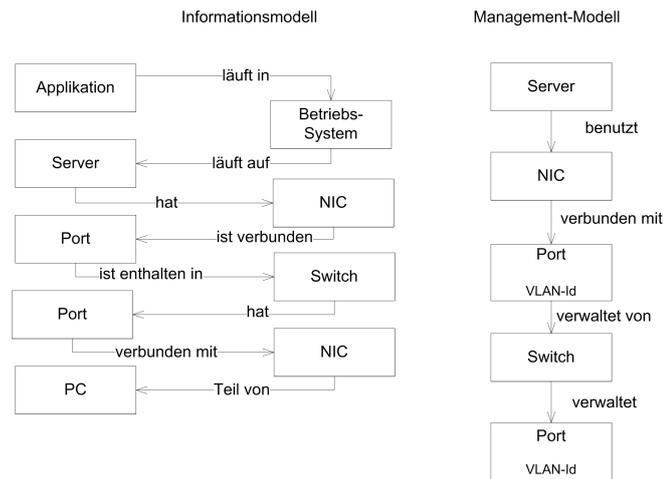


Abbildung 4.22: Informations- und Managementmodell ohne Virtualisierung für Szenario 2a

Modelle

In Abbildung 4.22 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung ohne Virtualisierung vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Das Informationsmodell umfasst die Elemente des Aufbaus angefangen bei den Applikationen, die in Betriebssystemen laufen, über den physischen Server, der über die physische NIC den Netzverkehr verarbeitet. Die NIC ist über einen Port mit einem Switch verbunden, der über einen anderen Port mit der NIC eines PCs verbunden ist. Das Managementmodell ohne Virtualisierung hat im Bezug auf Netze dieselben Komponenten wie das Informationsmodell. Hier gibt es den Server, der die NIC benutzt. Die NIC ist mit einem Port des Switches verbunden. Der Switch hat noch einen weiteren Port. Es findet eine direkte 1:1 Abbildung zwischen dem Managementmodell und dem Informationsmodell statt. Die Verwaltung der VLANs erfolgt über die Ports des Switches.

Arbeitsschritte

- Konfiguration
 - Netze
 - Storage
- Server Starten
- Softwareinstallation
 - Betriebssystem
 - Anwendungen
- Betrieb
 - Logs überprüfen
 - Fehler beheben

Zusammenfassung

Das Management dieses Szenarios umfasst mehrere Teilbereiche, die in einem Rechenzentrum meist getrennt betrieben werden, wie Server-, Netz-, Storage- und Desktop-Administration. Jeder der Teilbereiche hat Schnittpunkte zu mindestens einem der anderen Bereiche und jeder Bereich verwendet eigene Managementsysteme. Aus diesem Zusammenhang wird klar, dass das Management in diesem Fall sehr aufwändig ist. Die Server, die Switches und die Clients werden, soweit möglich, über SNMP gemanagt. Dafür wird ein Management-System im Rechenzentrum verwendet. Dadurch ist das Management der Hardware in diesem Szenario zumindest zum Teil durch eine Management-Anwendung zu handhaben. Falls Teile der Hardware nicht ausreichend über SNMP gesteuert werden können, muss auf proprietäre Lösungen der Hersteller zurückgegriffen werden, wodurch der Aufwand, vor allem in heterogenen Infrastrukturen, weiter anwächst. Das Management der Anwendungen erfolgt ebenso wie das der Betriebssysteme direkt auf den Servern mit den entsprechenden internen Lösungen. Auch das Management der VLANs muss extern auf den beteiligten Komponenten durchgeführt werden.

Bewertung

- A1 - Aufbau** Ohne den Einsatz von Virtualisierung ist die Erstellung einer virtuellen Infrastruktur nicht möglich.
- A2 - Betrieb** Ohne den Einsatz von Virtualisierung ist der Betrieb einer virtuellen Infrastruktur nicht möglich.
- A3 - Schnittstelle zum physischen Management** Es wird ausschließlich physisches Management durchgeführt.
- A4 - Automation** Automation ist nicht möglich.
- A5 - Mandantenfähigkeit** Das System ist nicht mandantenfähig.
- A6 - Rollen- und Rechtekonzept** Es gibt keine integrierte Nutzerverwaltung mit Rollen und Rechten.
- A7 - Transparenz der Virtualisierungslösung** Das Managementmodell entspricht dem Informationsmodell. Das Netz-Management wird nicht transparent gestaltet.
- A8 - Darstellung der Technik** Die Technik ist direkt dargestellt.

4.3.2 PAN

Für die Umsetzung dieses Szenarios mit PAN werden zwei pBlades als Rechenressource benötigt. Für die Speicherung der Daten und die nötigen Anwendungen werden sechs Disks benötigt. Die getrennte Netzanbindung an die beiden Abteilungen erfordert, dass zwei vSwitches benutzt werden, die eine Verbindung an das angeschlossene Netz bereitstellen. Mit diesen Ressourcen werden zwei LPANs angelegt, eines für jede der Abteilungen. Da beide Abteilungen, wie Abbildung 4.23 zu entnehmen ist, auf gleichwertige Systeme zugreifen sollen, werden beide LPANs gleich aufgebaut. Einem LPAN wird die Hälfte der oben aufgezählten Ressourcen zugeteilt. Das wären im einzelnen ein pBlade, drei Disks und ein vSwitch. Auf

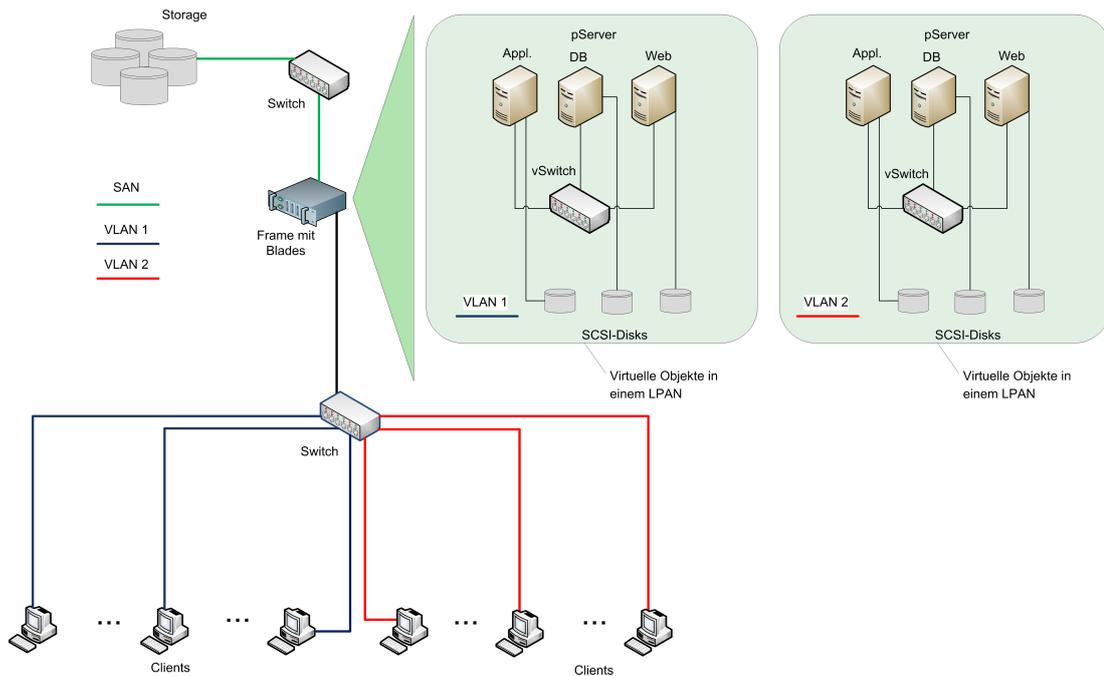


Abbildung 4.23: Szenario 2a mit PAN

den pBlades werden jeweils drei vBlades angelegt. Danach werden in dem LPAN drei pServer erstellt, denen jeweils ein vBlade und eine Disk zugeteilt werden. Alle drei pServer werden über ihre vEths mit dem vSwitch ihres LPAN miteinander und an das Netz angeschlossen. Damit ist die Trennung der Server und der Storage, die durch das Szenario gefordert werden, durchgeführt. Die Netz-Trennung wird über ein extern verwaltetes VLAN realisiert.

Modelle

In Abbildung 4.24 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit PAN vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Im Informationsmodell sind die folgenden Elemente enthalten: Eine Applikation läuft auf einem Betriebssystem, das auf einer virtuellen Maschine oder direkt auf dem Bladeserver läuft. Ob das Betriebssystem auf einer virtuellen Maschine oder auf der Hardware betrieben wird, ist abhängig von der Art des pServers (siehe weiter unten in diesem Abschnitt bei der Beschreibung der Abbildung vom Managementmodell auf das Informationsmodell). Die virtuelle Maschine benutzt eine virtuelle NIC, die mit einer virtuellen Bridge verbunden ist. Die drei virtuellen Komponenten werden durch den Hypervisor verwaltet. Der Hypervisor läuft wiederum auf einem Bladeserver, der über seine NIC den internen Switch benutzt. Über den internen Switch findet die Kommunikation mit dem cBlade statt. Dabei läuft Datenverkehr vom internen Switch über eine NIC des cBlades. Diese ist wiederum mit einer virtuellen Bridge verbunden, die über eine weitere NIC die Verbindung nach außen anbietet. Diese NIC ist mit dem Port eines Switches verbunden, der über einen weiteren Port mit der NIC eines PCs verbunden ist. Es werden nur die Teile des Informationsmodells von PAN gemanagt, die in der Abbildung zwischen den gestrichelten

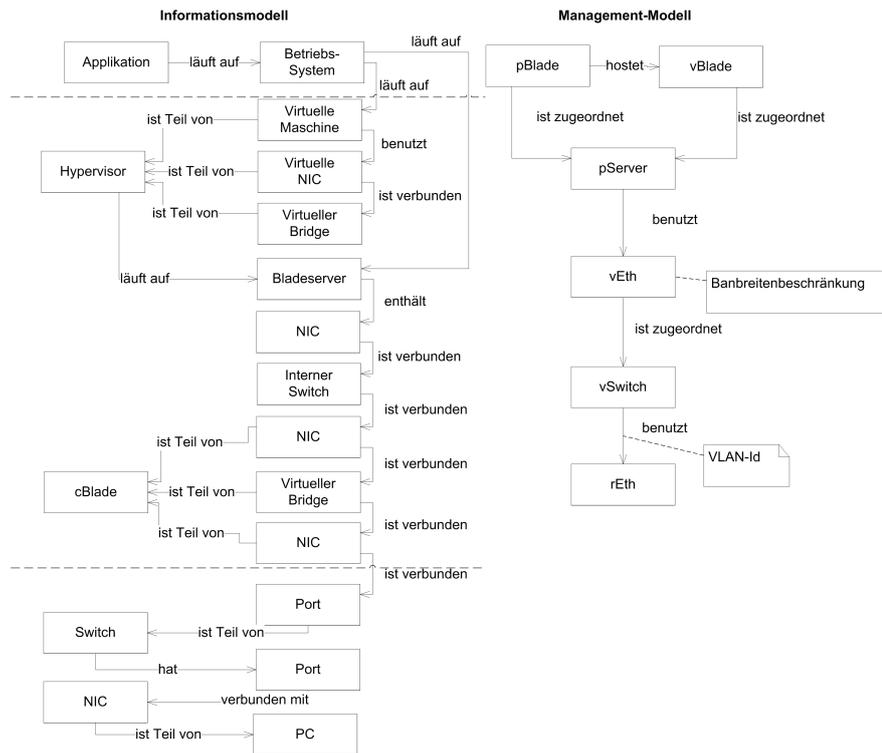


Abbildung 4.24: Informations- und Managementmodell bei PAN für Szenario 2a

Linien liegen. PAN kann zwar auch Applikationen auf Linux Gastssystemen verwalten, aber da hier speziell auf das Netz-Management eingegangen wird, ist dieser Teil ausgenommen. Das Managementmodell von PAN wurde schon in Abschnitt 2.1.2 erläutert. An dieser Stelle soll darauf eingegangen werden, wie das Managementmodell auf das Informationsmodell abgebildet wird. Die Abbildung des pServers ist abhängig von der Art des Blades, auf dem er gebootet ist. Die Abbildung ist eine andere, je nachdem, ob der pServer auf einem pBlade oder einem vBlade gebootet ist. Ist er auf einem pBlade gebootet, wird er auf einen Bladesserver abgebildet. In diesem Fall ist die vEth die NIC des Bladesservers. Ist der pServer auf einem vBlade gebootet, wird er auf eine virtuelle Maschine abgebildet und seine vEth auf eine virtuelle NIC. In beiden Fällen kann an der vEth eine Bandbreitenbeschränkung eingerichtet werden. Ein vSwitch wird abgebildet auf den internen Switch sowie die interne NIC des cBlades. Die rEth wird auf die virtuelle Bridge des cBlades und dessen externe NIC abgebildet. Bei der Zuordnung der rEth an den vSwitch wird die VLAN-Id vergeben.

Arbeitsschritte

- LPAN anlegen
- vSwitches anlegen und konfigurieren
- LPAN Ressourcen zuteilen
- pServer erstellen und konfigurieren (Verwendung eines vSwitch)

4 Umsetzung der Szenarien in den Modellen

- pServer starten
- Betriebssysteme und Applikationen installieren und konfigurieren
- Ereignisse auf Fehler prüfen
- Fehler lokalisieren und beheben

Zusammenfassung

PAN bietet an dieser Stelle wieder viele Vorteile durch ein integriertes Management. Die Hardwarekonfiguration der Server lässt sich wie in den bisherigen Szenarien wieder komplett über PAN erledigen. Auch die interne Netzkonfiguration über einen PAN-internen Switch samt VLAN ist möglich. Ebenso ist die Anbindung des PAN an das LAN über VLANs mit dem PAN-Manager zu bewerkstelligen. Nur die Konfiguration der VLANs außerhalb des PAN müssen mit externen Mitteln durchgeführt werden. Das Management der Server-Betriebssysteme mit ihren Anwendungen sowie die Verwaltung der Anwendungen müssen ebenfalls, wie in den vorherigen Szenarien, extern erledigt werden. Das Management der Desktops ist mit PAN auch in keiner Weise vorgesehen. Es muss also auch für diese Aufgabe eine weitere externe Lösung eingesetzt werden.

Bewertung

- A1 - Aufbau** Das Szenario kann nachgebildet werden. Vorlagen zum Erstellen von pServern sind jedoch nicht möglich.
- A2 - Betrieb** Mit den Einschränkungen aus 4.5.2 ist der Betrieb der Infrastruktur möglich.
- A3 - Schnittstelle zum physischen Management** Es existiert keine Schnittstelle zum Management der restlichen Infrastruktur.
- A4 - Automation** PAN beherrscht die Migration im Fehlerfall, nicht jedoch die lastabhängige. Auch die automatische Erstellung ist nicht möglich.
- A5 - Mandantenfähigkeit** Das System ist mandantenfähig.
- A6 - Rollen- und Rechtekonzept** PAN bietet ein adäquates Rollen und Rechtesystem an.
- A7 - Transparenz der Virtualisierungslösung** PAN ist als Virtualisierung für den Nutzer im Netzmanagement transparent.
- A8 - Darstellung der Technik** Die Darstellung der Technik ist das Abbild des logischen Modells von PAN. Daher ist die Darstellung angemessen.

4.3.3 VMware

Zunächst werden für dieses Szenario sechs virtuelle Festplatten angelegt. Danach werden auf dem ESX Host zwei virtuelle Netze (Portgruppen) mit unterschiedlichen VLANs an einem vSwitch definiert. Weiterhin sind sechs virtuelle Maschinen nötig, von denen jeweils zwei die selbe Softwarekonfiguration aufweisen. Pro Abteilung gibt es einen Web-, einen Application- und einen Datenbankserver, die je nach ihrer Abteilung über die virtuellen Netze an den vSwitch angeschlossen werden. Abbildung 4.25 stellt den Aufbau schematisch dar.

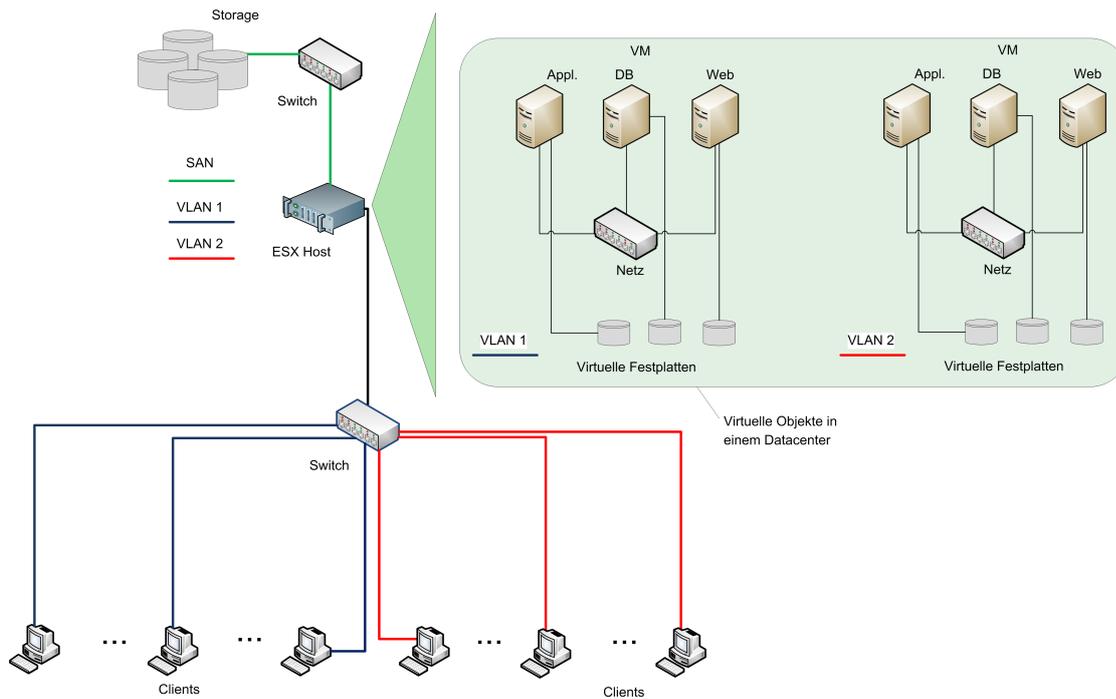


Abbildung 4.25: Szenario 2a mit VMware

Modelle

In Abbildung 4.26 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit VMware vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management der Netze in VMware arbeitet. Es werden nur die Teile des Informationsmodells von VMware gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. Das Informationsmodell umfasst die Applikationen, die in Betriebssystemen laufen, die virtuellen Maschinen, die über eine virtuelle NIC an einem virtuellen Port an einen virtuellen Switch angeschlossen sind. Dieser virtuelle Switch leitet Netzverkehr über den verwaltenden Hypervisor an den physischen Host, der ihn an die physische NIC übergibt. Die NIC ist über einen Port mit einem externen Switch verbunden, der über einen weiteren Port die Verbindung zur NIC eines PCs herstellt. Bei der Abbildung des Managementmodells auf das Informationsmodell wird wie folgt vorgegangen: Die virtuelle Maschine des Managementmodells wird auf die virtuelle Maschine des Informationsmodells abgebildet. Analog wird mit der virtuellen NIC vorgegangen. Die Portgruppe, über die die VLAN-Id verwaltet wird, wird auf virtuelle Ports abgebildet und der vSwitch auf den virtuellen Switch. Die NIC schließlich wird auf die NIC des Hosts abgebildet.

Arbeitsschritte

- Data Center anlegen
- vSwitches anlegen
- Portgruppen anlegen

4 Umsetzung der Szenarien in den Modellen

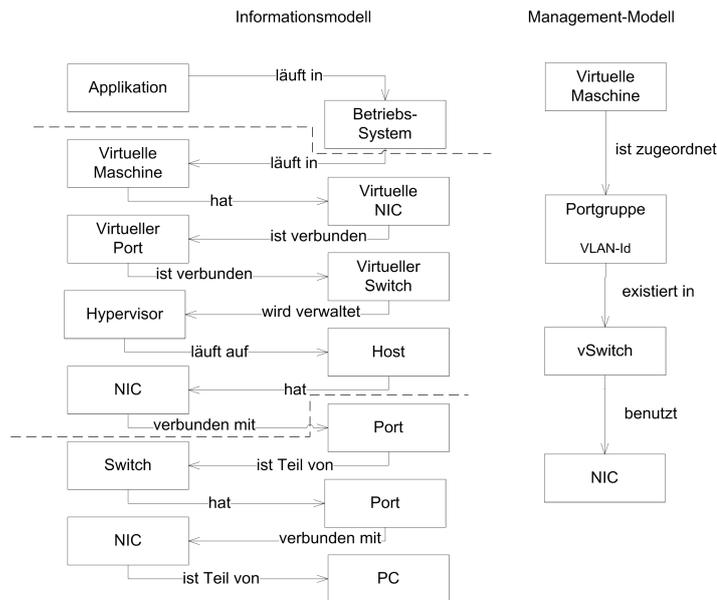


Abbildung 4.26: Informations- und Managementmodell von Szenario 2a mit VMware

- Storage definieren
- ESX Server Host zuweisen
- Virtuelle Maschine erstellen
- Virtuelle Maschine Portgruppe zuweisen
- Virtuelle Maschine booten
- Logs auf Fehler überprüfen
- Fehler lokalisieren und beheben

Zusammenfassung

Wie bei den vorangegangenen Szenarien kann der Administrator mit Virtual Center alle Aufgaben die Virtualisierung betreffend erledigen. Die Administration der Server, der externen Netze, der Storage und der Desktops muss aber wieder mit anderen Lösungen erfolgen.

Bewertung

- A1 - Aufbau** Die Infrastruktur des Szenarios lässt sich den Anforderungen entsprechend aufbauen.
- A2 - Betrieb** Gemäß den Beschränkungen aus 4.5.3 lässt sich die Infrastruktur betreiben.
- A3 - Schnittstelle zum physischen Management** VMware bietet keine Schnittstelle für das physische Management.
- A4 - Automation** Alle Arten der Automation für das Szenario werden angeboten.

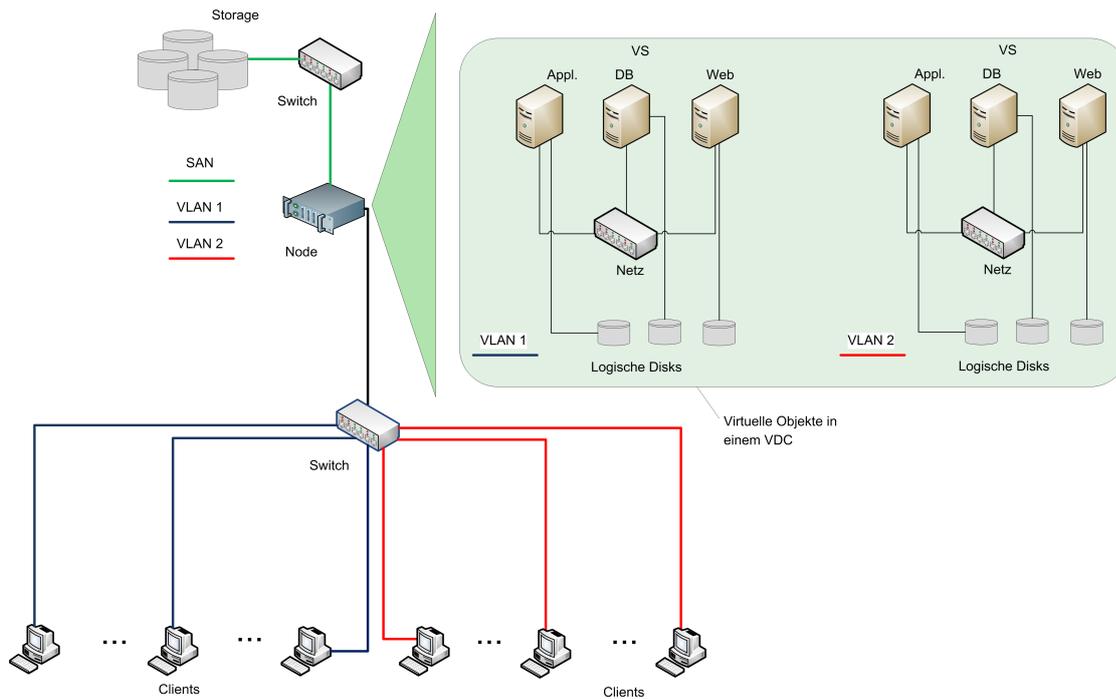


Abbildung 4.27: Szenario 2a mit VI

A5 - Mandantenfähigkeit Das Modell ist mandantenfähig.

A6 - Rollen- und Rechtekonzept VMware bietet ein Rollen- und Rechtesystem.

A7 - Transparenz der Virtualisierungslösung Das Managementmodell schafft Transparenz in der Verwendung. Es wird mit vereinfachten Konzepten gearbeitet, die die Arbeit erleichtern.

A8 - Darstellung der Technik Die Darstellung der Technik entsprechend dem logischen Modell ist angemessen.

4.3.4 Virtual Iron

Zur Umsetzung dieses Szenarios mit Virtual Iron ist auch diesmal, wie aus Abbildung 4.27 ersichtlich, ein Node nötig. Für die Vernetzung der beiden Abteilungen werden zwei logische Netze angelegt, denen jeweils die freien Ports der Nodes zugewiesen werden. Weiter wird das VDC angelegt, das den Node zugewiesen bekommt. Nun werden drei logische Disks auf dem SAN angelegt und drei VS erstellt, die gleich die logischen Disks zugewiesen bekommen. Damit ist die virtuelle Infrastruktur erstellt und es müssen noch die Betriebssysteme mit den Anwendungen installiert werden.

Modelle

In Abbildung 4.28 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit Virtual Iron vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer

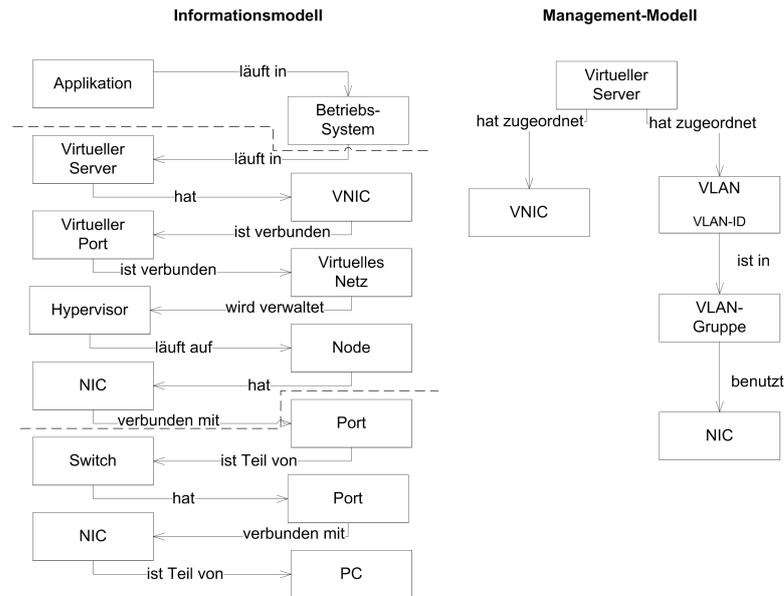


Abbildung 4.28: Informations- und Managementmodell bei Virtual Iron für Szenario 2a

beim Management des Netzes arbeitet. Es werden nur die Teile des Informationsmodells von Virtual Iron gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. Das Informationsmodell besteht aus den Komponenten Applikationen, Betriebssystem, virtueller Server, VNIC, virtueller Port, virtuelles Netz, Hypervisor, Node, NIC, Port, Switch, Port, NIC und PC. Diese Komponenten benutzen jeweils die auf sie folgende. Das Managementmodell von Virtual Iron wurde in Abschnitt 2.3.2 erläutert. Die Elemente des Managementmodells werden folgendermaßen auf das Informationsmodell abgebildet: Der Virtuelle Server wird auf die virtuelle Maschine des Informationsmodells abgebildet. Die virtuelle NIC wird analog dazu auf die virtuelle NIC abgebildet. Das VLAN mit der VLAN-Id wird zusammen mit der VLAN-Gruppe auf das virtuelle Netz des Informationsmodells abgebildet. Der Port des Managementmodells wird auf die NIC des Informationsmodells abgebildet. Im Managementmodell gibt es keine direkte Verbindung zwischen der virtuellen NIC und dem Port, eine solche wird über den virtuellen Server hergestellt. Im Informationsmodell besteht jedoch eine mittelbare Beziehung der korrespondierenden Komponenten, wodurch auch hier die Verbindung hergestellt wird.

Arbeitsschritte

- VNICs anlegen
- Netze anlegen
- Virtual Data Center anlegen
- Node zuweisen
- Logische Platten erstellen
- Virtual Server erstellen (dabei VNIC und Netz zuweisen)

- Virtual Server booten
- Logs auf Fehler überprüfen

Zusammenfassung

Für dieses Szenario bietet Virtual Iron wieder eine effiziente Möglichkeit, die virtuelle Infrastruktur zu erstellen und zu betreiben. Jedoch werden auch hier wieder an den Grenzen der Virtualisierung weitere Möglichkeiten gebraucht, um die restlichen Teile der Infrastruktur zu beherrschen.

Bewertung

- A1 - Aufbau** Die Infrastruktur des Szenarios lässt sich aufbauen.
- A2 - Betrieb** Der Betrieb der Infrastruktur ist mit den Einschränkungen aus Abschnitt 4.5.4 möglich.
- A3 - Schnittstelle zum physischen Management** Es gibt keine Schnittstelle zum physischen Management.
- A4 - Automation** Alle nötige Automation für die Dynamik ist vorhanden.
- A5 - Mandantenfähigkeit** Virtual Iron ist nur bedingt mandantenfähig.
- A6 - Rollen- und Rechtekonzept** Es gibt kein Rollen- und Rechtesystem.
- A7 - Transparenz der Virtualisierungslösung** Das Netz-Management wird bei Virtual Iron für den Nutzer transparent durchgeführt.
- A8 - Darstellung der Technik** Die Darstellung der Technik entsprechend dem logischen Modell ist für das Szenario angemessen.

4.3.5 VIOM

Für dieses Szenario werden mit VIOM sechs Blades benötigt. Von diesen sechs Blades sind jeweils drei für eine Abteilung vorgesehen. Generell besteht die Möglichkeit, die Trennung der Netze der beiden Abteilungen so durchzuführen, dass entweder getrennte Netze oder ein gemeinsames Netz mit VLAN eingesetzt wird. In dieser Umsetzung wird die Trennung der Netze durch VLAN verwendet, die auch in Abbildung 4.29 zu sehen ist, um dieselbe Technik zu verwenden, die auch bei den Umsetzungen der anderen Modelle dieses Szenarios benutzt wird. Dazu werden zwei Netzwerke vom Typ 'Netz mit VLAN-Id' angelegt, denen jeweils ein aktiver Port zugewiesen wird. Jetzt werden noch die nötigen Profile angelegt. Zunächst werden die beiden Profile für die beiden Webserver angelegt und mit den entsprechenden LUNs und jeweils mit einem der einzelnen Netze verbunden. Für jeden Application- und Datenbankserver wird ebenfalls ein Profil angelegt, die jeweils mit dem Netz der Abteilung verbunden werden. Auch diesen Profilen wird der entsprechende LUN zugewiesen.

4 Umsetzung der Szenarien in den Modellen

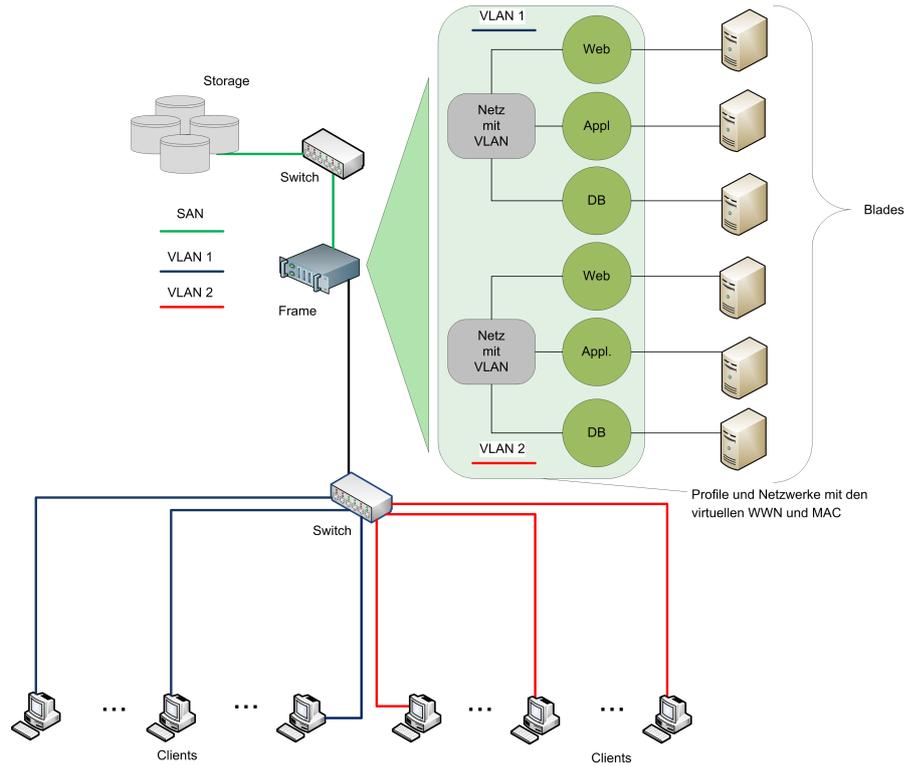


Abbildung 4.29: Szenario 2a Mit VIOM

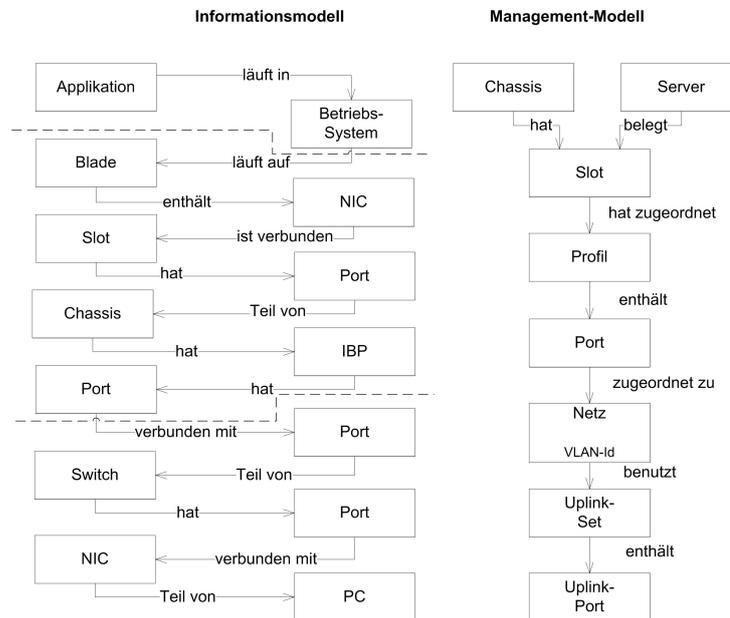


Abbildung 4.30: Informations- und Managementmodell bei VIOM für Szenario 2a

Modelle

In Abbildung 4.30 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit VIOM vorhanden sind. Es werden nur die Teile des Informationsmodells von VIOM gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. VIOM kennt im Informationsmodell die Applikationen, das Betriebssystem, das Blade mit einer NIC, der Slot in dem das Blade montiert ist, der Port des Slots, das Chassis, dessen Teil der Slot ist, das IBP, das Teil des Chassis ist, die darin enthaltenen Uplink-Ports, der Port am externen Switch, der Switch selbst, ein weiterer Port, die NIC des PCs und der PC selbst. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Nun wird die Abbildung der Elemente des Managementmodells auf die des Informationsmodells beschrieben. Das Chassis wird auf das Chassis und ein Server auf ein Blade abgebildet. Der Slot wird direkt auf einen Slot abgebildet. Das Profil wird auf eine Menge der Ports eines Slots im Informationsmodell abgebildet. Ein Port des Managementmodells wird auf einen Port eines Slots im Informationsmodell abgebildet. Nun wird ein Uplink-Set auf eine Menge von Ports des IBP abgebildet. Ein Netz ist eine Menge bestehend aus Ports der Slots (also der Abbildung eines Profils) und Ports des IBP (der Abbildung eines Uplink-Sets). Zusätzlich hält das Netz die VLAN-Id als Attribut. Ein einzelner Uplink-Port wird auf einen Port des IBP abgebildet.

Arbeitsschritte

- Anlegen und Konfigurieren der Netze
- Anlegen und Konfigurieren der Profile (Verwendung der Netze)
- Zuweisen der Profile an Slots
- Booten der Blades
- Neuzuweisen eines Profils an einen anderen Slot im Fehlerfall

Zusammenfassung

Auch in diesem Szenario lassen sich die grundsätzlichen Anforderungen des Szenarios gut mit VIOM erfüllen. Es ist jedoch wieder ein großer Aufwand außerhalb von VIOM erforderlich, um die gesamte Infrastruktur zu managen, da VIOM nur die Verwaltung der Blades und ihrer Adressen anbietet. Aufgaben wie die Storage-, Netz-, Desktop- und Serververwaltung (auf Betriebssystemebene) können nicht mit VIOM erfüllt werden.

Bewertung

- A1 - Aufbau** Die Infrastruktur des Szenarios lässt sich nachbilden.
- A2 - Betrieb** Der Betrieb der Infrastruktur ist mit den Begrenzungen, die in Abschnitt 4.5.5 beschrieben sind, möglich.
- A3 - Schnittstelle zum physischen Management** VIOM bietet keine Schnittstelle zum physischen Management an.

A4 - Automation Automation wird nicht unterstützt.

A5 - Mandantenfähigkeit VIOM ist eingeschränkt Mandantenfähig.

A6 - Rollen- und Rechtekonzept Ein Rollen- und Rechtekonzept ist nicht vorhanden.

A7 - Transparenz der Virtualisierungslösung Das Netz-Management von VIOM wird transparent durchgeführt.

A8 - Darstellung der Technik Die Darstellung der Technik ist den Erfordernissen des Szenarios angemessen.

4.3.6 Bewertung für das Szenario 2a

Modell	A1	A2	A3	A4	A5	A6	A7	A8
ohne Virt.	-	-	-	-	-	-	-	+
PAN	+	o	-	o	+	+	+	+
VMware	+	o	-	+	+	+	+	+
Virtual Iron	+	o	-	+	o	-	+	+
VIOM	o	o	-	-	o	-	+	+

+: gut o: neutral -: schlecht

Tabelle 4.3: Bewertung der Virtualisierungs-Management-Modelle für Szenario 2a

In Tabelle 4.3 ist dargestellt wie die einzelnen Virtualisierungs-Managementmodelle für dieses Szenario bewertet werden. VMware bietet in diesem Szenario durch die gute Unterstützung der Automation Vorteile. Nur in diesem Punkt wird VMware besser bewertet als PAN, das ansonsten dieselbe Bewertung hat. Virtual Iron hat durch die fehlende Nutzerverwaltung und die teils schwache Mandantenfähigkeit Nachteile in diesem Szenario. VIOM mangelt es zusätzlich zu Mandantenfähigkeit und dem Rollen- und Rechtekonzept auch an der Automatisierung.

4.4 Szenario 2b

Dieser Abschnitt zeigt auf, wie die Implementierung des Szenarios 2b (siehe Abschnitt 3.1.4) mit den Modellen möglich ist. Dieses Szenario bietet fast den selben Aufbau wie das vorangegangene, nur mit dem Unterschied, dass hier zusätzlich noch Desktopvirtualisierung eingesetzt wird.

4.4.1 Ohne Virtualisierung

Der Aufbau in diesem Fall ist bis auf die Handhabung der Client-PCs ähnlich wie im vorherigen Szenario. Abbildung 4.31 zeigt schematisch den Aufbau dieses Szenarios. Die Client-PCs sind in diesem Fall nur noch Thin-Clients, die sich über eine Terminal-Sitzung mit ihrem Desktop auf dem entsprechenden Server verbinden, die den Desktop des Nutzers bereitstellen. Für jede der beiden Abteilungen gibt es in diesem Szenario einen solchen Server. Die

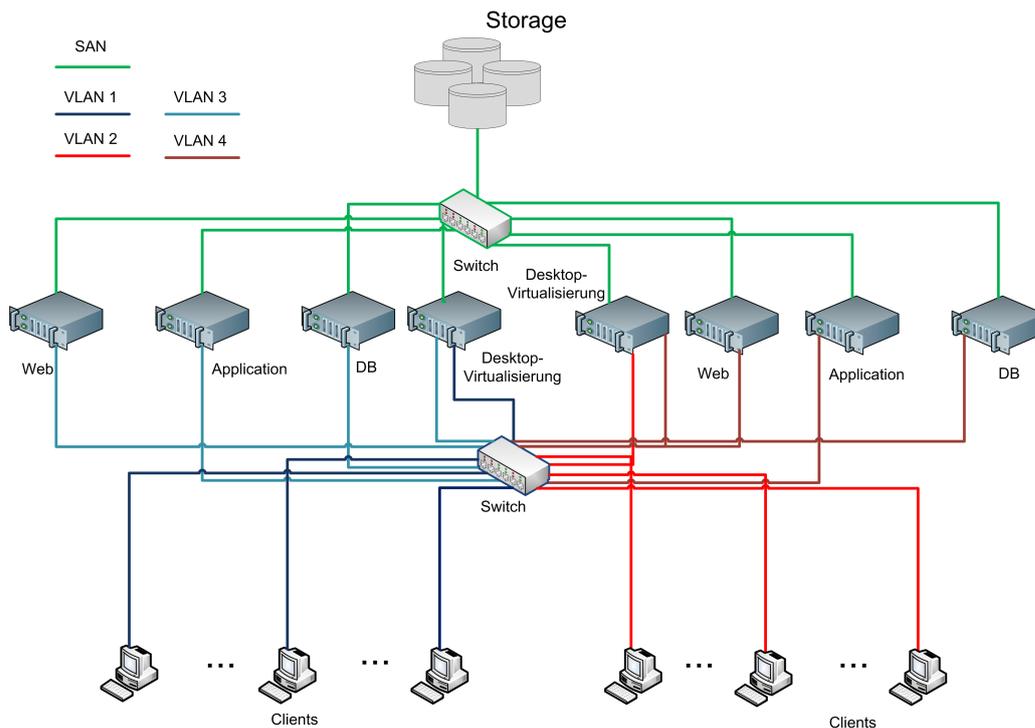


Abbildung 4.31: Szenario 2b ohne Virtualisierung

Verbindung läuft für jede Abteilung über ein anderes VLAN (VLANs 1 und 2). Die Server für die Desktopvirtualisierung brauchen auch einen Zugang zum SAN, der angelegt und verwaltet werden muss. Die drei weiteren Server pro Abteilung sind untereinander und mit dem zuständigen Server für die Desktopvirtualisierung über ein separates VLAN verbunden (VLANs 3 und 4).

Modelle

In Abbildung 4.32 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung ohne Virtualisierung vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Das Informationsmodell umfasst die Elementen angefangen bei den Applikationen, die in Betriebssystemen laufen, über den physischen Server, der über die physische NIC den Netzverkehr verarbeitet. Die NIC ist über einen Port mit einem Switch verbunden, der über einen anderen Port mit der NIC eines PCs verbunden ist. Das Managementmodell ohne Virtualisierung hat im Bezug auf Netze die selben Komponenten wie das Informationsmodell. Hier gibt es den Server, der die NIC benutzt. Die NIC ist mit einem Port des Switches verbunden. Der Switch hat noch einen weiteren Port. Es findet eine direkte 1:1 Abbildung zwischen dem Managementmodell und dem Informationsmodell statt. Die Verwaltung der VLANs erfolgt über die Ports des Switches. Für dieses Szenario werden 2 VLANs pro Abteilung benötigt, die vom Modell her identisch aufgebaut sind.

4 Umsetzung der Szenarien in den Modellen

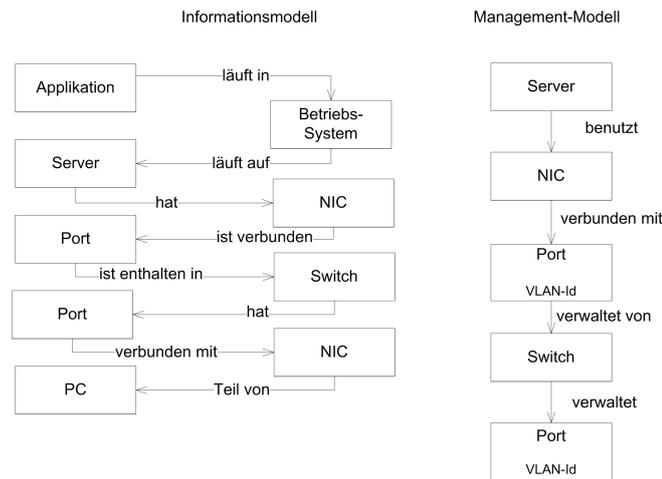


Abbildung 4.32: Informations- und Managementmodell ohne Virtualisierung für Szenario 2b

Arbeitsschritte

- Konfiguration
 - Netze
 - Storage
- Server Starten
- Softwareinstallation
 - Betriebssystem
 - Anwendungen
- Betrieb
 - Logs überprüfen
 - Fehler beheben

Zusammenfassung

Das Management in diesem Szenario ist durch das Hinzukommen der Desktopvirtualisierung noch komplexer als das des vorherigen Szenarios. Auch die Netz- und Storage-Verwaltung wurde durch dieses zusätzliche Element erweitert. Jedoch wurde das Management der Desktops vereinfacht, da es nun zentral durchgeführt werden kann und nicht auf den einzelnen PCs durchgeführt werden muss. Der prinzipielle Ablauf des Managements ändert sich aber nur in geringem Maße. Die Server, Switches, Betriebssysteme und Anwendungen und nun auch die Thin-Clients müssen über jeweils gesonderte Wege gemanagt werden, sofern sie nicht vollständig durch SNMP verwaltbar sind. Gleiches gilt für die Netze. Die Desktopvirtualisierung selbst hat wieder ein eigenständiges Management.

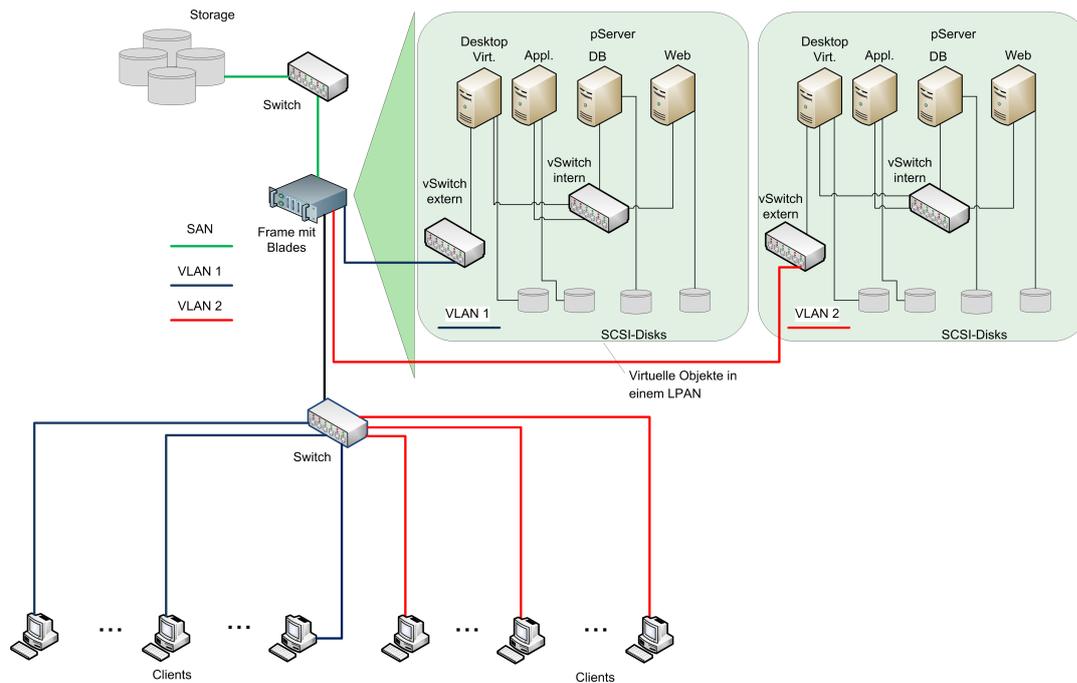


Abbildung 4.33: Szenario 2b mit PAN

Bewertung

- A1 - Aufbau** Das Erstellen einer virtuellen Infrastruktur ohne den Einsatz von Virtualisierung ist nicht möglich.
- A2 - Betrieb** Der Betrieb einer virtuellen Infrastruktur ohne den Einsatz von Virtualisierung ist nicht möglich.
- A3 - Schnittstelle zum physischen Management** Es findet nur physisches Management statt.
- A4 - Automation** Es gibt keine Automation.
- A5 - Mandantenfähigkeit** Das System ist nicht mandantenfähig.
- A6 - Rollen- und Rechtekonzept** Es existiert keine einheitliche Nutzerverwaltung mit einem Rollen- und Rechtekonzept.
- A7 - Transparenz der Virtualisierungslösung** Das Managementmodell entspricht dem Informationsmodell. Das Netz-Management wird nicht transparent gestaltet.
- A8 - Darstellung der Technik** Die Darstellung der Technik ist eine direkte Darstellung der vorhandenen Technik.

4.4.2 PAN

Der Aufbau des PAN für dieses Szenario entspricht fast dem aus Szenario 2a (beschrieben in Abschnitt 4.3.2). Da PAN keine direkte Möglichkeit bietet eine Desktopvirtualisierung anzubinden muss hier über Umwege vorgegangen werden, was in Abbildung 4.33 dargestellt

4 Umsetzung der Szenarien in den Modellen

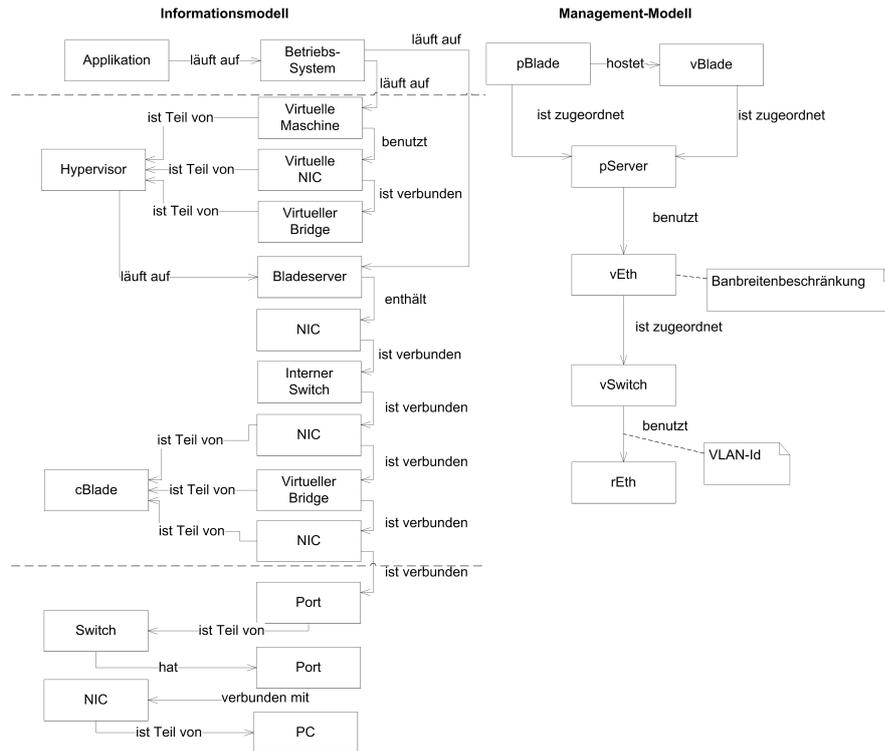


Abbildung 4.34: Informations- und Managementmodell bei PAN für Szenario 2b

ist. Eine Möglichkeit wäre ein im Vergleich zum vorherigen Szenario weiterer pServer pro LPAN, der einen Desktop für alle Nutzer gleichzeitig anbietet. Das bedeutet jeder Nutzer hat einen Standard-Desktop, den er nicht verändern kann und ihm alles anbietet, was er braucht. Hierfür würde ein gesonderter pServer benötigt. Die andere Möglichkeit wäre die Verwendung von individuellen Desktops für jeden Nutzer. Dafür müsste auch in einem gesonderten pServer eine spezielle Virtualisierungssoftware installiert werden, die es entweder ermöglicht den Nutzern ihren Desktop über die Verwendung ihrer persönlichen Konfigurationsdaten zu erreichen oder eine eigene virtuelle Maschine pro Nutzer erzeugt. In jedem Fall muss auf externe Software zurückgegriffen werden. Es wird pro Abteilung ein weiterer vSwitch benötigt. Ein vSwitch bildet ein lokales Netz, an dem die vier pServer angeschlossen sind. Der andere vSwitch ist Teil des Abteilungs-VLANs. Über dieses VLAN kommunizieren die Thin-Clients mit dem pServer für die Desktopvirtualisierung.

Modelle

In Abbildung 4.34 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit PAN vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Das Informationsmodell ist wie folgt aufgebaut: Eine Applikation läuft auf einem Betriebssystem, das auf einer virtuellen Maschine oder direkt auf dem Bladeserver läuft. Ob das Betriebssystem auf einer virtuellen Maschine oder auf der Hardware betrieben wird, ist abhängig von der Art des pServers (siehe weiter unten in diesem Abschnitt bei der Beschreibung der Abbildung vom Managementmodell auf das Informati-

onsmodell). Die virtuelle Maschine benutzt eine virtuelle NIC, die mit einer virtuellen Bridge verbunden ist. Die drei virtuellen Komponenten werden durch den Hypervisor verwaltet. Der Hypervisor läuft wiederum auf einem Bladeserver, der über seine NIC den internen Switch benutzt. Über den internen Switch findet die Kommunikation mit dem cBlade statt. Dabei läuft Datenverkehr vom internen Switch über eine NIC des cBlades. Diese ist wiederum mit einer virtuellen Bridge verbunden, die über eine weitere NIC die Verbindung nach außen anbietet. Diese NIC ist mit dem Port eines Switches verbunden, der über einen weiteren Port mit der NIC eines PCs verbunden ist. Es werden nur die Teile des Informationsmodells von PAN gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. PAN kann zwar auch Applikationen auf Linux Gastsystemen verwalten, aber da hier speziell auf das Netz-Management eingegangen wird, ist dieser Teil ausgenommen. Das Managementmodell von PAN wurde schon in Abschnitt 2.1.2 erläutert. An dieser Stelle soll darauf eingegangen werden, wie das Managementmodell auf das Informationsmodell abgebildet wird. Die Abbildung des pServers ist abhängig von der Art des Blades, auf dem er gebootet ist. Die Abbildung ist eine andere je nachdem, ob der pServer auf einem pBlade oder einem vBlade gebootet ist. Ist er auf einem pBlade gebootet, wird er auf einen Bladeserver abgebildet. In diesem Fall ist die vEth die NIC des Bladeservers. Ist der pServer auf einem vBlade gebootet, wird er auf die Virtuelle Maschine abgebildet und seine vEth auf die virtuelle NIC. In beiden Fällen kann an der vEth eine Bandbreitenbeschränkung eingerichtet werden. Ein vSwitch wird abgebildet auf den internen Switch sowie die interne NIC des cBlades. Die rEth wird auf die virtuelle Bridge des cBlades und deren externe NIC abgebildet. Bei der Zuordnung der rEth an den vSwitch wird die VLAN-Id vergeben. Zu dem bisher erwähnten Netz hat jede Abteilung des Szenarios noch ein zusätzliches Netz. Das zweite Netz für dieses Szenario ist ein lokales Netz, bei dem der vSwitch keine rEth zugeordnet bekommt.

Arbeitsschritte

- LPAN anlegen
- vSwitches anlegen und konfigurieren
- LPAN Ressourcen zuteilen
- pServer erstellen und konfigurieren (Verwendung eines vSwitch)
- pServer starten
- Betriebssysteme und Applikationen installieren und konfigurieren
- Ereignisse auf Fehler prüfen
- Fehler lokalisieren und beheben

Zusammenfassung

Der eigentliche Ablauf des Managements dieses Szenarios mit PAN stellt sich exakt so dar, wie im vorherigen Szenario (siehe Abschnitt 4.3.2). Doch dadurch, dass sich die Desktopvirtualisierung nicht direkt an PAN anbinden lässt, werden die Managementaufgaben um eben diesen Bereich erweitert.

4 Umsetzung der Szenarien in den Modellen

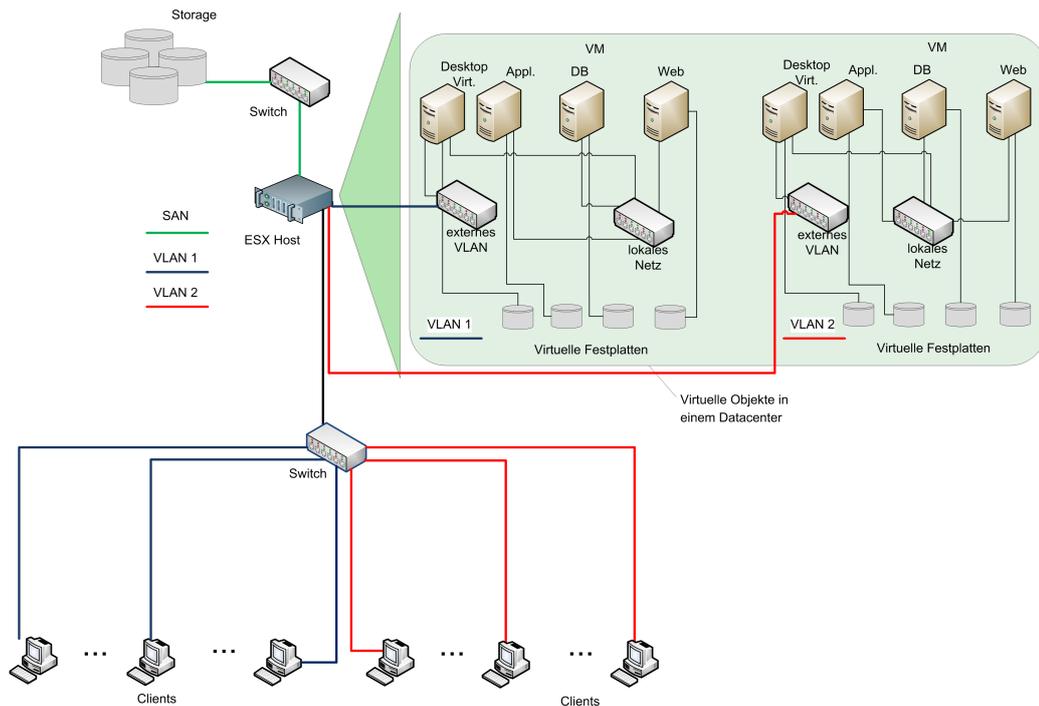


Abbildung 4.35: Szenario 2b mit VMware

Bewertung

- A1 - Aufbau** Die Infrastruktur lässt sich dem Szenario entsprechend aufbauen.
- A2 - Betrieb** Gemäß den Beschränkungen, die in Abschnitt 4.5.2 aufgeführt sind, lässt sich die Infrastruktur betreiben.
- A3 - Schnittstelle zum physischen Management** Es wird keine Schnittstelle zum physischen Management bereitgestellt.
- A4 - Automation** Die vom Szenario geforderte Automation ist bis auf die lastabhängige Migration von virtuellen Maschinen vorhanden.
- A5 - Mandantenfähigkeit** Das System ist mandantenfähig.
- A6 - Rollen- und Rechtekonzept** PAN bietet ein Rollen- und Rechtekonzept.
- A7 - Transparenz der Virtualisierungslösung** PAN ist als Virtualisierung für den Nutzer im Netzmanagement transparent.
- A8 - Darstellung der Technik** Die Darstellung der Technik als Repräsentation des PAN-Modells ist angemessen.

4.4.3 VMware

Der Aufbau in diesem Fall ist ähnlich dem aus Szenario 2a (siehe Abschnitt 4.3.3). Da hier jedoch die Desktopvirtualisierung hinzukommt, muss die Infrastruktur erweitert und etwas

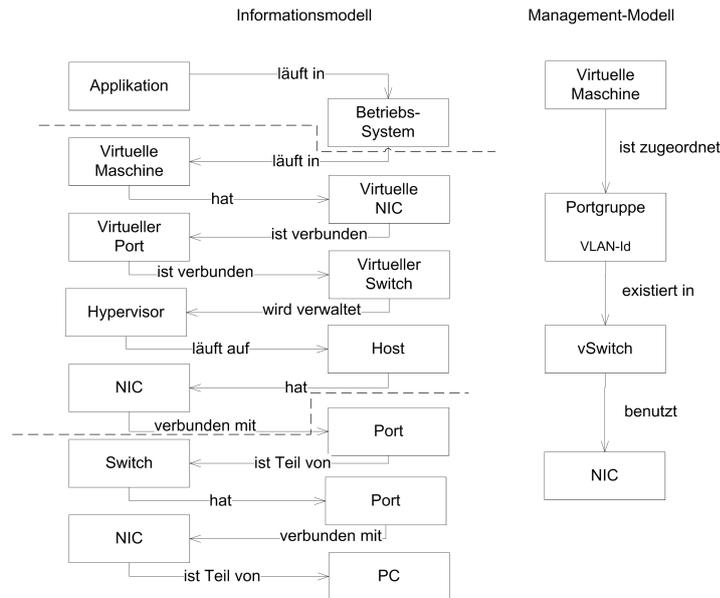


Abbildung 4.36: Informations- und Managementmodell von Szenario 2b mit VMware

anders aufgebaut werden. Dafür muss pro Abteilung eine weitere VM für die Desktopvirtualisierung und ein weiterer vSwitch mit einer Portgruppe angelegt werden. Die Verbindungen der VMs an die Portgruppen läuft pro Abteilung folgendermaßen: Die drei VMs für die Dienste der Abteilungen werden über ein lokales virtuelles Netz ohne Uplink angeschlossen. Die VM für die Desktopvirtualisierung wird sowohl an dieses, als auch an das zweite Netz angeschlossen, das ein VLAN ist und über einen Uplink verfügt. Die Thin-Clients verbinden sich über das VLAN mit der VM für die Desktopvirtualisierung, die ebenfalls auf das lokale Netz mit den drei weiteren VMs Zugriff hat. Auf der VM für die Desktopvirtualisierung ist der VDM (Virtual Desktop Manager) installiert, der die Verwaltung der virtualisierten Desktops übernimmt. Je nach Konfiguration des VDM ist es möglich die Desktop auf verschiedene Arten bereitzustellen. In diesem Fall wird die Variante 'Persistent Pool' gewählt, bei der jeder Nutzer einen Desktop aus einem Pool bekommt, der dann diesem Nutzer auch in späteren Sitzungen zur Verfügung steht. Das bedeutet, dass für jeden Nutzer dauerhaft eine eigene VM angelegt wird. Da in diesem Szenario jedoch recht kleine und genau bekannte Nutzerzahlen vorliegen, ist nicht zu erwarten, dass die permanente Bereitstellung von Desktops durch VMs zu Engpässen in der Leistung oder der Storage führt. Die VMs für die Desktops sind in Abbildung 4.35 nicht dargestellt, dafür aber der restliche schematische Aufbau.

Modelle

In Abbildung 4.36 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit VMware vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management der Netze in VMware arbeitet. Es werden nur die Teile des Informationsmodells von VMware gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. Das Informationsmodell umfasst die Applikationen, die in Betriebssystemen laufen,

über die virtuellen Maschinen, die über eine virtuelle NIC an einem virtuellen Port an einen virtuellen Switch angeschlossen sind. Dieser virtuelle Switch leitet Netzverkehr über den verwaltenden Hypervisor an den physischen Host, der ihn an die physische NIC übergibt. Die NIC ist über eine Port mit einem externen Switch verbunden, der über einen weiteren Port die Verbindung zur NIC eines PCs herstellt. Bei der Abbildung des Managementmodell auf das Informationsmodells wird wie folgt vorgegangen: Die virtuelle Maschine des Managementmodells wird auf die virtuelle Maschine des Informationsmodells abgebildet. Analog wird mit der virtuellen NIC vorgegangen. Die Portgruppe, über die die VLAN-Id verwaltet wird, wird auf virtuelle Ports abgebildet und der vSwitch auf den virtuellen Switch. Die NIC schließlich wird auf die NIC des Hosts abgebildet. Das Szenario erfordert pro Abteilung ein weiteres lokales Netz. Bei diesem wird ein vSwitch ohne Uplink über die NIC benutzt.

Arbeitsschritte

- Data Center anlegen
- vSwitches anlegen
- Portgruppen anlegen
- Storage definieren
- ESX Server Host zuweisen
- Virtuelle Maschine erstellen
- Virtuelle Maschine Portgruppe zuweisen
- Virtuelle Maschine booten
- Logs auf Fehler überprüfen
- Fehler lokalisieren und beheben

Zusammenfassung

Grundsätzlich ist hier dasselbe zu sagen, was auch bei Szenario 2a (Abschnitt 4.3.3) gilt. Jedoch ist in diesem Fall die Desktopvirtualisierung hinzugekommen, die sich zwar nicht über das Virtual Center verwalten lässt, dieses aber benutzt. Der VDM bietet eine eigenständige Managementanwendung, benutzt aber für die Umsetzung und den Betrieb der VDI die Infrastruktur des Virtual Center. Somit ist auch das Management der Desktops zumindest Teilweise in das Virtual Center integriert. Auch die Umsetzung mit getrennten lokalen Netzen für die VMs die die Dienste für die Nutzer anbieten, wird problemlos unterstützt.

Bewertung

A1 - Aufbau Die Infrastruktur lässt sich aufbauen.

A2 - Betrieb Mit den Einschränkungen aus Abschnitt 4.5.3 ist der Betrieb möglich.

A3 - Schnittstelle zum physischen Management Es wird keine Schnittstelle zum physischen Management bereitgestellt.

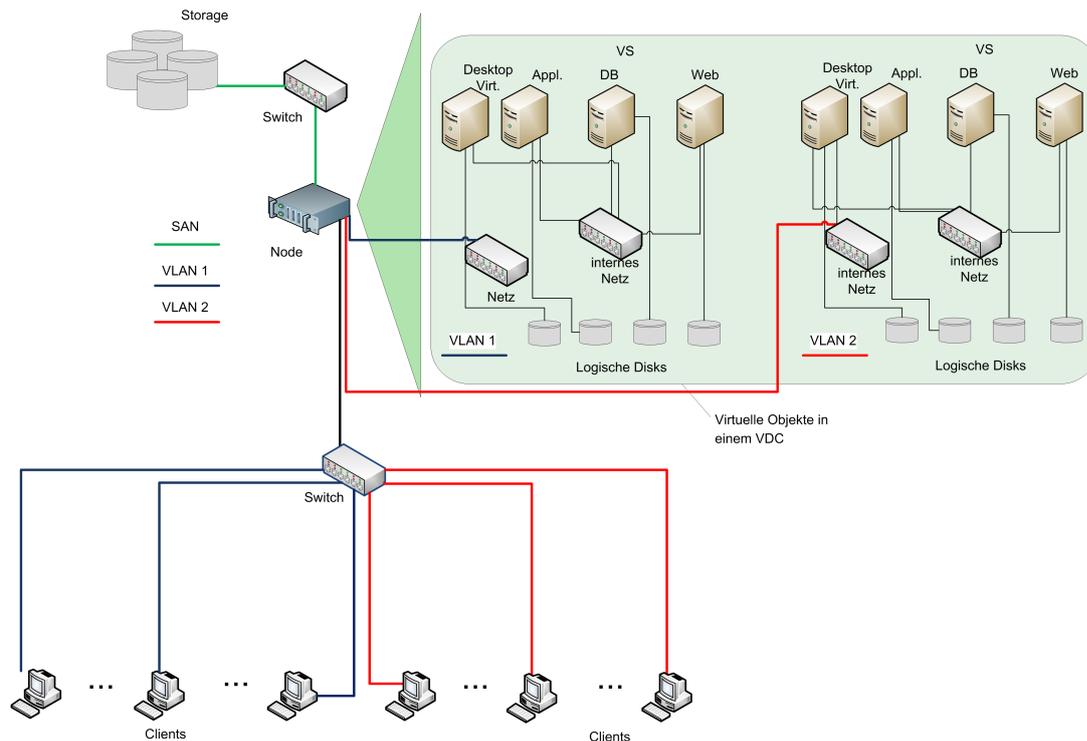


Abbildung 4.37: Szenario 2b mit VI

- A4 - Automation** Alle nötige Automation ist vorhanden.
- A5 - Mandantenfähigkeit** Das System ist mandantenfähig.
- A6 - Rollen- und Rechtekonzept** VMware bietet ein Rollen- und Rechtekonzept.
- A7 - Transparenz der Virtualisierungslösung** Das Managementmodell schafft Transparenz in der Verwendung. Es wird mit vereinfachten Konzepten gearbeitet, die die Arbeit erleichtern.
- A8 - Darstellung der Technik** Die Darstellung als Abbild des Modells von VMware ist angemessen.

4.4.4 Virtual Iron

Der Aufbau der virtuellen Infrastruktur für dieses Szenario orientiert sich wieder an dem in Abschnitt 4.3.4 beschriebenen. Die in diesem Szenario hinzukommende Desktopvirtualisierung macht es nötig, dass nochmals zwei VS zusätzlich zu den bisherigen aus Szenario 1a bereits vorhandenen bereitgestellt werden. Diese beiden VS werden, wie in Abbildung 4.37 dargestellt, jeweils für die Desktopvirtualisierung einer Abteilung eingesetzt. Zusätzlich werden zwei weitere Netze benötigt. Pro Abteilung wird ein internes Netz ohne Uplink und ein Netz mit Uplink und VLAN-Zugehörigkeit benutzt. Die vier VS sind über das interne Netz miteinander verbunden. Die VS für die Desktopvirtualisierung werden zusätzlich an das externe VLAN angeschlossen, über das die Kommunikation mit den Clients stattfindet.

4 Umsetzung der Szenarien in den Modellen

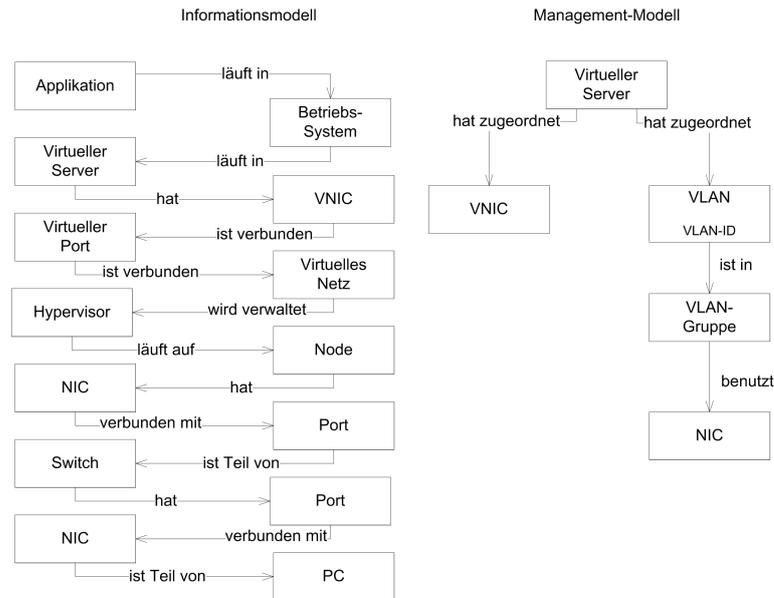


Abbildung 4.38: Informations- und Managementmodell bei Virtual Iron für Szenario 2b

Durch die Partnerschaft von Virtual Iron mit 2X und Provision Networks lassen die Produkte dieser Anbieter mit Virtual Iron kombinieren. Die genaue Integration konnte jedoch nicht getestet werden. Der Aufbau der Infrastruktur besteht aus einem Node, zwei logischen Netzen, vier VS pro Abteilung und vier logischen Disks pro Abteilung.

Modelle

In Abbildung 4.28 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit Virtual Iron vorhanden sind. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Es werden nur die Teile des Informationsmodells von Virtual Iron gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. Das Informationsmodell besteht aus den Komponenten Applikationen, Betriebssystem, virtueller Server, VNIC, virtueller Port, virtuelles Netz, Hypervisor, Node, NIC, Port, Switch, Port, NIC und PC. Diese Komponenten benutzen jeweils die auf sie folgende. Das Managementmodell von Virtual Iron wurde in Abschnitt 2.3.2 erläutert. Die Elemente des Managementmodells werden folgendermaßen auf das Informationsmodell abgebildet: Der Virtuelle Server wird auf die virtuelle Maschine des Informationsmodells abgebildet. Die virtuelle NIC wird analog dazu auf die virtuelle NIC abgebildet. Das VLAN mit der VLAN-Id wird zusammen mit der VLAN-Gruppe auf das virtuelle Netz des Informationsmodells abgebildet. Der Port des Managementmodells wird auf die NIC des Informationsmodells abgebildet. Im Managementmodell gibt es keine direkte Verbindung zwischen der virtuellen NIC und dem Port, eine solche wird aber über den virtuellen Server hergestellt. Im Informationsmodell besteht jedoch eine mittelbare Beziehung der korrespondierenden Komponenten, wodurch auch hier die Verbindung hergestellt wird. Das Szenario erfordert für ein weiteres lokales Netz, welches einfach ein weiteres virtuelles Ethernet (siehe Abschnitt 2.3.2) ohne zugeordneten Port ist.

Arbeitsschritte

- VNICs anlegen
- Netze anlegen
- Virtual Data Center anlegen
- Node zuweisen
- Logische Platten erstellen
- Virtual Server erstellen (dabei VNIC und Netz zuweisen)
- Virtual Server booten
- Logs auf Fehler überprüfen

Zusammenfassung

Auch hier ist das VI-Center eine effiziente Möglichkeit zu Verwaltung der virtuellen Infrastruktur. Leider kann keine Aussage über die Integration der Desktopvirtualisierung getroffen werden, aber vermutlich muss ein Großteil des Administrationsaufwandes mit eigenen Anwendungen bestritten werden. Jedoch bleibt auch hier zu sagen, dass ein nicht unbeträchtlicher Teil der Arbeit außerhalb des VI-Centers durchgeführt werden muss.

Bewertung

- A1 - Aufbau** Die Infrastruktur des Szenarios lässt sich aufbauen.
- A2 - Betrieb** Mit den Beschränkungen aus Abschnitt 4.5.4 ist der Betrieb der Infrastruktur möglich.
- A3 - Schnittstelle zum physischen Management** Virtual Iron stellt keine Schnittstelle zum physischen Management bereit.
- A4 - Automation** Die geforderte Automation wird angeboten.
- A5 - Mandantenfähigkeit** Das Modell ist beschränkt mandantenfähig.
- A6 - Rollen- und Rechtekonzept** Das Modell bietet kein Rollen- und Rechtesystem.
- A7 - Transparenz der Virtualisierungslösung** Das Netz-Management ist bei Virtual Iron für den Nutzer transparent.
- A8 - Darstellung der Technik** Die Darstellung der Technik entspricht den Anforderungen des Szenarios.

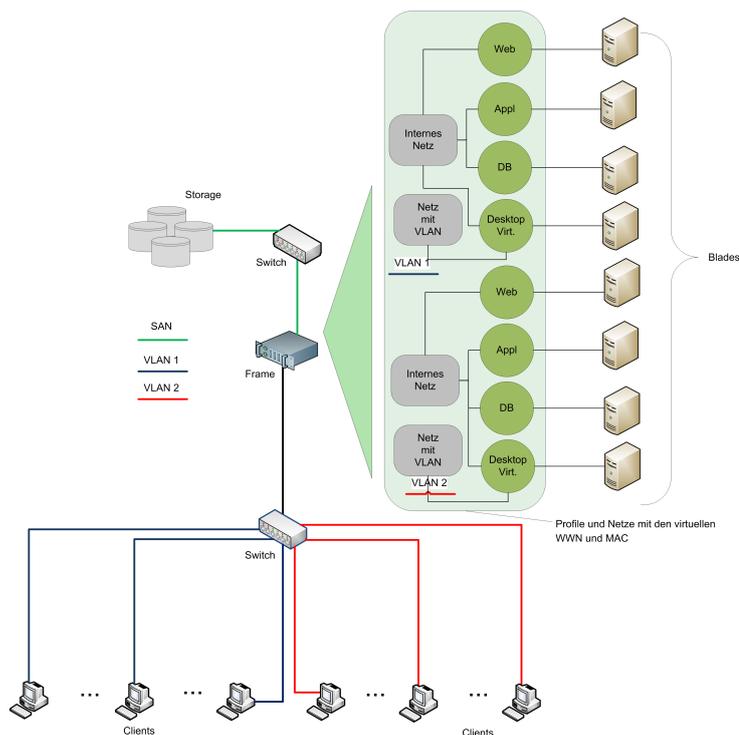


Abbildung 4.39: Szenario 2b Mit VIOM

4.4.5 VIOM

Der Eigentliche Aufbau der Infrastruktur dieses Szenarios ist wieder sehr ähnlich zu dem in Abschnitt 4.3.5 beschriebenen. Für den zusätzlichen Punkt der Desktopvirtualisierung gibt es bei VIOM keine Schnittstelle, an der er sich anfügen ließe.

Darum bleibt hier nur wieder ein Umweg über die zusätzliche Implementierung. Dazu wird für jede Abteilung ein weiteres Blade mit zusätzlichem Profil benötigt. Die Konfiguration der Netze wird anders durchgeführt als im vorherigen Szenario. Pro Abteilung wird ein 'Internes Netz' und ein 'Netz mit VLAN-Id' angelegt. An das interne Netz werden die vier Blades einer Abteilung angeschlossen. Das Blade für die Desktopvirtualisierung wird zusätzlich dazu an das VLAN-Netz angeschlossen. Über dieses Netz kommunizieren die Clients mit ihren Desktops. Mit den Profilen für die Web-, Application- und Datenbankserver wird auch, wie auch aus Abbildung 4.39 ersichtlich ist, genauso verfahren, wie vorher. Die Profile für die Desktopvirtualisierung bekommen die entsprechenden LUNs zugewiesen. Diese Profile für die Desktop-Virtualisierung werden dann noch den zwei zusätzlichen Blades zugewiesen.

Modelle

In Abbildung 4.40 sind die Informations- und Managementmodelle gegenübergestellt. Das Informationsmodell stellt die Klassen der Objekte dar, die in der Umsetzung mit VIOM vorhanden sind. Es werden nur die Teile des Informationsmodells von VIOM gemanagt, die in der Abbildung zwischen den gestrichelten Linien liegen. VIOM kennt im Informationsmodell die Applikationen, das Betriebssystem, das Blade mit einer NIC, der Slot in dem das Blade montiert ist, der Port des Slots, das Chassis, dessen Teil der Slot ist, das IBP, das Teil des

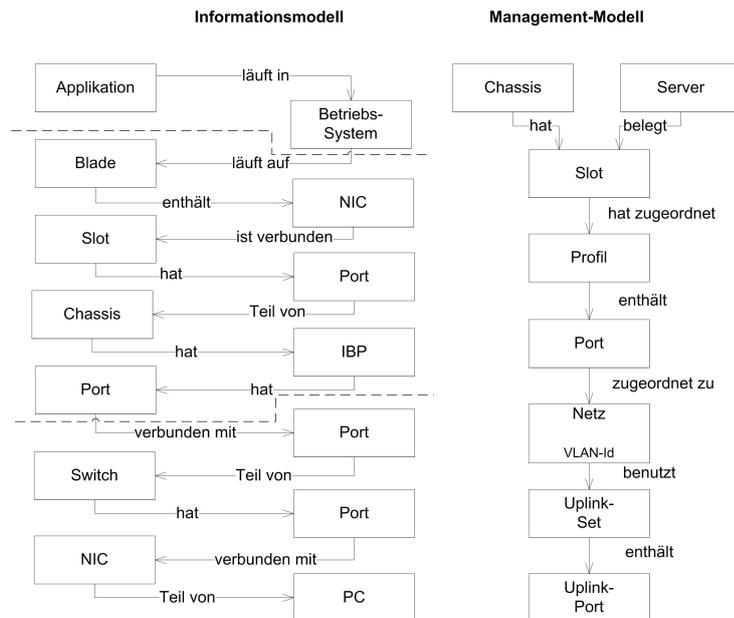


Abbildung 4.40: Informations- und Managementmodell bei VIOM für Szenario 2b

Chassis ist, die darin enthaltenen Uplink-Ports, der Port am externen Switch, der Switch selbst, ein weiterer Port, die NIC des PCs und der PC selbst. Das Managementmodell stellt die Objekte dar, mit denen der Nutzer beim Management des Netzes arbeitet. Nun wird die Abbildung der Elemente des Managementmodells auf die des Informationsmodells beschrieben. Das Chassis wird auf das Chassis und ein Server auf ein Blade abgebildet. Der Slot wird direkt auf einen Slot abgebildet. Das Profil wird auf eine Menge der Ports eines Slots im Informationsmodell abgebildet. Ein Port des Managementmodells wird auf einen Port eines Slots im Informationsmodell abgebildet. Nun wird ein Uplink-Set auf eine Menge von Ports des IBP abgebildet. Ein Netz ist eine Menge bestehend aus Ports der Slots (also der Abbildung eines Profils) und Ports des IBP (der Abbildung eines Uplink-Sets). Zusätzlich hält das Netz die VLAN-Id als Attribut. Ein einzelner Uplink-Port wird auf einen Port des IBP abgebildet. Für das zweite Netz für das Szenario wird ein weiteres Netz benötigt. Dabei handelt es sich um ein Netz ohne VLAN und ohne zugeordnetes Uplink-Set.

Arbeitsschritte

- Anlegen und Konfigurieren der Netze
- Anlegen und Konfigurieren der Profile (Verwendung der Netze)
- Zuweisen der Profile an Slots
- Booten der Blades
- Neuzuweisen eines Profils an einen anderen Slot im Fehlerfall

Zusammenfassung

Wie in Abschnitt 4.3.5 schon beschrieben, geht auch in diesem Szenario das Management mit VIOM in seiner begrenzten Welt einfach von der Hand, sobald man das Modell begriffen hat. Aber genauso kommen die Nachteile wieder zum Vorschein. Sei es in der nicht ganz intuitiven Verwendung innerhalb VIOMs, oder die Eingrenzung auf die I/O-Virtualisierung eines Frames.

Bewertung

- A1 - Aufbau** Die Infrastruktur lässt sich aufbauen.
- A2 - Betrieb** Mit Einschränkungen des Modells (siehe Abschnitt 4.5.5 kann die Infrastruktur betrieben werden.
- A3 - Schnittstelle zum physischen Management** Es steht keine Schnittstelle zum physischen Management bereit.
- A4 - Automation** Automation wird durch VIOM nicht angeboten.
- A5 - Mandantenfähigkeit** VIOM bietet ein eingeschränkt mandantenfähiges System.
- A6 - Rollen- und Rechtekonzept** Das Modell beinhaltet kein Rollen- und Rechtekonzept.
- A7 - Transparenz der Virtualisierungslösung** Das Netz-Management von VIOM schafft Transparenz.
- A8 - Darstellung der Technik** Die Darstellung der Technik entspricht den Gegebenheiten des Szenarios.

4.4.6 Bewertung für das Szenario 2b

Modell	A1	A2	A3	A4	A5	A6	A7	A8
ohne Virt.	-	-	-	-	-	-	-	+
PAN	+	o	-	o	+	+	+	+
VMware	+	o	-	+	+	+	+	+
Virtual Iron	+	o	-	+	o	-	+	+
VIOM	o	o	-	-	o	-	+	o

+: gut o: neutral -: schlecht

Tabelle 4.4: Bewertung der Virtualisierungs-Management-Modelle für Szenario 2b

In Tabelle 4.4 ist dargestellt, wie die einzelnen Virtualisierungs-Management-Modelle für dieses Szenario bewertet werden. VMware schneidet in diesem Szenario durch die gute Unterstützung der Automation am besten ab. Nur in diesem Punkt wird VMware besser bewertet als PAN. Virtual Iron hat durch die fehlende Nutzerverwaltung und die teils schwache Mandantenfähigkeit Nachteile in diesem Szenario. VIOM mangelt es zusätzlich zu Mandantenfähigkeit und dem Rollen- und Rechtekonzept auch an der Automatisierung.

4.5 Bewertung der Modelle

Nun wird noch eine generelle Bewertung der Modelle abgegeben. Dabei wird die Erfüllung der Anforderungen durch die Modelle insgesamt bewertet. In Tabelle 4.5 ist diese Bewertung der Modelle zusammengefasst. Dabei ist klar zu erkennen, dass die Umsetzung ohne Virtualisierung, wie zu erwarten war, keine der Anforderungen erfüllt. Ebenfalls ist sofort zu sehen, dass keines der Modelle die Anforderung A8 erfüllt, da keines der Modelle mit der Voraussetzung entwickelt wurde, für gering qualifizierte Nutzer einsetzbar zu sein.

Modell	A1	A2	A3	A4	A5	A6	A7	A8
ohne Virt.	✗	✗	✗	✗	✗	✗	✗	✗
PAN	(✓)	(✓)	✗	(✓)	✓	✓	✓	✗
VMware	✓	(✓)	✗	✓	✓	✓	✓	✗
Virtual Iron	✓	(✓)	✗	✓	✗	✗	✓	✗
VIOM	✗	✗	(✓)	✗	✗	✗	✓	✗

✓: erfüllt (✓): teilweise erfüllt ✗: nicht erfüllt

Tabelle 4.5: Bewertung der Virtualisierungs-Management-Modelle

Im folgenden werden nun die einzelnen Modelle gegen die Anforderungen bewertet. Dabei werden die Ergebnisse aus Tabelle 4.5 kurz textuell erläutert.

4.5.1 Ohne Virtualisierung

Die konventionelle Umsetzung ohne Virtualisierung ist nicht wirklich relevant, da sie nur zum Vergleich der Umsetzungen der Szenarien durchgeführt wurde.

4.5.2 PAN

PAN ermöglicht ein relativ übersichtliches Management großer und kleiner Infrastrukturen. Dabei können fast alle notwendigen Tätigkeiten für Aufbau (Vorlagen für virtuelle Maschinen werden nicht unterstützt) und Betrieb einer Infrastruktur durchgeführt werden. Folgende Tätigkeiten sind nicht möglich:

- Das explizite Migrieren eines pServers ist im Modell nicht vorgesehen
- Storage ist nur in Form von SCSI-Disks und -Tapes vorhanden
- Hardware, die von PAN benutzt werden kann, ist durch den jeweiligen Frame begrenzt
- Backup ist nur für PAN (die Infrastruktur selbst als DR (Disaster Recovery)) möglich. Die Disks der pServer können nicht gesichert werden
- Verwendung von Vorlagen für virtuelle Maschinen

Für das physische Management stellt PAN jedoch keine Schnittstelle zur Verfügung. PAN erkennt LUNs, die im SAN freigegeben werden zwar automatisch, aber es gibt keine Möglichkeit ein SAN zu verwalten. Dasselbe gilt für LANs. Automation wird nur in Form eines automatischen Failovers angeboten. Kann ein pServer nicht gestartet werden, wird versucht ein

anderes Blade zu benutzen (falls ein Failover-Blade festgelegt ist). PAN ist Mandantenfähig und bietet ein flexibles Rollen- und Rechtesystem an. PAN verwendet in der Präsentation des Management an allen Stellen das eigene logische Modell mit den spezifischen Begriffen und Konzepten (z.B. pServer und LPAN). Diese unterscheiden sich jedoch von dem zugrundeliegenden Informationsmodell, wodurch Transparenz erzeugt wird. Besonders ist zu erwähnen, dass intern ein Switch völlig transparent verwaltet wird. Die Darstellung der Technik entspricht dem logische Konzept von PAN. Es ist daher für professionelle Nutzer tauglich.

4.5.3 VMware

Das Management mit Virtual Center bietet die nötigen Möglichkeiten für das Anlegen virtueller Infrastrukturen an. Auch für den Betrieb lassen sich die meisten Aktionen durchführen. Folgende Aktionen sind nicht möglich:

- Das Backup der Gastsysteme an sich ist nicht möglich, kann aber über den Umweg über Snapshots durchgeführt werden.

Virtual Center bietet keine Schnittstelle zum physischen Management an. Jegliche Änderungen außerhalb der Virtualisierung müssen extern durchgeführt werden. Virtual Center kann virtuelle Maschinen automatisch verschieben, starten oder stoppen. Daher ist die Anforderung nach Automation erfüllt. Es ist auch möglich Teile der Infrastruktur getrennt von anderen zu verwalten, damit ist das System mandantenfähig. Auch die Benutzerverwaltung mit Rollen und Rechten ist vorhanden. Das Informationsmodell von VMware ist komplexer als das verwendete Managementmodell. Auch wenn eine relativ direkte Abbildung zwischen den Modellen durchgeführt wird, wird trotzdem noch Transparenz für den Nutzer erzielt. Die Darstellung der Technik ist schließlich eine dem logischen Konzept entsprechende direkte Darstellung der Technik.

4.5.4 Virtual Iron

Virtual Iron erfüllt die Anforderungen zum Erstellen einer Infrastruktur. Es lassen sich eine Vielzahl der nötigen Schritte für den Betrieb durchführen. Folgende Aufgaben lassen sich mit Virtual Iron jedoch nicht ausführen:

- Das Backup der virtuellen Maschinen lässt sich nur über den Workaround erledigen, dass Snapshots der Maschinen gemacht werden.

Virtual Iron bietet keine Schnittstelle zum physikalischen Management, ausgenommen die Möglichkeit auf SAN-Geräten logische Unterteilungen zu erstellen. Die Möglichkeiten zur Automation bieten Benachrichtigungen über Ereignisse, Starten kompletter VDC und System Backups zu festgelegten Zeiten. Es können aber auch virtuelle Server abhängig von der Systemlast der Nodes migriert werden. Teile der Infrastruktur lassen sich unabhängig von anderen Teilen verwalten, jedoch nur mit den Einschränkungen der Nutzerverwaltung. Wirkliche Mandantenfähigkeit ist dadurch nicht gegeben. Die Nutzerverwaltung von Virtual Iron kennt keine Rollen und Rechte für die Nutzer. Virtual Iron ist transparent, da das Managementmodell das Informationsmodell abstrahiert und so dem Nutzer ein abstrakteres Modell zum Management anbietet, als es das Informationsmodell wäre. Die Darstellung der Technik ist eine direkte Wiedergabe des logischen Modells von Virtual Iron.

4.5.5 VIOM

Mit VIOM kann an sich keine virtuelle Infrastruktur aufgebaut werden. Es können also auch keine virtuellen Systeme damit verwaltet werden. Jedoch lässt sich das entsprechende Frame damit verwalten. VIOM bietet damit eine Mischung aus Virtualisierung und dem Management eines physischen Systems. Es ist möglich virtuelle Adressen zu erstellen und diese an Slots eines Frames zu vergeben. Die Adressen können mit Netz-Ports verbunden werden. Vorhandene Blades können gestartet und gestoppt werden. Automation wird von VIOM nicht angeboten. VIOM ist nicht mandantenfähig und bietet keine Möglichkeit zur Vergabe von Rollen und Rechten. Das Netz-Management ist für den Nutzer bei VIOM transparent, da das Managementmodell das Informationsmodell, wenn auch nur gering, abstrahiert. Die Darstellung der Technik ist stark an dem physischen Aufbau von VIOM ausgerichtet. Daher ist sie nicht für weniger qualifizierte Nutzer geeignet.

4.6 Zusammenfassung

In diesem Kapitel wurden die Szenarien mit den Modellen aus Kapitel 2 umgesetzt. Dabei wurde überprüft, wie gut sich die Modelle für die einzelnen Szenarien eignen. Anschließend wurde eine Bewertung der Modelle durchgeführt. Als Grundlage für die Bewertung wurden die Anforderungen an ein Virtualisierungs-Management-Modell herangezogen.

5 Entwurf des neuen Modells

In diesem Kapitel wird ein neues Virtualisierungs-Management-Modell erstellt. Das Ziel ist eine abstrakte Beschreibung eines generischen Ansatzes, der es ermöglichen soll, eine virtuelle Infrastruktur unabhängig von der verwendeten Virtualisierungstechniken zu verwalten. Dabei ist Wert darauf zu legen, dass unterschiedliche Nutzeranforderungen bedient werden. Es wird von zwei Arten Nutzern ausgegangen, wie sie schon in den Szenarien in Abschnitt 3.1 beschrieben wurden. Die erste Art Nutzer ist ein nicht-professioneller Nutzer, der eine virtuelle Infrastruktur möglichst einfach verwalten will und nicht über tiefgehendes Fachwissen verfügt. Der zweite Nutzer-Typ ist ein professioneller Administrator mit entsprechendem Fachwissen, der das Management entsprechend detailliert durchführen muss.

5.1 Anforderungen

Bevor mit der eigentlichen Modellierung angefangen werden kann, müssen die Grundlagen dafür geschaffen werden. Als erstes wird auf die Anforderungen an das Virtualisierungs-Management-Modell, die in Abschnitt 3.2 aufgestellt wurden, eingegangen. Die aufgeführten Anforderungen muss das hier erstellte Modell erfüllen. Zunächst wird untersucht, was das Modell leisten muss, um den Ansprüchen zu genügen.

- A1 - Aufbau** Die Funktionalität zum Erstellen der Infrastruktur wird durch die Management-Plattform gesteuert. Das Virtualisierungs-Management-Modell muss dem Nutzer die Möglichkeit bieten, diese Funktionalität zu benutzen.
- A2 - Betrieb** Die Aktionen, die der Administrator einer Infrastruktur zum Betrieb der Infrastruktur ausführen muss, müssen durch das Virtualisierungs-Management-Modell bereitgestellt werden. Die Funktionalität wird durch die Management-Plattform erbracht.
- A3 - Schnittstelle zum physischen Management** Das Management der Virtualisierung soll möglichst den Bruch abschwächen, der zwischen den einzelnen Management-Domänen und dem Management der Virtualisierung besteht.
- A4 - Automation** Teile der Automation in einer virtuellen Infrastruktur werden bereits durch die Virtualisierungslösung oder durch die Management-Plattform erbracht. Weitere Automationen, die z.B. nicht-professionellen Nutzern die Arbeit erleichtern oder durch die Automation erst möglich machen, müssen durch das Virtualisierungs-Management-Modell erbracht werden.
- A5 - Mandantenfähigkeit** Mandantenfähigkeit wird dadurch erreicht, dass Teile der Infrastruktur getrennt voneinander gehandhabt werden. Einen wichtigen Beitrag dazu leistet das Rollen- und Rechte-Konzept.

- A6 - Rollen- und Rechtekonzept** Das Rollen- und Rechtekonzept wird durch die Management-Plattform bereitgestellt und wird durch das Virtualisierungs-Management-Modell benutzt.
- A7 - Transparenz der Virtualisierungslösung** Das Management soll Transparenz bieten. Das bedeutet, dass zugrundeliegenden Strukturen für das Management auf ein geeignetes Modell abgebildet werden, das es den Nutzern ermöglicht, ihre Aufgaben zu erledigen.
- A8 - Darstellung der Technik** Dies ist eine der großen Herausforderungen des Virtualisierungs-Management-Modell. Das Modell muss die Trennung der Nutzer durchführen und ihnen je nach Qualifikation die passenden Informationen und Möglichkeiten bieten.

Aus dieser Beschreibung werden nun die Punkte aufgelistet, die von dem Virtualisierungs-Management-Modell erfüllt werden müssen:

- Das Modell muss Management-Informationen und -Aktionen für den Nutzer bereitstellen
- Es soll zwischen professionellen und nicht-professionellen Nutzer unterschieden werden und die Präsentation des Managements entsprechend durchführen
- Um den Bruch zwischen Management-Domänen abzuschwächen, soll das Modell geeignete Maßnahmen treffen
- Um vor allem nicht-professionellen Nutzern die Arbeit zu erleichtern, muss Automation benutzt werden
- Das Modell soll mandantenfähig sein und Nutzer mit Rollen und Rechten versehen können
- Das Modell muss die Transparenz der Virtualisierung, die durch die Management-Plattform erzielt wird beibehalten und wenn möglich vergrößern

Damit ist geklärt, welche Aufgaben das Virtualisierungs-Management-Modell erfüllen können muss und es kann nun mit der Modellierung begonnen werden.

5.2 Anbindung an die Management-Plattform

Um funktionieren zu können, muss das Virtualisierungs-Management-Modell mit der Management-Plattform kommunizieren. Nach [HAN99, S. 282ff] ist der Oberflächenbaustein für die Nutzerschnittstelle zuständig. In [Bit08, S. 24f] wird im Oberflächenbaustein eine Schnittstelle definiert, über die Nutzerschnittstelle oder Anwendungen mit der Management-Plattform kommunizieren können. Im folgenden wird daher angenommen, dass die Management-Plattform eine solche Schnittstelle besitzt, die den Zugriff von außen erlaubt. Demzufolge muss das Virtualisierungs-Management-Modell in der Lage sein, auf diese Schnittstelle zuzugreifen. Da über die Art des Zugriffs, also das verwendete Protokoll keine Aussage getroffen werden kann, wird eine *Kommunikations-Schnittstelle* benötigt, die durch konkrete Implementierungen genutzt werden kann. Über diese Schnittstelle werden auf der Management-Plattform die nötigen Operationen aufgerufen. Diese Operationen ermöglichen Zugriff auf alle Daten, alle Ereignisse und alle Management-Aktionen in der betreffenden Infrastruktur.

5.2.1 Rollen und Rechte

Es wird die Authentifizierung und Autorisierung der Management-Plattform benutzt. Die Rollen werden den Nutzern anhand der Daten der Nutzerverwaltung zugewiesen. Beim Zugriff auf eine Ressource des Virtualisierungs-Management-Modell muss überprüft werden, ob ein Nutzer die nötigen Rechte über seine Rollen besitzt.

5.3 Benutzermodi

Es muss zunächst geklärt werden, wie professionellen und nicht-professionellen Nutzern das Management entsprechend ihren Nutzeranforderungen präsentiert werden kann. Ein professioneller Nutzer stellt andere Anforderungen an das Management als ein nicht-professioneller Nutzer. Um diesen Nutzeranforderungen gerecht zu werden, werden verschieden detaillierte Präsentationsstufen benötigt. Bei grobgranularen Präsentationsstufen besteht der Vorteil einer geringeren Komplexität des Virtualisierungs-Management-Modells. Jedoch würde evtl. sowohl ein professioneller als auch ein nicht-professioneller Administrator es vorziehen, die Granularität freier einzustellen. An dieser Stelle wird zunächst aus Gründen der Einfachheit eine grobgranulare Version entworfen, die jedoch noch verfeinert werden kann. Es wird im Folgenden ein zweistufiges Modell mit einem *einfachen* und einem *komplexen* Modus entwickelt.

Nun muss bestimmt werden, was in den beiden Modi angezeigt wird. Der komplexe Modus wird zumindest einen Großteil der Informationen und Möglichkeiten bieten, die ihm von der Management-Plattform angeboten werden. Der einfache Modus hingegen muss mehr Abstraktion leisten, da hier zwischen relevanten und nichtrelevanten Daten, die die Management-Plattform liefert, unterschieden werden muss.

5.3.1 Der einfache Modus

Der „einfache“ Benutzer ist eher an einer vereinfachten Darstellung seiner Infrastruktur interessiert. Er möchte alle anfallenden Aufgaben einfach erledigen, ohne zu sehr mit Details in Berührung zu kommen. Die Information, ob ein Objekt virtuell oder physisch vorhanden ist, ist für diesen Nutzer nicht oder nur wenig relevant.

Die Anforderungen an das Virtualisierungs-Management-Modell wurden zu Beginn dieses Kapitels erörtert. Diese gelten auch für diesen Modus. Die Vereinfachung dieses Modus bedingt jedoch, dass einzelne Aktionen aus den Anforderungen A1 und A2 nicht direkt durch den Nutzer ausgeführt werden sollen. Aus diesem Grund wird zunächst zusammengefasst, welche Aktionen ein Nutzer des einfachen Modus ausführen können soll. Laut der Anforderung A8 (siehe Seite 40) soll der Nutzer dabei nur die Komponenten *Server* und *Netz* kennen.

- Server aus Vorlage erstellen
- Netz erstellen
- Nutzer anlegen
- Server starten
- Server stoppen

- Verändern Server (CPU-Leistung, RAM, Netzzugehörigkeit, Festplatte(Größe, Anzahl der Platten))
- Backup
- Meldungen lesen
- Server löschen
- Netz löschen
- Nutzer löschen
- Vorlagen löschen

Damit sind nun die Aktionen aufgeführt, die der „einfache“ Nutzer ausführen können muss. Diese Aktionen lösen gegebenenfalls weitere Aktionen automatisch aus. Daher wird nun dargestellt welche Aktionen des einfachen Modus welche Aktionen des komplexen Modus benutzen. Die aufgeführten Aktionen des komplexen Modus müssen durch die Management-Plattform bereitgestellt werden, mit der das Virtualisierungs-Management-Modell betrieben wird.

Server aus Vorlage erstellen Der Nutzer erstellt einen Server durch Benutzung einer Vorlage und Angabe der nötigen Parameter. Dabei wird eine virtuelle Maschine aus der Vorlage erstellt und evtl. nötige Anpassungen werden automatisch durchgeführt.

Netz erstellen Der Nutzer kann ein Netz erstellen, bei dem er auswählen kann, ob es sich um ein internes Netz oder ein Netz mit Anbindung an das LAN handelt. Dadurch wird die Erstellung eines virtuellen Netzes mit den nötigen Eigenschaften ausgelöst.

Nutzer anlegen Es wird in der Nutzerverwaltung ein neuer Nutzer erstellt eine Rollen zugewiesen.

Starten Server Eine virtuelle Maschine wird gestartet.

Stoppen Server Eine virtuelle Maschine wird gestoppt.

Verändern Server Parameter einer virtuellen Maschine verändern. Im einfachen Modus sind das CPU, RAM und Festplatten.

Backup Das Backup, das durch den einfachen Modus ausgelöst wird, beinhaltet das Backup der Virtualisierungslösung sowie aller virtuellen Maschinen (evtl. durch Erstellung und Sichern eines Snapshots).

Nachricht lesen Treten in der Infrastruktur Ereignisse ein, seien es Fehlermeldungen oder Ereignisse, die durch das Monitoring entstehen, auf die der Nutzer reagieren muss, werden dem Nutzer Nachrichten darüber angezeigt. Der Inhalt der Nachricht muss eventuell an den Detailgrad des einfachen Modus angepasst werden. Wird eine Lösungsmöglichkeit angeboten, kann diese akzeptiert werden. Dadurch werden automatische Schritte zur Fehlerbehebung ausgelöst.

Server löschen Eine virtuelle Maschine wird gelöscht.

Netz löschen Ein virtuelles Netz wird gelöscht.

Nutzer löschen Ein Nutzer wird in der Nutzerverwaltung gelöscht.

Vorlage löschen Entfernen einer Vorlage aus dem System.

5.3.2 Der komplexe Modus

Der komplexe Modus bietet das Management mit allen Details an. Dabei sind sowohl alle virtuellen Komponenten, als auch die physischen sichtbar, soweit diese von der Management-Plattform erfasst werden. Generell werden alle Managementaktionen, die in den Anforderungen (siehe Seite 34) aufgeführt wurden unterstützt. Tatsächliche Grundlage dafür bildet jedoch die Management-Plattform, die diese Funktionalitäten anbieten muss. Das Update der Virtualisierungsplattform selbst ist eventuell nicht über das Virtualisierungs-Management-Modell und die Management-Plattform durchführbar, da es sich hierbei prinzipiell um das Update bzw. die Installation einer Anwendung handelt.

5.3.3 Rollen der Nutzer

Für die Benutzung des einfachen Modus ist es nötig, dass der Nutzer über alle Berechtigungen für alle Objekte der Infrastruktur verfügt. Das bedeutet, er muss die Rolle des Administrators der gesamten Infrastruktur in der Benutzerverwaltung eingetragen haben.

Die Rollen der Nutzer des komplexen Modus sind abhängig von ihren individuellen Aufgaben, so dass die Rollen aus der Benutzerverwaltung benutzt werden müssen.

5.4 Informationsmodell

Das Informationsmodell einer Management-Plattform definiert Klassen für die Objekte, die durch eine Plattform verwaltet werden. In [Bit08, S. 29ff] wird z.B. ein Informationsmodell für die einheitliche Verwaltung unterschiedlicher Virtualisierungslösungen entwickelt. An dieser Stelle ein gesamtes Informationsmodell zu entwerfen, das alle Klassen einer MIB (Management Information Base) enthält, wäre nicht angebracht. Das hier entwickelte Modell soll mit beliebigen Management-Plattformen arbeiten können, die jeweils mit ihre eigenen Informationsmodellen arbeiten. Für diese Zusammenarbeit muss das Informationsmodell des Virtualisierungs-Management-Modell auf das Informationsmodell der Management-Plattform abgebildet werden. Das Informationsmodell des Virtualisierungs-Management-Modell ist demnach als eine Art Schnittstelle zu einer Management-Plattform zu verstehen. Daher wird hier im Virtualisierungs-Management-Modell nur ein „abgespecktes“ Informationsmodell mit den nötigsten Klassen, die im Management benötigt werden, entworfen, um die Abbildung vom Virtualisierungs-Management-Modell auf das Informationsmodell möglichst einfach und flexibel zu gestalten. So wird eine Anpassung an ein konkretes Informationsmodell einer Management-Plattform erleichtert.

Die im folgenden entwickelten Klassen bilden das Informationsmodell, das als Grundlage für die Entwicklung eines Managementmodells dienen wird. Entwickelt wird dieses Informationsmodell auf Basis der Umsetzungen der Szenarien mit den Modellen der bestehenden

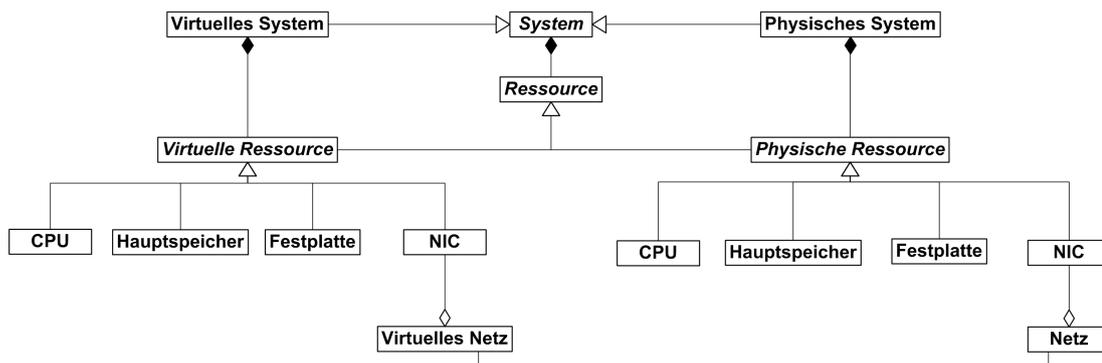


Abbildung 5.1: Informationsmodell

Lösungen aus Kapitel 4. Das Modell ist in Abbildung 5.1 dargestellt. Zunächst gibt es eine abstrakte Klasse *System*. Diese Klasse stellt die Generalisierung der beiden Typen *virtuelles System* und *physisches System*¹ dar. Ein virtuelles System repräsentiert eine virtuelle Maschine während ein physisches System die Hardwareplattform darstellt, auf der eine Virtualisierungslösung läuft. Ein System setzt sich zusammen aus *Ressourcen*, die entsprechend den Typen von Systemen in die Unterklassen *virtuelle Ressourcen*² und *physische Ressourcen* unterteilt werden. Diese Ressourcen-Klassen sind abstrakt. Unterklassen der virtuellen Ressourcen sind *CPU*, *Hauptspeicher*, *Festplatte* und *NIC*. Die physischen Ressourcen sind *CPU*, *Hauptspeicher*, *Festplatte* und *NIC*. Eine Festplatte ist ein Festspeicher, der physisch bereitgestellt wird. Dabei ist unerheblich, wie er angeschlossen ist. Eine NIC stellt die Verbindung in physische Netze dar. Weiterhin gibt es ein virtuelles Konstrukt, das *virtuelle Netz*, an dem virtuelle NICs angeschlossen sind. Soll das virtuelle Netz eine Verbindung in physische Netze haben, können physische NICs angeschlossen werden. Wie die virtuellen Festplatten letztlich realisiert und verwaltet werden, hängt von der Management-Plattform ab.

Es bleibt zu erwähnen, dass das Management der physischen Komponenten nicht die eigentliche Aufgabe des Virtualisierungs-Management-Modells ist. Sie sind im Informationsmodell enthalten, um die Möglichkeit zu bieten, zusätzlich physische Systeme im Virtualisierungs-Management-Modell abzubilden. Letztlich hängt es von den Fähigkeiten der Management-Plattform ab, ob dies möglich ist.

5.5 Managementmodell

Nun wird das Managementmodell erstellt. Zunächst müssen die Objekte, mit denen der Nutzer arbeiten soll festgelegt werden und im Anschluss daran wird festgelegt, wie das Managementmodell auf das Informationsmodell abgebildet wird. Da die beiden Modi dem

¹Die in Kapitel 2 beschriebenen Modelle benutzen teilweise unterschiedliche Arten von Hardwareplattformen. PAN und VIOM haben an sich keine einzelne Plattform, sondern einen Frame mit Blades, während VMware und Virtual Iron als Grundlage von einer einzelnen Plattform, einem Host, ausgehen. Ein Blade in einem Frame kann aber auch wieder als vollständiger Host aufgefasst und als solcher modelliert werden.

²VIOM stellt eine Ausnahme dar, da es sich hierbei im Gegensatz zu den anderen Produkten um eine Lösung zur Virtualisierung von Adressen eines Frames handelt, während die anderen Hosts und Netze virtualisieren.

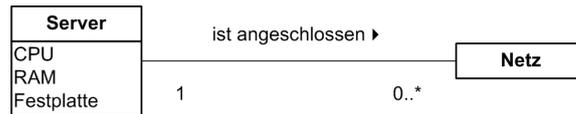


Abbildung 5.2: Managementmodell des einfachen Modus

Nutzer unterschiedlich detaillierte Sichten bieten, muss die Festlegung und die Abbildung jeweils für beide Modi durchgeführt werden.

5.5.1 Objekte des einfachen Modus

In der Anforderung A8 (siehe Abschnitt 3.2) wurde bereits beschrieben, dass der nicht-professionelle Nutzer nur mit den Objekten *Server* und *Netz* arbeiten können soll. Im Modell gibt es Klassen mit den entsprechenden Namen. Die Klasse *Server* hat Attribute, die sie beschreiben. Diese Attribute sind *CPU*, *RAM* und *Festplatte*. Die Klasse *Netz* hat kein Attribut. Um beide Klassen miteinander zu verbinden, wird eine Assoziation „ist angeschlossen“ zwischen beiden Klassen eingerichtet. Die NIC des Servers ist implizit durch die Verbindung zum Netz vorhanden. Das beschriebene Modell ist in Abbildung 5.2 zu sehen.

Um dieses Managementmodell auf das Informationsmodell abzubilden wird folgendermaßen vorgegangen: Ein Server wird auf ein virtuelles System abgebildet. Dabei werden die Attribute des Servers als die Teile der virtuellen Maschine aufgefasst. Das Attribut *CPU* wird auf die Klasse *CPU* des Informationsmodells abgebildet. Die Attribute *RAM*, *Festplatte* und *NIC* werden auf Hauptspeicher, Festplatte und *NIC* abgebildet. Das Netz wird direkt auf ein virtuelles Netz des Informationsmodells abgebildet.

5.5.2 Objekte des komplexen Modus

Um dem größeren Wissen und den daraus resultierenden höheren Anforderungen der Nutzer des komplexen Modus gerecht zu werden, wird hier ein komplexeres Managementmodell benötigt. Zunächst wird eine abstrakte Basisklasse *Maschine* benötigt. Diese ist eine Generalisierung der beiden Ausprägungen *virtuelle Maschine* und *Host*, wobei *Host* eine physische Plattform darstellt, auf der die Virtualisierung durchgeführt wird. Eine Maschine setzt sich aus den Teilen *CPU*, *Hauptspeicher*, *Festplatte* und *NIC* zusammen. Ein *Netz* ist eine gesonderte Struktur, an die NICs einer Maschine angeschlossen werden können. Die genannten Klassen und Zusammenhänge sind in Abbildung 5.3 dargestellt. Durch die Unterklassen *virtuelle Maschine* und *Host* lassen sich sowohl virtuelle als auch physische Maschinen modellieren, wobei in der Darstellung für den Nutzer nicht zwingend unterschieden werden muss, ob es sich um eine virtuelle oder eine physische Maschine handelt. Selbiges gilt für Netze. Auf dieser Grundlage können virtuelle und physische Teile einer Infrastruktur auf dieselbe Weise dargestellt und verwaltet werden.

Die Abbildung des komplexen Managementmodells wird sehr direkt durchgeführt. Eine virtuelle Maschine wird auf ein virtuelles System abgebildet. Die Klassen *CPU*, *RAM*, *Festplatte* und *NIC* werden auf die Klassen *CPU*, *Hauptspeicher*, *Festplatte* und *NIC* des Informationsmodells abgebildet. Die Klasse *Netz* wird auf die Klasse *virtuelles Netz* im Informationsmodell abgebildet. Die Abbildung der *Hosts* erfolgt analog auf die Klasse des physischen Systems. Es werden die Klassen *CPU*, *RAM*, *Festplatte* und *NIC* auf die physischen Ressourcen *CPU*, *Hauptspeicher*, *Festplatte* und *NIC* abgebildet. Das Netz schließlich

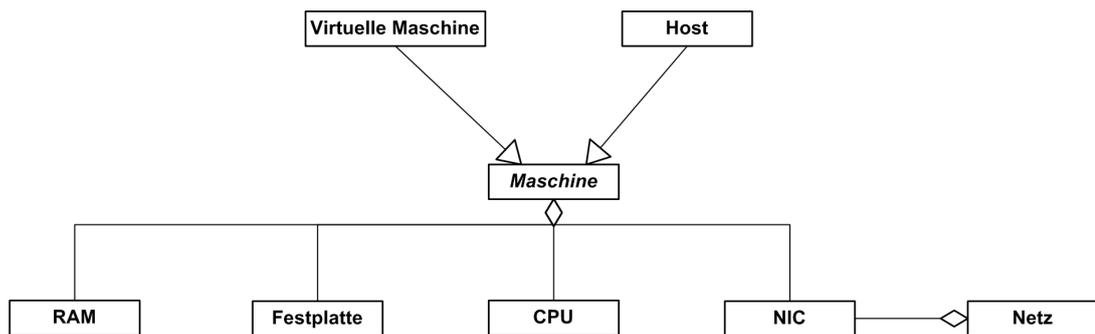


Abbildung 5.3: Managementmodell des komplexen Modus

wird auf die physische Ressource Netz abgebildet.

5.6 Management-Grenzen des Modells

Nun ist zu klären, in wie weit die physischen Ressourcen dem Management durch das Virtualisierungs-Management-Modell unterliegen sollen und umgekehrt. Wie in Anforderung A3 (siehe Seite 38) bereits beschrieben, ist es unter Umständen nicht erwünscht, Änderungen durch das Virtualisierungs-Management-Modell über dessen Grenzen hinaus zu propagieren, obwohl das durch Nutzung offener Standards wie z.B. CIM (Common Information Model) durchaus realisierbar wäre. Ein Beispiel dafür wäre das Einrichten eines VLAN in einem LAN, das durch die Erstellung eines neuen virtuellen Netzes mit einer VLAN-Id innerhalb des Virtualisierungs-Management-Modell nötig wird. In einer kleinen Infrastruktur mit nur einem Administrator kann die automatische Anpassung des LAN mit einer neuen VLAN-Id angemessen sein, da der Administrator der virtuellen Infrastruktur ebenfalls Administrator des physischen Netzes ist. In einer großen Infrastruktur, bei der das Management der virtuellen Systeme in einer anderen Management-Domäne durchgeführt wird als die Netzverwaltung, ist dies jedoch meist nicht erwünscht. Die Administratoren der virtuellen Systeme wissen in einem solchen Fall nicht, ob eine bestimmte Id vergeben werden darf oder kann. Dadurch wird klar, dass das physische Management selbst nicht durch das Virtualisierungs-Management-Modell durchgeführt werden darf, da es sonst, abgesehen von Problemen mit der organisatorischen Struktur, zu Inkonsistenzen der Konfiguration kommen kann. Stattdessen muss definiert werden, wie die Kommunikation zwischen den einzelnen Management-Domänen und dem Management mittels des Virtualisierungs-Management-Modell realisiert werden kann, um diesen Bruch im Management und die daraus resultierende Fehlerquelle zu mindern.

Auf Änderungen außerhalb der Virtualisierung kann das Virtualisierungs-Management-Modell nicht automatisch reagieren. Sie haben zwar evtl. Auswirkungen auf die virtuellen Infrastrukturen, aber sie sind für das Virtualisierungs-Management-Modell nicht direkt feststellbar.

Durch das Rollen und Rechtekonzept, über das das Virtualisierungs-Management-Modell verfügen soll, können den Administratoren der anderen Management-Domänen jedoch die entsprechenden Berechtigungen für die Objekte der virtuellen Infrastruktur erhalten, die als physische Objekte ebenfalls in ihre Zuständigkeit fallen würden. Damit ist die eine Richtung der Abhängigkeiten der administrativen Domänen erfüllt. Es bleibt die Frage, wie Änderun-



Abbildung 5.4: Ablauf der Anfrage

gen der physischen Infrastruktur veranlasst bzw. deren Notwendigkeit kommuniziert werden können, wenn diese durch Aktionen des Virtualisierungs-Management-Modell bedingt sind. Hierbei ist ein einfaches System denkbar, das die nötigen Anpassungen als Anfrage in Textform per Email an die zuständigen Managementdomänen verschickt. Die jeweiligen Administratoren können dann die Anpassungen durchführen oder die Anfrage zurückweisen. Die Administratoren der virtuellen Infrastruktur müssten dann im Fall der Zurückweisung durch interne Anpassung und erneute Anfrage auf Änderung reagieren. Es wäre denkbar, die internen Modifikation von einem positiven Bescheid von außen abhängig zu machen und diese dann automatisch durchzuführen. Jedoch kann ein solcher automatischer Mechanismus auch wieder unerwünscht sein. Letztlich wäre die zuletzt genannte, automatische Variante vermutlich die am geeignetste, da sie eine funktionierende Konfiguration gewährt. Jedoch besteht das Problem, dass Modifikationen in der virtuellen Infrastruktur nicht sofort ausgeführt werden können, da sobald Änderungen innerhalb der Infrastruktur die äußere Infrastruktur betreffen, diese erst nach den durchgeführten und bestätigten Anpassung außen durchgeführt werden können.

Deswegen wird folgende Variante favorisiert (dargestellt in Abbildung 5.4): Der Administrator der virtuellen Infrastruktur führt Änderungen durch, die Änderungen außerhalb bedingen. Bei Durchführung der Änderung veranlasst der Administrator eine Benachrichtigung, deren Empfänger (Administratoren der jeweiligen Bereiche) und Inhalt (nötige Änderungen) er mit angibt. Die Benachrichtigung mit der Anfrage zu den nötigen Änderungen wird vom System per Email verschickt. Die externen Administratoren haben nun die Möglichkeit, die Änderungen zu akzeptieren und durchzuführen oder aber sie zurückzuweisen und einen alternativen Vorschlag zu machen. Wird die Änderung akzeptiert ist der Vorgang zu Ende, wird sie zurückgewiesen, müssen die internen Änderungen überarbeitet werden und der Ablauf beginnt von neuem. Auch hierdurch wird eine fehlerfreie Konfiguration gewährt und die jeweiligen Zuständigkeiten bleiben gewahrt.

5.7 Automationen des Virtualisierungs-Management-Modell

In Anforderung A4 (siehe Seite 39) wurde automatisches Verhalten beschrieben, das das System leisten soll. Vieles davon wird durch die Virtualisierungslösungen selbst schon erbracht. Hier wird nun aufgelistet, welche automatischen Abläufe das Virtualisierungs-Management-Modell selbst bereitstellen muss.

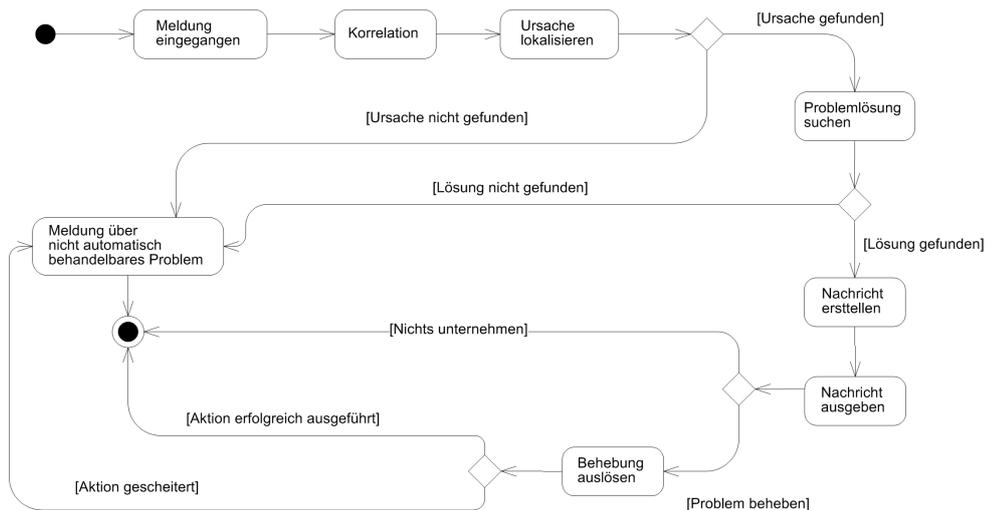


Abbildung 5.5: Ablauf der Vereinfachung von Meldungen

5.7.1 Erstellen von virtuellen Maschinen aus Vorlagen

Der Nutzer soll nur so wenig Daten wie möglich angeben müssen. Die erstellte virtuelle Maschine wird erstellt und mit den angegebenen Parametern konfiguriert. Zusätzlich werden nicht angegebene Parameter durch das System gesetzt.

5.7.2 Konfiguration von virtuellen Netzen

Im einfachen Modus ist es nicht möglich, den Nutzer mit einer detaillierten Konfiguration der virtuellen Netze zu beauftragen. Daher kann ein Nutzer dort nur ein Netz anlegen. Die Konfiguration desselben muss automatisch geschehen.

5.7.3 Erstellung von zeitlich gesteuerten Aufgaben

Um die Arbeit zu erleichtern, soll es möglich sein, Aufgaben zeitlich gesteuert automatisch auszuführen. Dazu kann für jede Aktion des Virtualisierungs-Management-Modells, die keine Nutzerinteraktion benötigt, ein Auftrag angelegt werden. Zur Erstellung wird die Aktion ausgewählt, ein Zeitpunkt, gegebenenfalls ein Intervall, angegeben, wann die Aktion ausgeführt werden soll. Diese Aufträge werden dann zur gegebenen Zeit automatisch ausgeführt.

5.7.4 Vereinfachung von Meldungen an den Nutzer und Reaktion auf Ereignisse

Meldungen über Fehler in der Infrastruktur müssen vom Virtualisierungs-Management-Modell an den Nutzer weitergeleitet werden. Fehlermeldungen sind gewöhnlich stark an der Technik orientiert. Ein Nutzer des einfachen Modus hat bedingt durch den Modus einen begrenzten Bezug zur Technik, wodurch das Verständnis und eine geeignete Reaktion auf die Meldung, eingeschränkt ist. Daher muss die Meldung so bearbeitet werden, dass der Inhalt derselben technischen Ebene entspricht, wie die Präsentation der Technik des Modus. In Abbildung 5.5 wird der gesamte Ablauf der im Folgenden aufgeführten Schritte dargestellt. Dort ist zu sehen, wie die einzelnen Aufgaben zusammenarbeiten.

Korrelation

Eventuell zusammenhängende Fehlermeldungen sollen, so weit möglich, korreliert werden, um die Ursache bestimmen zu können und um dem Nutzer möglichst wenige Meldungen zu präsentieren.

Ursachen finden

Um auf eventuell zusammenhängende Fehler reagieren zu können, müssen deren Ursachen identifiziert werden. Falls keine Ursache identifiziert werden konnte, wird der Nutzer aufgefordert, Support zu beantragen.

Problemlösungen vorschlagen

Abhängig von der identifizierten Ursache der Meldungen schlägt das System Lösungen vor. Kann das System keine Lösungen vorschlagen, wird dem Nutzer empfohlen Support zu beantragen.

Nachricht an Nutzer ausgeben

Die erstellte Nachricht wird dem Nutzer angezeigt. Die Nachricht besteht aus einer angepassten Beschreibung der Ursache, falls diese identifiziert werden konnte und, falls vorhanden, einem Lösungsvorschlag.

Lösungsvorschläge ausführen

Akzeptiert der Nutzer einen Lösungsvorschlag führt das System diesen aus und informiert den Nutzer über die Aktion und deren Erfolg.

5.7.5 Weitere Automationen

In der Anforderung A4 werden einige Arten von Automationen beschrieben. Bisher wurden an dieser Stelle die Automationen aufgeführt, die durch die Management-Plattform nicht erbracht werden, und durch das Virtualisierungs-Management-Modell geleistet werden müssen. Andere automatische Abläufe, wie das dynamische, z.B. lastabhängige, Verhalten von virtuellen Maschinen werden durch die Virtualisierungslösung selbst erbracht. Zu von der Management-Plattform erbrachten Automationen gehört beispielsweise die Reaktion auf Verletzungen von QoS-Parametern.

5.8 Ansichten

Die Darstellung der Infrastruktur und ihrer Teile ist abhängig von dem Modus, in dem der Nutzer arbeitet. Um darzustellen, welche Elemente in welcher Schärfe in welchem Modus angezeigt werden, werden zunächst die verschiedenen benötigten Ansichten definiert.

Infrastruktur Die Infrastruktur-Ansicht gibt eine Übersicht über die virtuelle Infrastruktur als Ganzes.

Server Die Server-Ansicht bietet eine Darstellung der vorhandenen virtuellen Maschinen der Infrastruktur.

Netze In der Server-Ansicht werden die virtuellen Netze der virtuellen Infrastruktur angezeigt.

Ressourcen Die Ressourcen-Ansicht bietet einen Überblick über die Ressourcen die in der Infrastruktur zur Verfügung stehen.

Nutzer In der Nutzer-Ansicht werden die Nutzer und Rollen angezeigt und können bearbeitet werden.

Nun muss für jede Ansicht festgelegt werden, welche Informationen und Aktionen in welchem Modus angezeigt werden.

5.8.1 Infrastruktur-Ansicht

Diese Ansicht bietet einen Überblick über die virtuelle Infrastruktur.

Einfacher Modus

Informationen

- *Infrastruktur*
 - Liste der vorhandenen Server
 - Liste der vorhandenen Netze
 - Liste der vorhandenen Vorlagen
- *Nachrichten*
 - Alle Nachrichten der Infrastruktur

Aktionen

- *Infrastruktur*
 - Starten Server
 - Stoppen Server
 - Server hinzufügen
 - Netz hinzufügen
 - Backup erstellen
 - Zustand aus Backup wiederherstellen

Komplexer Modus

Informationen

- *Infrastruktur*
 - *Virtuelle Maschinen*
 - * Liste der vorhandenen virtuelle Maschinen
 - Mögliche Gruppierung:

- Rechenzentren – enthalten Gruppen oder Hosts
- Gruppen – enthalten Hosts
- Hosts enthalten VMs
- *Netze*
 - * Liste der vorhandenen Netze
- *Hosts*
 - * Liste der vorhandenen Hosts
- *Vorlagen*
 - * Liste der vorhandenen Vorlagen
- *Nachrichten*
 - Alle Nachrichten der Infrastruktur

Aktionen

- *Infrastruktur*
 - Starten Server
 - Stoppen Server
 - Server hinzufügen
 - Netz hinzufügen
 - Backup erstellen
 - Zustand aus Backup wiederherstellen
 - Host hinzufügen
 - Rechenzentrum hinzufügen
 - Gruppe hinzufügen
 - Rechenzentrum entfernen
 - Gruppe entfernen
 - Gruppe Rechenzentrum zuweisen
 - Host Rechenzentrum zuweisen
 - Host Gruppe zuweisen

5.8.2 Server-Ansicht

In dieser Ansicht werden Details zu den vorhandenen virtuellen Maschinen angeboten.

Einfacher Modus

Informationen

- *Konfiguration*
 - CPU
 - * Anzahl
 - * Leistung
 - Hauptspeicher
 - * Menge
 - Festplatte
 - * Anzahl
 - * Menge
- *Leistung*
 - CPU-Auslastung
 - Hauptspeicher-Auslastung
 - Festplatte-Belegt
- *Nachrichten*
 - Alle Nachrichten dieses Servers

Aktionen

- *Konfiguration*
 - Bearbeiten:
 - * CPU
 - Anzahl
 - Leistung
 - * Hauptspeicher
 - Menge
 - * Festplatte
 - Anzahl
 - Größe
 - Server löschen
 - Server starten
 - Server stoppen

Komplexer Modus

Informationen

- *Konfiguration*
 - CPU
 - * Anzahl
 - * Leistung
 - Hauptspeicher
 - * Menge
 - Festplatte
 - * Anzahl
 - * Menge
 - Virtuelle NIC
 - * Anzahl
 - * MAC
 - Dynamisches Verhalten der virtuellen Maschine
- *Leistung*
 - CPU-Auslastung
 - Hauptspeicher-Auslastung
 - Festplatte-Belegt
- *Nachrichten*
 - Alle Nachrichten dieser virtuellen Maschine

Aktionen

- *Konfiguration*
 - Bearbeiten
 - * CPU
 - Anzahl
 - Leistung
 - * Hauptspeicher
 - Menge
 - * Festplatte
 - Anzahl
 - Größe
 - * Virtuelle NIC
 - Anzahl

- MAC
 - * Dynamisches Verhalten
 - Virtuelle Maschine auf anderen Host migrieren
 - Virtuelle Maschine löschen
 - Virtuelle Maschine starten
 - Virtuelle Maschine stoppen

5.8.3 Netz-Ansicht

In der Netz-Ansicht ist das Management der virtuellen Netze möglich.

Einfacher Modus

Informationen

- *Konfiguration*
 - Name des Netzes
 - Angeschlossene Server
- *Nachrichten*
 - Alle Nachrichten dieses Netzes

Aktionen

- *Konfiguration*
 - Netz löschen

Komplexer Modus

Informationen

- *Konfiguration*
 - Name des Netzes
 - Virtueller Switch
 - * Uplinks
 - * Bandbreite
 - * VLAN-Zugehörigkeit
- *Nachrichten*
 - Alle Nachrichten dieses virtuellen Netzes

Aktionen

- *Konfiguration*
 - Bearbeiten
 - * Name
 - * Uplinks
 - * Bandbreite
 - * VLAN-Zugehörigkeit
 - Netz löschen

5.8.4 Ressourcen-Ansicht

In der Ressourcen-Ansicht werden im einfachen Modus die Vorlagen verwaltet. Der komplexe Modus verwaltet zusätzlich die Hosts.

Einfacher Modus**Informationen**

- *Vorlagen*
 - Vorlagen
 - * Name
 - * Gastsystem

Aktionen

- *Vorlagen*
 - Vorlagen
 - * Löschen

Komplexer Modus**Informationen**

- *Hosts*
 - Konfiguration
 - * CPU
 - Anzahl
 - Auslastung
 - * Hauptspeicher
 - Größe
 - Auslastung
 - * NIC

5 Entwurf des neuen Modells

- MAC-Adresse
- Bandbreite
- Auslastung
- * HBA
 - WWN
 - Auslastung
- *Vorlagen*
 - Name
 - Gastsystem

Aktionen

- *Hosts*
 - Starten
 - Stoppen
- *Vorlagen*
 - Anlegen
 - Löschen
 - Ändern
 - * Name

5.8.5 Nutzer-Ansicht

Diese Ansicht bietet Möglichkeiten zur Verwaltung der Nutzer.

Einfacher Modus, Komplexer Modus

Informationen

- *Übersicht*
 - Liste der Nutzer
 - Liste der Rollen
- *Nutzer*
 - Name
 - Rollen
- *Rolle*
 - Name
 - Berechtigungen

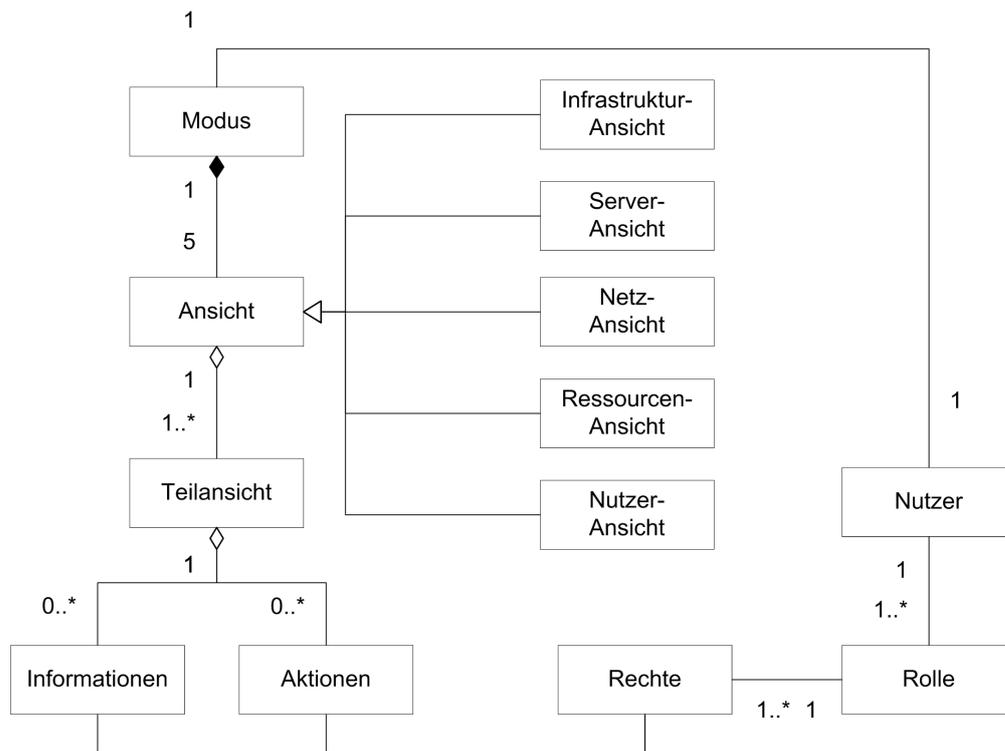


Abbildung 5.6: Modell der Ansicht

Aktionen

- *Übersicht*
 - Nutzer Anlegen
 - Rolle anlegen
 - Nutzer löschen
 - Rolle löschen
- *Nutzer*
 - Bearbeiten Nutzer
 - * Name
 - * Rollen
- *Rolle*
 - Bearbeiten Rollen
 - * Name
 - * Berechtigungen

5.8.6 Modell der Ansichten

In Abbildung 5.6 wird die Modellierung der Ansichten dargestellt. Darin ist zu sehen, dass ein Modus fünf Ansichten hat, die durch die eben beschriebenen Ansichten (Infrastruktur-, Server-, Netz-, Ressourcen- und Nutzer-Ansicht) definiert werden. Dabei besteht eine Ansicht aus ein oder mehreren Teilansichten. Die Teilansichten beinhalten jeweils die Informationen und Aktionen die in den Abschnitten 5.8.1 bis 5.8.5 beschrieben wurden. Die in den genannten Abschnitten kursiv gedruckten Begriffe stellen die Teilansichten dar. Diese würden sich in einer GUI z.B. durch Reiter umsetzen lassen, während auf die Ansichten selbst über ein Navigationsmenü wie es von Webseiten bekannt (oder in den Abbildungen 2.4, 2.7, 2.10 jeweils auf der linken Seite zu sehen) ist, zugegriffen werden kann. Der Zugriff auf Informationen und Aktionen wird über Rollen gesteuert, die der jeweilige Nutzer inne hat. Die Rollen bestimmen die Rechte, die der Nutzer auf Informationen und Aktionen hat. Ob die jeweiligen Informationen und Aktionen für einen Nutzer verfügbar sind, ist demnach von seinen Rollen abhängig. Ein Nutzer benutzt in dem Modell genau einen Modus.

5.9 Erfüllung der Anforderungen

Dass das hier entworfene Modell alle gestellten Anforderung erfüllt, wird nun gezeigt.

- A1 - Aufbau** In beiden Modi ist es, teils durch Automation, möglich die nötigen Elemente anzulegen. Damit gilt diese Anforderung als erfüllt.
- A2 - Betrieb** In beiden Modi können alle nötigen Schritte unternommen werden, die zum Betrieb einer virtuellen Infrastruktur nötig sind, wodurch die Anforderung als erfüllt zu betrachten ist.
- A3 - Schnittstelle zum physischen Management** Es ist eine Schnittstelle zum physischen Management gegeben, die dabei unterstützt eine fehlerfreie Konfiguration zu erhalten. Dadurch kann der Bruch zwischen den Management-Domänen zwar nicht behoben werden, trotzdem bietet das Modell eine Abschwächung des Bruches und bietet einen Mechanismus, der konsistente Konfigurationen erleichtert. Damit ist die Anforderung als erfüllt zu betrachten.
- A4 - Automation** Das Virtualisierungs-Management-Modell bietet die nötigen Automationen an. Dies sind teilweise Verknüpfungen von einfachen Managementaktionen, die sonst einzeln ausgeführt werden müssen, aber auch Vereinfachungen für den Nutzer. Dadurch lässt sich die Anforderung als erfüllt betrachten.
- A5 - Mandantenfähigkeit** Das System ist mandantenfähig, da einzelne Teile der Infrastruktur vom Modell unabhängig von anderen sind. Das zeigt sich in der Modellierung aller Teile als einzelne Typen. Jeder Teil des Managementmodells (Maschinen, Netze) sind unabhängig von anderen Teilen. Ebenso können virtuelle Maschinen gruppiert werden, so dass sie sich unabhängig von anderen Gruppierungen verwalten lassen.
- A6 - Rollen- und Rechtekonzept** Durch Benutzung der Benutzerverwaltung der Management-Plattform können die Rollen und Rechte im Virtualisierungs-Management-Modell benutzt werden. Würde die Management-Plattform diese Funktionalität nicht bieten, wäre das Virtualisierungs-Management-Modell nicht zu gebrauchen.

A7 - Transparenz der Virtualisierungslösung Im einfachen Modus wird eine größere Abstraktion durchgeführt, als im komplexen Modus. Jedoch wird in beiden Modi das Management transparent angeboten. Auch wenn das Managementmodell des komplexen Modus quasi dem Informationsmodell entspricht, ist durch die Abbildung des Informationsmodells des Virtualisierungs-Management-Modell auf das der Management-Plattform vorhanden.

A8 - Darstellung der Technik Durch die Nutzung der unterschiedlichen Modi werden den Nutzern die Details angezeigt, die für ihre Qualifikation angemessen sind. Die Ansichten bestimmen ihren Inhalt je nach Modus, wobei noch die Berechtigungen des Nutzers mit einbezogen werden, ob ein Inhalt angezeigt wird oder nicht. Damit wird gewährleistet, dass ein Nutzer das Management entsprechend seiner Qualifikation durchführen kann. Durch die Modi ist der Technikbezug in den Ansichten definiert, wodurch die Anforderung erfüllt ist.

5.10 Zusammenfassung

Dieses Kapitel dient dem Entwurf des Virtualisierungs-Management-Modells. Zu Beginn wurde erfasst welche Fähigkeiten das Modell benötigt, um die Anforderungen zu erfüllen. Anschließend wurde das Modell schrittweise entwickelt und dargestellt. Zum Ende des Kapitels wurde die Erfüllung der Anforderungen durch das Modell überprüft.

6 Zusammenfassung und Ausblick

In diesem Kapitel wird die vorliegende Arbeit resümiert und es wird auf die Fähigkeiten des Modells eingegangen. Weiterhin wird aufgezeigt, wie das Modell weiterentwickelt werden kann.

6.1 Zusammenfassung

Zu Beginn der Arbeit wurde das Thema eingegrenzt und der Begriff Virtualisierungs-Management-Modell definiert. Dieser Begriff beschreibt das Modell, das in dieser Arbeit zu erstellen war. Ziel dieser Arbeit war die Erstellung eines generischen Management-Modells für virtuelle Infrastrukturen, um sowohl professionellen, als auch nichtprofessionellen Nutzern das Management einer solchen Infrastruktur zu ermöglichen. Dabei sollte die verwendete Virtualisierungslösung keine Rolle für das Management spielen. Diese Abstraktion von dem verwendeten Produkt wird durch die Verwendung einer Management-Plattform erreicht, die verschiedene Virtualisierungslösungen managen kann und ein vereinheitlichtes Management anbietet. Das Virtualisierungs-Management-Modell bildet dabei die Grundlage für eine Benutzeroberfläche für eine solche Plattform. Daraufhin wurden Grundlagen der Virtualisierung erklärt, mit denen im Rahmen der Arbeit gearbeitet wurde. Anschließend wurde das Vorgehen und der Aufbau der Ausarbeitung beschrieben.

In Kapitel 2 wurden dann die existierenden Modelle vorgestellt, die getestet wurden um einen Vergleich der Modelle erstellen zu können und um Erfahrungen zu sammeln, wie bereits existierende Produkte ihren Nutzern das Management anbieten.

Die Beschreibung der Szenarien wurde in Kapitel 3 durchgeführt. Mit Hilfe dieser Szenarien werden die Modelle aus dem vorhergehenden Kapitel getestet. Weiterhin wurden in diesem Kapitel die Anforderungen formuliert, die an ein Virtualisierungs-Management-Modell gestellt werden.

Kapitel 4 beschreibt die Umsetzung der Szenarien mit den zuvor beschriebenen Modellen. Dabei wurde jedes Szenario mit allen Modellen umgesetzt. Zusätzlich wurde ein „klassischer“ Aufbau ohne Virtualisierung beschrieben, der als Vergleich zum traditionellen Management dienen soll. Es wurde für jedes Szenario bewertet, ob die Möglichkeiten der Modelle für das Szenario genügen oder nicht. Anschließend an die Umsetzungen der Szenarien wurde eine generelle Bewertung der Modelle anhand der Anforderungen durchgeführt.

Der Entwurf des Virtualisierungs-Management-Modells wurde schließlich in Kapitel 5 durchgeführt. Dabei wurde ein Modell entworfen, das den gestellten Anforderungen entspricht. Mit ihm ist es möglich, den unterschiedlichen Ansprüchen unterschiedlicher Nutzergruppen gerecht zu werden. Dazu werden zwei Modi angeboten, die das Management einer Infrastruktur entsprechend der unterschiedlichen Nutzeranforderungen unterstützen. Die Ansichten und ihre Inhalte wurden für beide Modi definiert. Desweiteren werden Mechanismen angeboten, die die Kommunikation mit anderen Management-Domänen unterstützen, und die Arbeit des Nutzers durch Automation erleichtern.

6.2 Ausblick

Das vorliegende Modell wurde mit dem Schwerpunkt Netze entworfen. Weitere Teile von Infrastrukturen, beispielsweise Storage, wurden nur am Rande beachtet. Darin liegt Potential für Weiterentwicklungen.

Im vorliegenden Modell wurde High Availability (Optionen zur Hochverfügbarkeit) nicht berücksichtigt. Die Modelle, die High Availability unterstützen, haben unterschiedliche Ansätze mit diesem Thema umzugehen. Ist die Management-Plattform in der Lage das Thema High Availability einheitlich zu handhaben, kann das Virtualisierungs-Management-Modell um diesen Punkt erweitert werden.

Ebenso verhält es sich mit der Definition und Einhaltung von QoS-Parametern. Sofern eine Management-Plattform vorhanden ist, die die Dienstgüte angemessen steuern kann, ist es möglich das Modell zu erweitern.

a) Je nach Bedarf könnte es interessant sein, die Granularität der Modi zu verfeinern. So könnten verschieden komplexe Ansichten erstellt werden, die den Nutzern gerade so viel Details bieten, wie es nötig ist. Insbesondere ist auch ein System denkbar, bei dem die Schärfe modifizierbar ist. Ein Nutzer kann im einfachen Modus starten und bei Bedarf immer weiter in die Details „hinabsteigen“. Dasselbe wäre dann ebenfalls in die umgekehrte Richtung möglich.

Das Management der Desktops ist nicht integriert. Das wäre jedoch vor allem für den einfachen Modus interessant. Das ist zum Teil darauf zurückzuführen, dass das Desktopmanagement ein anderer Management-Bereich ist, der eigene Tools einsetzt. Andererseits muss die Management-Plattform zur Integration in der Lage sein. Weiterhin wäre es möglich, das Management der Desktopvirtualisierung mit einzubeziehen. Die Fehlende Integration in das Management der Virtualisierung am Markt zeigen auch die Erfahrungen in Abschnitt 4.4.

Weiterhin vorteilhaft wäre, zumindest im einfachen Modus, das Management der Betriebssysteme mit aufzunehmen. Auch die Kontrolle der dort angebotenen Dienste durch das Virtualisierungs-Management-Modell wäre von Vorteil. Ebenso wäre es dafür wünschenswert, das Management der physischen Systeme mit einzubeziehen. Das wäre durch die Struktur des Virtualisierungs-Management-Modell möglich, da die verwalteten Systeme von der Modellierung her auch ebenso gut physische Systeme sein können. Hierfür muss jedoch die Management-Plattform die nötigen Grundlagen bereitstellen. Technisch gesehen wäre dieses Vorhaben z.B. durch die Verwendung von CIM machbar.

Für die automatische Bearbeitung von Nachrichten für den einfachen Modus müssen Mechanismen entwickelt werden, die automatisch Lösungsvorschläge anbieten können. Das könnte trivialerweise der Neustart der betreffenden Komponente sein, oder ein anderer, durch komplexeres Untersuchen gefundener Schritt. Ebenso fehlt ein Mechanismus zur Umformulierung der Nachrichten.

Die letzte Idee zur Vervollkommnung des Modells ist eine dienstorientierte Sicht auf die Infrastruktur. Diese sollte den Zustand der in der Infrastruktur angebotenen Dienste anzeigen. So kann auf einen Blick festgestellt werden, ob die Dienste, für die die Infrastruktur betrieben wird, angemessen laufen.

Abbildungsverzeichnis

1.1	Einordnung der Aufgabenstellung	2
2.1	Hardware Struktur eines BladeFrame auf dem PAN eingesetzt werden kann (aus [Ege07])	10
2.2	Logische Struktur von PAN	12
2.3	Das Netz-Management-Modell bei PAN	13
2.4	Screenshot des Pan Manager Dashboards	14
2.5	Basiskomponenten einer VMware-Infrastruktur (aus [VMw08a])	17
2.6	Das Netz-Management-Modell bei VMware	18
2.7	Der VI-Client	20
2.8	Schematischer Aufbau einer VI-Infrastruktur (aus[Vir08])	21
2.9	Das Netz-Management-Modell bei Virtual Iron	22
2.10	Screenshot des VI-Centers mit angezeigtem Resource Center	23
2.11	Schematische Darstellung des VIOM-Aufbaus	25
2.12	Das Netz-Management-Modell bei VIOM	27
3.1	Szenario 1a	30
3.2	Szenario 1b	31
3.3	Szenario 2a	32
3.4	Szenario 2b	33
4.1	Szenario 1a Ohne Virtualisierung	44
4.2	Informations- und Managementmodell ohne Virtualisierung für Szenario 1a	45
4.3	Szenario 1a mit PAN	47
4.4	Informations- und Managementmodell bei PAN für Szenario 1a	48
4.5	Szenario 1a mit VMware	51
4.6	Informations- und Managementmodell von Szenario 1a mit VMware	52
4.7	Szenario 1a mit VI	53
4.8	Informations- und Managementmodell bei Virtual Iron für Szenario 1a	54
4.9	Szenario 1a Mit VIOM	57
4.10	Informations- und Management-Modell bei VIOM für Szenario 1a	58
4.11	Szenario 1b Ohne Virtualisierung	60
4.12	Informations- und Managementmodell ohne Virtualisierung für Szenario 1b	61
4.13	Szenario 1b mit PAN	63
4.14	Informations- und Managementmodell bei PAN für Szenario 1b	64
4.15	Szenario 1b mit VMware	66
4.16	Informations- und Managementmodell von Szenario 1b mit VMware	67
4.17	Szenario 1b mit VI	69
4.18	Informations- und Managementmodell bei Virtual Iron für Szenario 1b	70
4.19	Szenario 1b Mit VIOM	72

4.20	Informations- und Managementmodell bei VIOM für Szenario 1b	73
4.21	Szenario 2a ohne Virtualisierung	75
4.22	Informations- und Managementmodell ohne Virtualisierung für Szenario 2a .	76
4.23	Szenario 2a mit PAN	78
4.24	Informations- und Managementmodell bei PAN für Szenario 2a	79
4.25	Szenario 2a mit VMware	81
4.26	Informations- und Managementmodell von Szenario 2a mit VMware	82
4.27	Szenario 2a mit VI	83
4.28	Informations- und Managementmodell bei Virtual Iron für Szenario 2a	84
4.29	Szenario 2a Mit VIOM	86
4.30	Informations- und Managementmodell bei VIOM für Szenario 2a	86
4.31	Szenario 2b ohne Virtualisierung	89
4.32	Informations- und Managementmodell ohne Virtualisierung für Szenario 2b .	90
4.33	Szenario 2b mit PAN	91
4.34	Informations- und Managementmodell bei PAN für Szenario 2b	92
4.35	Szenario 2b mit VMware	94
4.36	Informations- und Managementmodell von Szenario 2b mit VMware	95
4.37	Szenario 2b mit VI	97
4.38	Informations- und Managementmodell bei Virtual Iron für Szenario 2b	98
4.39	Szenario 2b Mit VIOM	100
4.40	Informations- und Managementmodell bei VIOM für Szenario 2b	101
5.1	Informationsmodell	112
5.2	Managementmodell des einfachen Modus	113
5.3	Managementmodell des komplexen Modus	114
5.4	Ablauf der Anfrage	115
5.5	Ablauf der Vereinfachung von Meldungen	116
5.6	Modell der Ansicht	125

Literaturverzeichnis

- [BHK04] BORN, M., E. HOLZ und O. KATH: *Softwareentwicklung mit UML 2*. Addison-Wesley, München, 2004.
- [Bit08] BITTNER, FLORIAN: *Eine erweiterbare Management-Plattform für Hostvirtualisierungslösungen*. Diplomarbeit, Ludwig-Maximilians-Universität-München, <http://www.nm.ifi.lmu.de/pub/Diplomarbeiten/bitt08/PDF-Version/bitt08.pdf>, 2008. Letzer Abruf: 01.12.08.
- [Ege] EGENERA, INC.: *PAN Manager auf der Egenera Webseite*. <http://www.egenera.com/products-panmanager-ex.htm>. Letzter Aufruf: 12.09.08.
- [Ege07] EGENERA, INC.: *PRIMERGY BladeFrame Technical Overview*, Mai 2007.
- [Fuja] FUJITSU SIEMENS COMPUTER: *BladeFrame auf der Fujitsu Siemens Computer Webseite*. http://www.fujitsu-siemens.de/products/standard_servers/bframe/index.html. Letzter Abruf: 12.09.08.
- [Fujb] FUJITSU SIEMENS COMPUTER: *PRIMERGY BX600 auf der Fujitsu Siemens Computer Webseite*. http://www.fujitsu-siemens.de/products/standard_servers/blade/primergy_bx_600.html. Letzter Abruf: 12.09.08.
- [Fuje] FUJITSU SIEMENS COMPUTER: *VIOM auf der Fujitsu Siemens Computer Webseite*. http://www.fujitsu-siemens.de/products/standard_servers/system_management/serverview_viom.html. Letzter Abruf: 12.09.08.
- [HAN99] HEGERING, HEINZ-GERD, SEBASTIAN ABECK und BERNHARD NEUMAIR: *Integriertes Management vernetzter Systeme*. dpunkt Verlag, Heidelberg, 1999.
- [HK03] HITZ, M. und G. KAPPEL: *UML @ Work*. dpunkt Verlag, Heidelberg, 2003.
- [KR08] KUROSE, JAMES F. und KEITH W. ROSS: *Computernetzwerke*. Pearson Studium, München, 4. Auflage, 2008.
- [Kri07] KRIESER, MARKUS: *Dienstvirtualisierung mit Hilfe von VMware am Beispiel der Astrium GmbH*. Diplomarbeit, Ludwig-Maximilians-Universität-München, <http://www.nm.ifi.lmu.de/pub/Diplomarbeiten/krie07/PDF-Version/krie07.pdf>, 2007. Letzter Abruf: 19.12.08.
- [Lar07] LARISCH, DIRK: *Praxisbuch VMware Server*. Hanser, München, 2007.
- [Lin06] LINDINGER, TOBIAS: *Virtualisierung einer Praktikumsinfrastruktur zur Ausbildung im Bereich Sicherheit vernetzter Systeme*. Diplomarbeit, Ludwig-Maximilians-Universität-München, <http://www.nm.ifi.lmu.de/pub/Diplomarbeiten/lind06/PDF-Version/lind06.pdf>, 2006. Letzter Abruf: 27.11.08.

- [Rad06] RADONIC, ANDREJ UND MEYER, FRANK: *XEN3*. Franzis Verlag, Poing, 2006.
- [Rob01] ROBBE, BJÖRN: *SAN*. Hanser, München, 1. Auflage, 2001.
- [Spr07] SPRANG, HENNING ET AL.: *Xen*. Open Source Press, München, 2007.
- [Stö05] STÖRRLE, HARALD: *UML 2 für Studenten*. Pearson Studium, München, 1. Auflage, 2005.
- [Ste01] STEFFEN, A. UND DARIMONT, A.: *Der Netzwerkadministrator*. Addison-Wesley, München, 2001.
- [Tab06] TABELING, PETER: *Softwaresysteme und ihre Modellierung*. Springer-Verlag, Berlin, 2006.
- [Tan03] TANENBAUM, ANDREW S.: *Computernetzwerke*. Pearson Studium, München, 4. Auflage, 2003.
- [Tat04] TATE, JOHN: *Virtualization in a SAN*. <http://www.redbooks.ibm.com/redpapers/pdfs/redp3633.pdf>, 2004. Letzter Abruf: 04.12.08.
- [The06] THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, INC.: *IEEE Standard for Local and metropolitan area networks - Virtual Bridged Local Area Networks*. <http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf>, 2006. Letzter Abruf: 27.11.08.
- [TLM06] TATE, J., F. LUCHESE und R. MOORE: *Introduction to Storage Area Networks*. IBM Corp., <http://www.redbooks.ibm.com/redbooks/pdfs/sg245470.pdf>, 4. Auflage, 2006. Letzter Abruf: 04.12.08.
- [Vira] VIRTUAL IRON SOFTWARE INC.: *Server-Hosted Virtual Desktop Infrastructure (VDI)*. <http://www.virtualiron.com/Resource-Center/Whitepapers/index.php>. Letzter Abruf: 28.10.08.
- [Virb] VIRTUAL IRON SOFTWARE INC.: *Virtual Iron and Virtual Desktop Infrastructure (VDI)*. <http://www.virtualiron.com/Resource-Center/Whitepapers/index.php>. Letzter Abruf: 28.10.08.
- [Virc] VIRTUAL IRON SOFTWARE INC.: *Virtual Iron auf der Virtual Iron Software Webseite*. <http://www.virtualiron.com>. Letzter Abruf: 28.10.08.
- [Vir08] VIRTUAL IRON SOFTWARE INC.: *VI-Center Administrator Guide V4.4*. http://s3.amazonaws.com/20080903_000-982181/AdministratorGuide4413.pdf, 2008. Letzter Abruf: 30.10.08.
- [VMwa] VMWARE, INC.: *ESX Server auf der VMware Webseite*. <http://www.vmware.com/de/products/vi/esx/>. Letzter Abruf: 11.11.08.
- [VMwb] VMWARE, INC.: *Virtual Center auf der VMware Webseite*. <http://www.vmware.com/de/products/vi/vc/>. Letzter Abruf: 11.11.08.

- [VMw08a] VMWARE, INC.: *Kurzreferenz Update 2 für ESX Server 3.5, Virtual Center 2.5*. http://www.vmware.com/files/de/pdf/vi3_35_25_u2_quickstart_de.pdf, 2008. Letzter Abruf: 11.11.08.
- [VMw08b] VMWARE, INC.: *VDM 2.1 Reviewers Guide*. http://www.vmware.com/files/pdf/vdm_2.1_reviewers_guide.pdf, 2008. Letzter Abruf: 11.11.08.
- [Wika] WIKIPEDIA: *Non-functional requirements*. http://en.wikipedia.org/wiki/Non-functional_requirements. Letzter Aufruf: 18.12.08.
- [Wikb] WIKIPEDIA: *Preboot Execution Environment*. http://de.wikipedia.org/wiki/Preboot_Execution_Environment. Letzter Aufruf: 16.01.09.

Index

Betriebssystem-Virtualisierung, 5
cBlade, 10
Desktop-Virtualisierung, 6
Emulation, 4
Hardware unterstützte Virtualisierung, 4
Hypervisor, 3
LPAN, 11
MMB, 10
PAN, 9
PAN-Manager, 10
Paravirtualisierung, 4
pBlade, 9
Plattform-Virtualisierung, 3
pServer, 11
sBlade, 10
Storage-Virtualisierung, 7
vBlade, 11, 15
VIOM, 24
Virtual Iron, 19
Virtualisierungs-Management-Modell, 2
VLAN, 5
VMM, 3
VMware ESX, 16
VMware Virtual Center, 16
Vollständige Virtualisierung, 4
VPN, 6
vSwitch, 16

Glossar

- 3-Schichten-Architektur** Ein Konzept in der Software-Architektur, bei dem die Software in drei Bereiche eingeteilt wird. Es gibt eine Schicht für die Präsentation, eine für die Logik und eine für die Datenpersistenz. Siehe auch Schichtenmodell.
- CLI** Command Line Interface, eine textbasierte Benutzerschnittstelle, bei der auf einer Textkonsole Kommandos eingegeben werden müssen, wodurch Programme aufgerufen werden.
- FC** Fibre-Channel, Eine Netzwerktechnologie, die speziell für SANs eingesetzt wird.
- GUI** Graphical User Interface, eine grafische Benutzeroberfläche, die dem Nutzer, im Gegensatz zu einer CLI die Möglichkeit bietet, graphische Elemente zur Bedienung des Systems zu benutzen.
- HBA** Host Bus Adapter, eine Hardwareschnittstelle über die Computer eine Verbindung in ein Rechner- oder Speichernetz aufbauen kann. Für gewöhnlich wird dieser Begriff nur für Komponenten verwendet, die als Schnittstelle zu Speichernetzen dienen. Für die Verbindung in Rechnernetze siehe NIC.
- Hypervisor** Der Hypervisor ist eine Softwareschicht, die grundlegende Aufgaben in der Virtualisierung übernimmt. Der Hypervisor ist für die Verwaltung der Systemressourcen und deren Zuteilung an die Gastsysteme zuständig.
- iSCSI** internet Small Computer System Interface, wird benutzt, um Speicherprotokolle über TCP zu übertragen. Dadurch können Speichersysteme über bestehende Ethernetverbindungen angeschlossen werden, und brauchen keinen gesonderten Anschluss wie z.B. FC
- JRE** Java Runtime Environment, Laufzeitumgebung für Java.
- LAN** Local Area Network, ein Rechnernetz, das örtlich auf einen relativ kleinen Raum eingegrenzt ist. Die angeschlossenen Rechner können über das Netz miteinander kommunizieren.
- LDAP** Lightweight Directory Access Protocol. Ein Protokoll zur Abfrage und Veränderung von Daten eines Verzeichnisdienstes. Oft wird die Bezeichnung LDAP auch für den Verzeichnisdienst an sich verwendet.
- LUN** Logical Unit Numbers, repräsentiert die SCSI-Einheit, die die I/O-Operation durchführt. Das ist meist ein Teil einer logischen Unterteilung, die auf einer physischen Platte erstellt wird.
- MAC** Media Access Control, eine eindeutige Adresse auf OSI=Schicht 2.

Index

- MMB** Management Blade, ein Blade in einem BladeServer Frame, das für die Verwaltung des Frames und der darin enthaltenen Hardware zuständig ist. Bei einer ‘herkömmlichen’ Verwaltung ohne PAN kann das MMB über SNMP verwaltet werden und liefert Informationen über das Chassis.
- NIC** Network Interface Card, ein Computerkomponente, die zur Herstellung einer Verbindung des Computers mit einem Rechnernetz dient.
- PXE** Preboot Execution Environment, ein Verfahren zum booten von Systemen über ein angeschlossenes Netz[Wikib].
- QoS** Quality of Service, Dienstgüte. Festlegung von Parametern eines Dienstes, die im Rahmen eines Vertrages zwischen Dienstanbieter und Dienstanutzer, dem SLA (Service Level Agreement), geschieht.
- RDP** Remote Desktop Protokoll, ist ein Protokoll das von der Firma Microsoft entwickelt wurde, um einen graphischen Terminaldienst zu realisieren.
- SAN** Storage Area Network, ein Speichernetz, in dem Speicher für Computersysteme bereitgestellt wird. Der Speicher steht meist in Form von Disk-Arrays und Tape-Libraries bereit.
- Schichtenmodell** Ein gängiges Prinzip der Informatik. Ein System wird zunächst logisch in übereinanderliegende Schichten eingeteilt, die später auch bei der Implementierung so umgesetzt werden. Bei einem Schichtenmodell hat immer nur eine höhere Schicht Zugriff auf eine niedrigere Schicht; der Zugriff in umgekehrter Richtung ist verboten.
- SNMP** Simple Network Management Protocol, ein Protokoll für die Verwaltung und die Überwachung von Rechnern und Netzkomponenten in Rechnernetzen. Das Protokoll wurde von der IETF entwickelt. Aktuell ist derzeit die Version 3.
- Software-Stack** Mit Software-Stack wird eine Menge von Software beschrieben, die zum Betrieb eines Systems verwendet wird.
- VMM** Virtual Machine Monitor, siehe Hypervisor.
- WWN** World Wide Name, ist eine eindeutige Adresse in einem Fibre-Channel SAN