



Disaster Recovery mit Xen

*„Design und Implementierung eines Disaster-Recovery Programms für
Xen-virtualisierte Linux-Server im Falle eines
kompletten Ausfalls eines Rechenzentrums“*

Diplomarbeit

Hervé Marcy

Deutsch-Französisches Hochschulinstitut (DFHI)

Fachbereich Informatik

herve.marcy@hp.com

Matrikelnummer 3414582

Firma: Hewlett-Packard GmbH, Im Breitspiel 7, 69126 Heidelberg

Betreuer (HTW des Saarlandes): Prof. Dr. Reiner Güttler

Gutachter (Hewlett Packard GmbH): Bernard Dreher

Eidesstattliche Erklärung:

Ich versichere an Eides statt:

1. Ich habe die vorliegende Arbeit selbständig verfasst und nur die angegebenen Hilfsmittel benutzt.
2. Soweit Textpassagen aus anderen Quellen übernommen wurden, sind sie als Zitat gekennzeichnet.
3. Ich habe diese Arbeit noch nicht an anderer Stelle zur Erlangung eines akademischen Grades vorgelegt.

Heidelberg, den 31.10.2007

Hervé Marcy

Kurzfassung

Ziel dieser Diplomarbeit ist es, das Design und die Implementierung eines auf der Xen Virtualisierungstechnologie basierten „Disaster-Recovery“ Programms zu erklären und entsprechend zu dokumentieren. Dieses Programm ist dazu gedacht, den Betrieb geschäftskritischer Services auch im Falle eines kompletten Ausfalls eines Rechenzentrums gewährleisten zu können. Nur die Linux-Server werden hier erwähnt, wobei das Programm zusätzlich andere Systeme umfasst.

Dieses Programm hat es mir erlaubt, mich mit der Virtualisierungstechnologie „Xen“ vertraut zu machen, die sehr innovativ ist und interessante Perspektiven bietet. Ich habe während der zweimonatigen Bearbeitungsdauer mit den neuesten Technologien und Produkten arbeiten können und meine Kompetenzen im Bereich der System- und Netzwerkverwaltung erweitern können.

Die meisten Schwierigkeiten sind durch die fehlende Produktreife von „Xen“ entstanden. Sie wurden jedoch überwunden und das „Disaster-Recovery“ Programm ist nach erfolgreichen Tests vom Kunden akzeptiert worden.

Abstract

The aim of this dissertation is to explain and properly document the design and the implementation of a Disaster-Recovery Program, based on the virtualization technology Xen. This program was designed to ensure that business-critical services still run in case of a general failure in a data center. Only Linux servers are mentioned in this document, though the program includes several other systems.

This program gave me the possibility to make myself familiar with the virtualization technology „Xen“, which is very innovative and offers interesting prospects. I have had the possibility during these three months to work with the latest technologies and products and could extend my skills in various fields of the system and network administration.

The main challenges came from the immaturity of Xen, that has been overcome, though, and the Disaster Recovery Project eventually passed successfully the tests.

Danksagung

Bedanken möchte ich mich an dieser Stelle zunächst bei meinen Betreuern Bernhard Dreher und Prof. Dr. Reiner Güttler.

Bernhard Dreher hat mich während der ganzen Dauer des Praktikums und besonders während der drei Monate des DR-Projekts ständig unterstützt. Die Zusammenarbeit mit ihm hat mir großen Spaß bereitet.

Beim Prof. Dr. Reiner Güttler möchte ich mich für die wertvollen Tipps und die Hinweise zur Gestaltung der Diplomarbeit bedanken.

Besonderen Dank gilt auch an Michael Stepke und Michael Fusser, die mir erlaubt haben, an diesem Projekt teilnehmen zu dürfen und diese Diplomarbeit zu schreiben.

Danke auch an alle Heidelberger Kollegen, besonders an Christoph Schneider und Frank Koehring, die mir für meine Aufgaben in Rat und Tat während der Umsetzung des Projekts geholfen haben.

Inhaltsverzeichnis

Eidesstattliche Erklärung:	3
Kurzfassung	4
Abstract	4
Danksagung	5
Vorwort	9
1. Einleitung ins Projekt	11
1.1 Anlass zum Programm	11
1.2 Aktueller Zustand des Netzes	12
1.2.1 Standortserver	12
1.2.2 Server im Rechenzentrum	13
1.2.2.1 Cerberus	13
1.2.2.2 ZBS001	14
1.2.2.3 ZBS002	15
1.3 Projektziel	16
1.3.1 Design und Planung	16
1.3.2 Die Desasterfälle	22
1.3.3 Das DR-Projekt für Linux	25
1.3.4 Die virtuellen Maschinen	30
2. Die Xen Technologie	34
2.1 Einführung	34
2.1.1 Allgemeines	34
2.1.2 Xen steuern	36
2.2 Verwaltung vom Netz	38
2.2.1 Booten der Domain0	38
2.2.2 Booten des Domains U	39
2.2.3 Bridged Networking	40
2.3 Lösung unserer Netzproblematik	41
3. Implementierung und Ergebnis des Programms	44
3.1 Implementierung	44
3.1.1 Installation von Themis	44
3.1.2 Installation von xenka01 und xenwsl01	50
3.1.3 Installation von den produktiven virtuellen Maschinen	52
3.1.3.1 lws-xen01	52
3.1.3.2 tomcat-xen01	55
3.2 Tests und Ergebnis	59
3.2.1 Tests der virtuellen Maschinen	59
3.2.2 Tests der Performance	60
3.2.3 Tests des ganzen DR-Programms	62

3.3 Akzeptanz beim Kunden und Weiterentwicklung.....	63
3.3.1 Akzeptanz beim Kunden.....	63
3.3.2 Weiterentwicklung.....	64
Glossar.....	5
Abkürzungsverzeichnis.....	7
Abbildungsverzeichnis.....	8
Literaturverzeichnis.....	9

Vorwort

Die Hewlett-Packard GmbH ist die deutsche Abteilung des amerikanischen Konzerns Hewlett-Packard. Ihr Sitz befindet sich in Böblingen. HP ist dafür bekannt, der breiten Öffentlichkeit Drucker sowie Rechner zu verkaufen, jedoch besteht die Aktivität von HP ebenfalls aus dem Verkauf von IT-Infrastruktur und IT-Dienstleistung für andere Firmen (Hardware sowie Service). Dies ist die Beschäftigung der TSG Division (Technology Solution Group).

Der Operation Center Heidelberg (OPC) ist ein Standort der TSG Division. Hier werden die IT-Infrastrukturen der Firmen MLP AG (Finanzdienstleistungen) sowie von Panasonic (Unterhaltungstechnik) teilweise ausgelagert.

Die MLP AG ist eine Finanzdienstleistungsfirma, die mit ihren Produkten speziell auf junge Absolventen mit hohem Potential (Führungskräfte aus Wirtschaft und Technik, Freiberufler und Selbstständige, Juristen, Mediziner und Pharmazeuten) abzielt. In der Regel hat sie Standorte in unmittelbarer Nähe von Hochschulen und Universitäten, nicht nur in Deutschland, sondern auch in Spanien, Österreich, den Niederlanden und Großbritannien.

Die MLP AG bietet eine breite Produktpalette (Bank, Versicherung, usw...) an und braucht dafür eine starke IT-Infrastruktur. Um die Kosten besser kalkulieren zu können und sich auf ihr Kerngebiet zu konzentrieren, hat sich die MLP AG schon ab 1997 mit dem Outsourcing von speziellen IT-Dienstleistungen beschäftigt.

Um die Internet-Wende nicht zu verpassen, hat sich der Konzern dazu entschlossen, das Betreiben seines Netzwerks sowie seiner Rechenzentren auszulagern. Schwerpunkte für die Bewerber waren: Zukunftssicherheit, Know-How über Verfügbarkeit und Sicherheit von IT-Systemen, Internet-Kompetenz sowie Zuverlässigkeit.

Da Hewlett-Packard schon seit 1992 als Hardware-Lieferant und Support-Anbieter von der MLP AG gut bewertet wurde, machte HP bei der Auswahl das Rennen.

Nach nur neun Monaten begannen die ersten Verhandlungen und in Oktober 1999 wurde der Vertrag unterzeichnet.

Heute betreut HP die Hardware (ca. 200 Server und 3 600 Clients – davon 2 690 Notebooks in 310 Geschäftsstellen) und das Netzwerk der Finanzdienstleistungsfirma und übernimmt die Verantwortung für den reibungslosen Betrieb der gesamten Hardware mit deren Wartung, sowie der Administration einer komplexen Infrastruktur (Novell-Netzwerk unter HP-UX und Windows NT-Servern). Die MLP AG hat eine langjährige Partnerschaft mit Novell und die bekanntesten Produkte der amerikanischen Firma (SuSE Linux, ZENworks, NetWare und eDirectory) sind die zentralen Komponenten der IT-Infrastruktur.

MLP hat einen Support-Vertrag (Premium Support Vertrag 5000) mit Novell abgeschlossen. Ein Mitarbeiter (Dedicated support engineer) von der Software-Firma steht den HP-Mitarbeitern jederzeit für technische Fragen zur Verfügung. Die HP Mitarbeiter müssen Richtlinien befolgen, um den Service zu beanspruchen. So wird z.B. die Linux Version SLES 8 nicht mehr unterstützt. Fragen zu diesem Thema können an den Dedicated support engineer gestellt werden, er kann jedoch keine solcher Fragen eskalieren. Die HP-Mitarbeiter sind ebenso von MLP offiziell leistungsberechtigt und können z.B. SLES-Lizenzen einem neuen Server erteilen.

Im Laufe des Jahres werden verschiedene Projekte durchgeführt um die Verfügbarkeit sowie die Performance des Netzes und der Server zu verbessern.

1. Einleitung ins Projekt

1.1 Anlass zum Programm

Die Notwendigkeit, Risiken zu kontrollieren und einen ständigen und sicheren Betrieb zu gewährleisten, besitzt in jedem Unternehmen eine sehr hohe Priorität. Heutzutage sehen Unternehmen sich zunehmend mit Gefahren für die Sicherheit und Verfügbarkeit von Systemen und Daten konfrontiert – Viren, Hacker, Terrorismus, Naturkatastrophen. Zudem wächst auch der Druck innerhalb des Unternehmens. Immer mehr rechtliche Bestimmungen verlangen eine strengere Kontrolle über Service-Verfügbarkeit und Datensicherheit.

Moderne Unternehmen sind stark von der IT abhängig, sodass sich Ausfälle und Datenverlust in hohen Kosten niederschlagen können – von Umsatz- und Produktivitätsverlusten bis hin zur Unfähigkeit, Services überhaupt noch zur Verfügung stellen zu können. Daher muss eine umfassende Strategie formuliert werden, die Kontinuität, Verfügbarkeit und Datensicherheit berücksichtigt, um solche Herausforderungen kosteneffektiv zu meistern.

Die gesetzlichen Forderungen, die in Deutschland angewendet werden, spielen also eine große Rolle: Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) kann z.B. die Erteilung einer Bank- oder Finanzdienstleistungslizenz im §33 des Kreditwesengesetzes (KWG) aufgrund mangelnder organisatorischer Vorkehrungen versagen.

Die Erlaubnis ist zu versagen, wenn

§33, Nr. 7: Das Institut nicht bereit oder in der Lage ist, die erforderlichen organisatorischen Vorkehrungen zum ordnungsmäßigen Betreiben der Geschäfte, für die es die Erlaubnis beantragt, zu schaffen;

vgl. <http://www.bafin.de/gesetze/kwg.htm>

Seit einigen Jahren hat sich die MLP AG auf ihr Bankgeschäft konzentriert, wobei sie diese Funktion in den letzten Jahren eher ausgelagert hatte. Sie hat unter anderen ihre Lebensversicherungsbranche verkauft und setzt sich völlig in ihrem neuen Kerngeschäft ein.

Es ist also für die MLP AG, als Finanzdienstleistungsgesellschaft, extrem wichtig, dass ihre Werkzeuge ständig zur Verfügung stehen. Dafür hat die MLP AG ein Service Level Agreement mit HP vereinbart, das den reibungslosen Betrieb der IT garantieren soll.

1.2 Aktueller Zustand des Netzes

1.2.1 Standortserver

Alle Standorte der MLP AG besitzen einen sogenannten Standort-Server. Alle Geschäftsstellen sind einem Standortserver zugewiesen wobei mehrere Geschäftsstellen sich einen Server teilen können, je nachdem, wie groß sie sind.

Die Standortserver übernehmen folgende Funktionen:

- Datensicherung (DaSi) der Benutzer. Die Dateien selbst sind nicht auf dem Server gesichert sondern sind in einem für alle Servern gemeinsamen SAN gespeichert. Dieser SAN befindet sich in Wiesloch und bekommt die Daten aus den Geschäftsstellen über eine Kette von internen Servern.
- Verwaltung der Drucker des Standorts mit dem Samba-Protokoll
- E-mail Versand und Datenbank (Domino-Notes)

Bei den Servern handelt es sich um HP Proliant Server, die das Linux SLES 10 Betriebssystem nutzen.

1.2.2 Server im Rechenzentrum

Die Rechenzentren der MLP AG in Karlsruhe und Wiesloch stellen ein einziges Netz dar, wobei es Router innerhalb des Gesamtnetzes gibt. Die IP-Adressen sind Adressen der A-Klasse und sind RFC 1918 konform. Sie folgen dem Schema 10.96.x.x

Drei Linux Server befinden sich im Moment im Rechenzentrum der MLP AG in Wiesloch, die vom Disaster Recovery Projekt (DRP) betroffen sein werden:

- Cerberus
- zbs001
- zbs002

1.2.2.1 Cerberus

Technische Eigenschaften:

Typ: HP ProLiant DL380 G4 X3,6

Festplattenkapazität (GB): 560

Prozessor: Intel Xeon G4 3,6

Takt (Mhz): 3600

Anzahl der Prozessoren: 4

Hauptspeicher (MB): 3988

Dieser Server verfügt über 4 Netzwerkschnittstellen (NIC):

- eine für den Administrator-Zugang
- eine für die Backups
- eine für die Users bzw. Anwendungen
- eine für die Remote Console

Diese letzte NIC -mit zusätzlicher Hardware- heißt iLO (Integrated Lights out) und erlaubt einen remote-Zugriff auf die Maschine auch wenn das Betriebssystem noch nicht komplett hochgefahren wurde, z.B. auf den Boot-Loader und erlaubt eine grafische Remote-Installation)

Er hat verschiedene Funktionen:

- Tomcat-Server: Er besitzt eine Datenbank für Druckertreiber. Ein User kann eine Anfrage machen, um herauszufinden, welche Drucker in seinem LAN-Segment sich befinden und stellt ihm Druckertreiber zur Verfügung.
- Proxy-Server: Er dient dazu, den Inhalt von Seiten zu speichern, damit sie dem Benutzer schneller zur Verfügung stehen und den externen Internet-Verkehr verringern. Der Proxy kann sie dazu filtern und nur Zugang nur für bestimmte Webseiten freischalten.
- DNS-Server: er kümmert sich um die Namensauflösung innerhalb des MLP-Netzes
- Sync-Server: Aufgabe dieses Servers ist es, Software-Pakete und Images für die Einrichtung von Clients zur Verfügung zu stellen (es ist Teil des Novell-Systems ZENwork – Zero Effort Network). Diese Pakete sind in einem Storage-Disk-Array XP1024 gespeichert und werden über ein SAN-System ausgezogen (siehe Abbildung 1.4). Dieses System erlaubt z.B. den Rechner aus dem Netz hochzufahren und das Betriebssystem sowie sämtliche Pakete neu zu installieren.

1.2.2.2 ZBS001

Typ: HP ProLiant ML370 G3 R03

Festplattenkapazität (GB) 726.7

Prozessor: Intel Xeon

Takt (Mhz): 2783

Anzahl der Prozessoren: 4

Hauptspeicher (MB): 2526

Dieser Server verfügt über 4 Netzwerkschnittstellen:

- eine für den Admin-Zugang
- eine für die Backups
- eine für die Users
- eine, die einem ILO zugeordnet ist.

Er synchronisiert und sichert die Dateien, die die Benutzer auf den Standorten gespeichert haben (Datensicherung – DaSi). Genau so wie bei Cerberus greift zbs001 auf das selbe Storage-Disk-Array XP1024 über ein SAN-System zu, um die Dateien der Benutzer zu speichern. Diese werden nicht auf den lokalen Festplatten des Servers gelagert. Er wird nur als Übergang benutzt (siehe Abbildung 1.4).

1.2.2.3 ZBS002

HP ProLiant ML370 G3 R03

Festplattenkapazität (GB) 119.6

Prozessor: Intel Xeon

Takt (Mhz): 2783

Anzahl der Prozessoren: 4 (2 CPU + HyperThreading technology)

Hauptspeicher (MB): 2526

Dieser Server verfügt über 3 Netzwerkschnittstellen:

- eine für den Admin-Zugang
- eine für die Backups
- eine für die Users
- eine für ILO

Er ist hauptsächlich als Ersatzmaschine für die Synchronisierung, falls der Server ZBS001 ausfällt gedacht. Daher ist er ebenfalls am SAN angeschlossen und kann

auf das Storage Disk Array XP1024 zugreifen.

Er wird aber auch daneben als Web-Server betrieben (sein DNS-Alias heißt lws.mlp-ag.com - Linux Web Services). Das CMS Typo3 ist darauf installiert und wird für verschiedene Management-Zwecke benutzt:

- Samba-Paßwörter der Benutzer auf den Standortservern ändern
- Status des Ausrollens von SLES 10 für die Standortservern
- Überprüfung des Erfolgs der DaSi zwischen Cerberus und den Geschäftsstellen
- Administrative Tools für die Standortserver in den Geschäftsstellen.

1.3 Projektziel

1.3.1 Design und Planung

Das Disaster-Recovery-Programm, ist ein wichtiges Projekt für die MLP AG. Ziel dieses Programms ist es, eine ganze produktive Umgebung, in einem definierten Zeitrahmen aus einem Rechenzentrum in Wiesloch in ein anderes in Karlsruhe zu verschieben und weiter betreiben zu können, wenn ein ganzes Rechenzentrum aus irgendeinem Grund (siehe Tabelle 1) ausfällt.

Die Projektleiter von HP haben sich mit den IT-Verantwortlichen der MLP AG beraten und alle geschäftskritischen Services aufgelistet und nach maximalen Ausfallzeit und Datenverlust sortiert. Da aber die Organisation nach den ITIL-Richtlinien gestaltet wurde, wurden alle Services nach Bereich untersucht, um eine Bewertung in Form einer Liste von Systemen, die entweder betroffen waren („In scope“) oder nicht („Out of scope“).

Es wurden dann Lösungen skizziert, um zu definieren, welche Verfahren notwendig sind und dieses ehrgeizige Projekt wurde auf die Beine gestellt. Dieses DRP hätte noch abgespeckt werden können und mit günstigeren Lösungen (wie einfache Backup-Restore oder Hardware-Mieten) geplant werden. Aufgrund der Größe des Unternehmens und der komplexen Verfahren, die sie regieren, konnten solche Produkte

jedoch nicht eingesetzt werden, auch wenn sie z.B. für kleinere Unternehmen geeignet wären.

Die IT-Bereiche sind bei HP in großen Delivery Towers aufgegliedert (z.B. Lotus Notes, Novell-Linux, usw.). Dies hat die Entwicklung des DRP's bedingt, da sich in jedem Container Spezialisten für die jeweiligen Technologien und Anwendungen befinden. Sie wurde also nach Lieferbereichen gestaltet, damit jeder genau seine Plattform perfekt beherrscht.

Die Projektleiter des DRP's haben nur den Ausfall eines einzigen Standorts berücksichtigt. Zwar kann es passieren, dass ein Atomkraftwerk explodiert, in diesem Fall hätte die Region aber ganz andere Probleme als nur das Disaster-Recovery Plans einer Bank einzusetzen.

Es wurden also zwei Rechenzentren ausgewählt :

- Wiesloch.

Es handelt sich um das „historische“ Rechenzentrum der MLP AG.

- Karlsruhe.

Die minimale Entfernung zwischen den beiden Rechenzentren musste mindestens 10 Kilometer betragen. Zwar hätte die MLP AG ein näher gelegtes Rechenzentrum auswählen können, aber die redundanten physikalischen Kommunikationswege im Netzwerk und für die Fibre Channel haben die Entscheidung beeinflusst.

Dem Kunden wurde ebenso eine Lösung von Storage on Demand (SoD) angeboten: es wird ihm beliebig viel Speicher zur Verfügung gestellt, er zahlt aber nur den Speicher, den er tatsächlich verbraucht.

Der Linux-Teil, wovon in dieser Diplomarbeit die Rede ist, ist nicht allein vom Programm betroffen. Es fasst ein ganzes System mit z.B. Notes-, eDirectory-, oder Zenworks-Servern, die verschiedene Virtualisierungstechnologien, wie Vmware ESX, oder Xen einsetzen, um (siehe Abbildung 1.1).

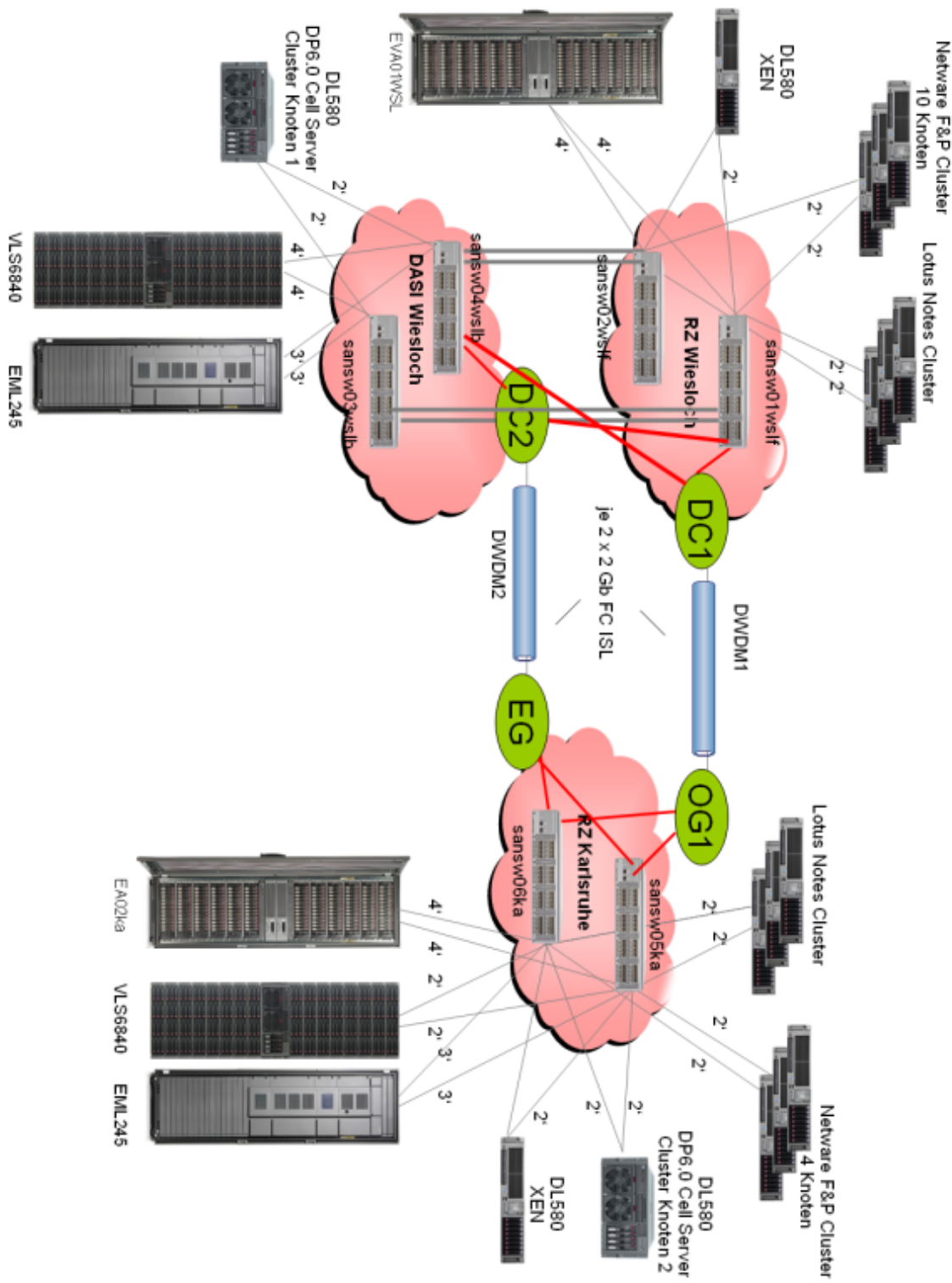


Abbildung 1.1: Physikalische Einstellung in den Rechenzentren

Die Entscheidung für Xen im Linux-Bereich ist aus mehreren Gründen gefallen:

- Im Gegensatz zu Vmware ist Xen freie Software, die in der Linux Distribution (SuSE Linux Enterprise Server 10) enthalten ist. Das heißt, dass keine Gebühren für die Lizenz der Software verlangen werden können.
- Es handelt sich um ein „Technology refresh“ (technologisches Auffrischen), die eine Erweiterung sowie eine Verstärkung der Services den Richtlinien der ITIL nach erlauben soll. Damit können auch Folgegeschäfte entstehen.
- Das Know-How und die Kompetenz der Mitarbeiter werden erweitert. So sind sie in der Lage, diese Kompetenzen in dieser innovativen Technologie weiter benutzen zu können.

Das Backup der verschiedenen Konfigurationen der Server erfolgt jeden Freitag vollständig und jeden Tag differenziell (d.h. alle Daten, die seit Freitag verändert wurden werden gesichert).

Am Ende der Implementierung des DR-Projekts wurden von den HP Mitarbeitern Tests nach einem Testplan durchgeführt.

Zusätzlich zu diesen Test werden mehrere Abnahmetests, an denen der Kunde teilnimmt, durchgeführt. Ziel ist es nicht, ein unkontrolliertes Ausschalten des Rechenzentrums auszulösen (dies wäre eher ein Fail-over-Test), sondern sie je nach Services anzuwenden (in-scope-Tests). Z.B. kann nur die USV eines einzigen Server ausgeschaltet werden, um seine Funktionen zu überprüfen und dann diese Operation auf die anderen Servern wiederholen.

Der Kunde wird bei diesen Tests unmittelbar sehen, was passiert. Er wird eine bestimmte Anzahl an Benutzern mit Tests beschäftigen, um zu überprüfen, ob alles läuft, wie geplant.

Nach dieser Testsitzung werden die Funktionen und Leistungen der verschiedenen Services und nach Abnahmekriterien bewertet. Diese Bewertung wird dann

entscheiden, ob das DRP vom Kunden abgenommen wird, oder nicht.

Für das ganze Projekt wurde ein Implementierungsplan erstellt (siehe Abbildung 1.2). Die Implementierung des DRP hat insgesamt ca. 2 Monate (inkl. Abnahmetests) dauern.

Einleitung ins Projekt

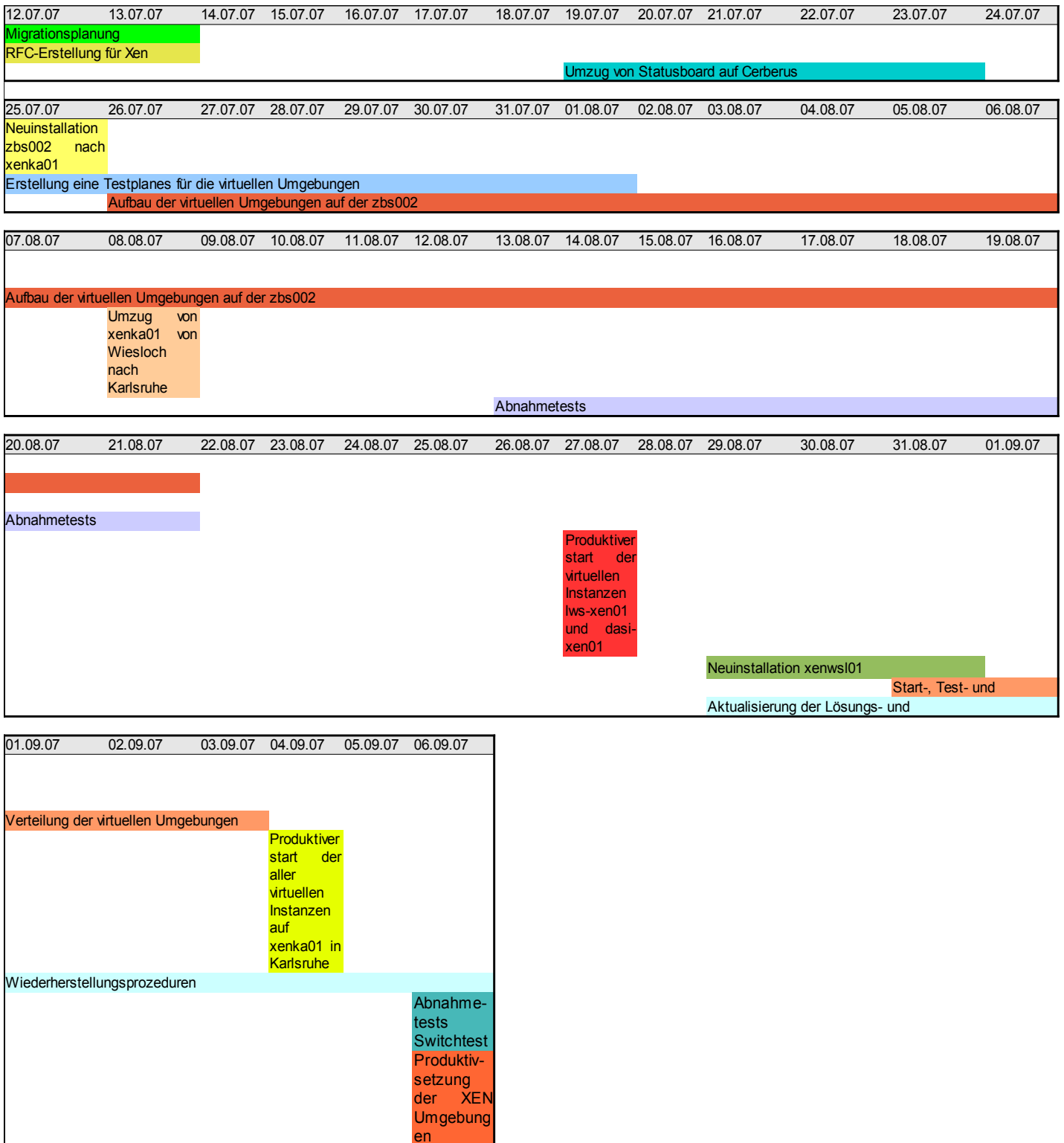


Abbildung 1.2 : Implementierungsplan

1.3.2 Die Desasterfälle

Es wurden verschiedene mögliche Fälle erforscht, analysiert und je nach Gefahr einer Klasse zugeordnet:

IT-Notfall Kategorie	Desaster Fälle	Kategorie Klasse	Beschreibung der Einschränkung
Katastrophe	GAU (z.B. Atomkraftwerk - Radioaktiver Unfall Phillipsburg)	1	<ul style="list-style-type: none">• Komplettausfall aller Rechenzentren oder• Ausfall aller Kommunikationsverbindungen (WAN / SAN / LAN) oder• Ausfall aller Versorgungseinrichtungen (Strom / USV / Klima)
Notfall	Bio/Chemie Unfall Brand/Explosion Wasserschäden	2	<ul style="list-style-type: none">• Ausfall Rechenzentrum, Telekomraum, Datensicherungsraum, Tresorraum• Ausfall einer Versorgungseinrichtung (Strom / USV / Klima) je RZ
Ausfall	HW Defekt am Server	3	<ul style="list-style-type: none">• Ausfall eines einzelnen HW-Systems oder HW-Komponente

Tabelle 1: Desasterfälle

Nachdem der Desaster geschehen ist, können Meldewege für die Alarmauslösung über zwei verschiedene Wege erfolgen:

- den HP Helpdesk Serviceline Hub Delivery, der die Information an den Manager on Duty (MoD) weiterleitet.
- die MLP-Sicherheitsleitstelle, die die Informationen den verantwortlichen DR-Manager weiterleitet.

Die folgenden Maßnahmen müssen sofort nach dem Desaster getroffen werden:

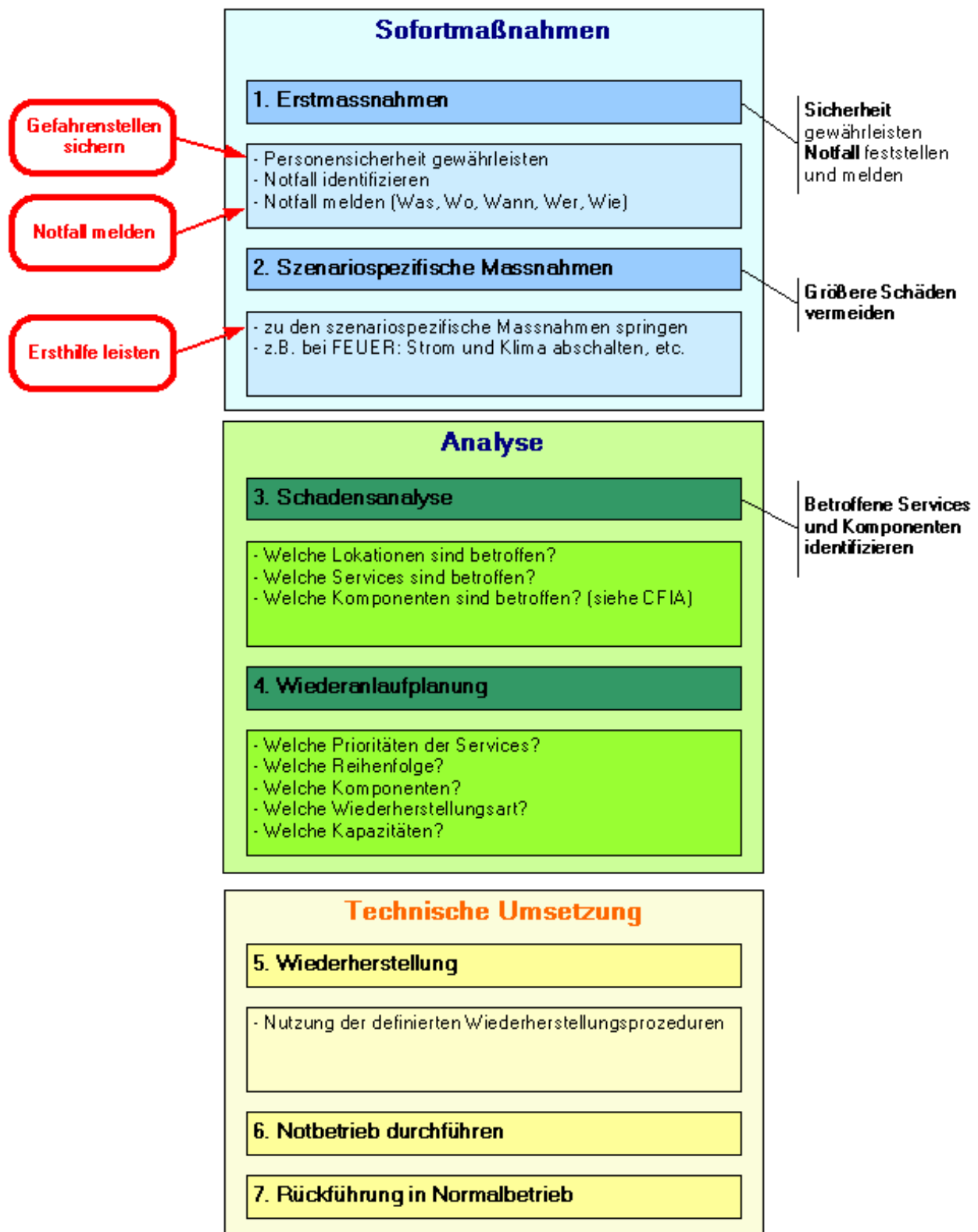


Abbildung 1.3: Maßnahmenabfolge

Über die Definition geschäftskritischer Services wurde für den Notfall eine Strategie abgeleitet, welche Applikationen / Services im Notbetrieb benötigt werden und welche abgeschaltet oder reduziert werden können.

Die maximale Ausfallzeit beträgt hierfür einen Werktag, d.h. bei einem Ausfall an einem Werktag um 15 Uhr, müssen die definierten Services bis zum nächsten Werktag 15 Uhr wieder zur Verfügung stehen. Bei einem Ausfall an einem Nicht-Werktag gilt als Ausfallzeit der Beginn der Servicezeit (6 Uhr morgens) des darauf folgenden Werktags.

Die Zeit bis zur Entscheidung, dass der Recovery Plan anläuft, wird mit 4 Stunden angenommen. Danach bestehen 20 Stunden für die Recovery Phase. Die Zeit zur Wiederherstellung definierter Services, ergibt somit 24 Stunden.

In der folgenden Tabelle sind verschiedene mögliche Disasterfälle, ihre Gründe und die maximale Dauer, bis der DR-Plan ausgelöst werden muss, zu sehen

Ereignis	Beispiele	Quantität	Max. Zeit / Dauer nach Eintritt/ Wahrnehmung bis DR-Plan ausgerufen werden muss	Wer stellt fest
Technisches Versagen	"IN Scope" Systeme sind ausgefallen bzw. nicht mehr nutzbar	100%	Max. 4h	hp
Technisches Versagen	Stromausfall und gleichzeitiger Ausfall Stromgenerator (Anlaufen nicht möglich)	100%	Max. 4h	hp
Technisches Versagen Höhere Gewalt Menschliches Versagen	RZ (abhängig von der Lösung ggfs. auch DASI-, Datakom-, Tresorraum) ist nicht begehbar, (infolge Brand, Wasserflutung, Verseuchung, Strahlung, Löschanlage hat ausgelöst)	Data Center /Datakom Raum/ Tresorraum / DASI-Raum ist betroffen	Max. 4h	MLP Sicherheitsleitstelle
Technisches Versagen	Netzwerkausfall	100% des Data Centers bzw. 100% des Datakom Raumes bzw. 100% des DASI-Raum	Max. 4h	hp

Vorsätzliche Handlung		100%		
Technisches Versagen	Klimatisierung Datacenter		ca. 2h	hp (CDM-Team 8x5, MLP Sicherheitsleitstelle)
Höhere Gewalt	Erdbeben Bergwerkschäden, Holräume Flugzeugabsturz Flut Tornado, Wirbelstürme Feuer Regen Schnee Eis	Data Center /Datakom Raum/ Tresorraum / DASI-Raum ist betroffen	Max. 4h	hp (CDM-Team 8x5), MLP Sicherheitsleitstelle
Vorsätzliche Handlungen	Terror Drohung Bomben Spionage Sabotage Verseuchung (chem.,biol.) Vandalismus Hacker, Viren	Data Center /Datakom Raum/ Tresorraum / DASI-Raum ist betroffen	Max. 4h	hp/mlp
Organisatorische Mängel	Fehlende Abstimmung (Stromabschaltung) Nicht beachtete Vorgaben (Kernbohrung im RZ) Keine Abstimmung bei großen Change Aktionen	Data Center /Datakom Raum/ Tresorraum / DASI-Raum ist betroffen	Max. 4h	hp/mlp
Menschliches Versagen	Not Aus (versehentlich gedrückt) Falscher Personaleinsatz / Ausbildungsstand Rauschmittel (Drogen, Alkohol)	Data Center /Datakom Raum/ Tresorraum / DASI-Raum ist betroffen	Max. 4h	hp/mlp

Tabelle 2: Entscheidungskriterien

1.3.3 Das DR-Projekt für Linux

Bisher befanden sich 3 Server unter Linux, die vom DRP von MLP betroffen sind:

- Cerberus
- zbs001

- zbs002

Nach dem Projekt müssen nur noch zwei übrig bleiben:

- xenka01 (in Karlsruhe, ehemals zbs001)
- xenwsl01 (in Wiesloch, ehemals zbs002)

Die beiden Server werden mehr Hauptspeicher bekommen, um die Last von 3 virtuellen Maschinen tragen zu können (siehe Kapitel 1.1.3.3).

Nachdem das Projekt fertig ist, sollen sich die Server wie folgt verhalten: im normalen Betrieb laufen insgesamt 6 virtuelle Maschinen, 3 in Wiesloch auf dem Server xenwsl01 und 3 in Karlsruhe auf dem Server xenka01. Ihre Funktionen und Eigenschaften werden im Kapitel 1.1.3.3 erläutert.

Ein System von „Desaster Tolerantes Backup“ soll eingesetzt werden. D.h. die gleiche Backupinfrastruktur wie in Wiesloch, wird nochmals in Karlsruhe aufgebaut. Die Backups verlaufen über beide Standorte, um im Ausfall eines Standortes direkt auf die redundante Backup-Infrastruktur des anderen Standortes zugreifen zu können.

Das ganze wird in Virtual Library System (Tapes) gespeichert.

Die Hosts (xenka01 und xenwsl01) befinden sich jeweils in Wiesloch und in Karlsruhe und sind je an einem HP EVA8000 Storage Disk Array über ein SAN angeschlossen. In der Praxis bedeutet das, dass jeder Host diesen freien Raum als lokal angeschlossene SCSI-Festplatten betrachtet, wobei der Datenstrom übers Netz läuft (dies bleibt für die Rechner aber transparent).

Die Host-Maschinen sind auf lokalen Festplatten installiert, die virtuellen Maschinen sind aber auf dem Storage Disk Array gelagert. Da aber der Host diesen Raum als lokale SCSI-Festplatten betrachtet, können sie ganz normal von dem Gastbetriebssystem hochgefahren werden.

Diese Art, die VM's zu lagern hat einen guten Grund: die beiden Storage Disk Arrays sind durch Fibre Channel-Verbindung miteinander verbunden und alle ihre Einheiten werden ständig über eine HP Software, genannt „Continuous Access“, aus dem Wieslocher Rechenzentrum ins Karlsruher Rechenzentrum gespiegelt.

Die virtuellen Instanzen befinden sich im Storage Disk Array. Jeder LUN (Logical Unit Number) des Arrays wird eine virtuelle Instanz zugewiesen. Diese LUN bildet aus Sicht von „Continuous Access“, eine DR-Gruppe (Disaster Recovery). Jede DR-Gruppe wird genau aus Wiesloch nach Karlsruhe gespiegelt. Dies bedeutet in der Praxis, dass der Inhalt der Festplatten der virtuellen Instanzen exakt der selbe ist, in Wiesloch wie in Karlsruhe, auch wenn die VM's in Karlsruhe nicht hochgefahren werden.

Leider ist es unmöglich gleichzeitig die Dateien aus Wiesloch nach Karlsruhe und umgekehrt zu spiegeln, so, dass nur die Richtung WSL → KA gewählt wurde. Da aber der Server xenwsl01 auf die Karlsruher EVA (HP Storage Disk Array) im Ausnahmefall zugreifen kann, stellt das aber kein ernstes Problem.

Im Normalbetrieb laufen die virtuellen Maschinen auf einem definierten Server. Die zwei Host-Maschinen, die das Virtualisierungsverfahren ermöglichen (siehe Kapitel 2) können nicht irgendeine virtuelle Maschine kontrollieren. Zuerst müssen die betroffenen DR-Gruppen von der EVA an die Hosts mit der HP-Software, die das SAN kontrolliert, „präsentiert“ werden. Grund dafür ist, dass zwei verschiedene Rechner, jeweils auf eine LUN und auf die gespiegelte Version dieser LUN, nicht gleichzeitig zugreifen dürfen. Dies würde nämlich zu einer Inkonsistenz im Filesystem bzw. zu Problemen mit der Spiegelung auslösen.

Im Desasterfall müssen also die DR-Gruppen der verbliebenen VM's, die nach Karlsruhe verschoben werden sollen, von der EVA an den Server xenka01 präsentiert werden, so, dass der Rechner auf die betroffenen LUN zugreifen und die restlichen VM's hochfahren kann.

Darüber hinaus bietet „Continuous Access“ zwei Modi:

- Das synchrone Modus: die Zugriffe auf die Festplatten in Wiesloch sind ausgeschaltet, bis die Spiegelung erfolgt ist.
- Das asynchrone Modus: die virtuellen Maschinen können weiter auf die Festplatten zugreifen, auch wenn eine Spiegelung am Laufen ist.

Das zweite Modus wurde aufgrund der erfordernten hohen Verfügbarkeit und der Flexibilität für das DR-Projekt gewählt.

Alles in allem bedeutet das, dass die Änderungen am Inhalt der Festplatten, die in Wiesloch vorgenommen werden, genauso in Karlsruhe vorgenommen werden werden.

Wenn das Rechenzentrum in Wiesloch aus irgendeinem Grund (siehe Tabelle 1) ausfällt und das Disaster-Recovery-Programm eingeschaltet wird, kann der Xen-Server in Karlsruhe den Betrieb übernehmen, indem dort einfach die virtuellen Maschinen hochgefahren werden. Da die Inhalte der Festplatten gleich sind, gehen keine Dateien verloren.

Da die Rechenzentren der MLP AG in Karlsruhe und Wiesloch ein einziges Netz darstellen (siehe Kapitel 1.2.2), brauchen die Netzwerkschnittstellen nicht, umkonfiguriert zu werden.

Diese VM's werden mit einem niedrigeren Anspruch an Ressourcen hochgefahren und stellen ihre Dienste wieder zur Verfügung.

Die Flexibilität und der beschränkte Bedarf an Konfiguration dieser Lösung ist einer seiner Vorteile.

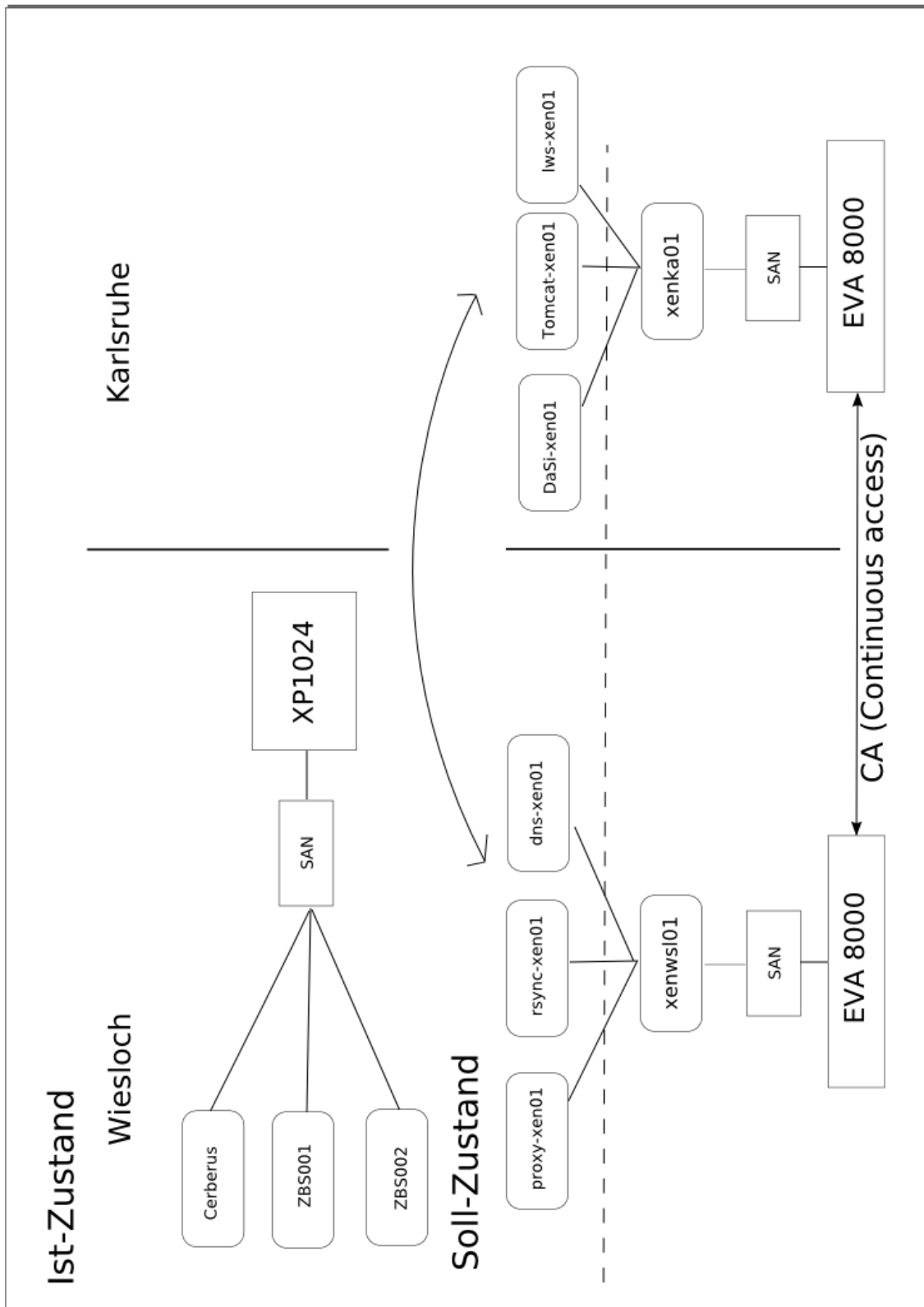


Abbildung 1.4: Ist- und Soll-Zustand

1.3.4 Die virtuellen Maschinen

Die virtuellen Maschinen spielen jeweils eine bzw. mehrere Rollen:

dasi-xen01

- Transfer der Groupshare Daten von den Standortservern
- Transfer der MLP-Backup Daten von den Standortservern. Diese Daten werden auf Band mit DataProtector gesichert.
- Groupshare für Mobile User (groupshares.mlp-ag.com)
- Globale Groupshares für Firmenkundenberater
- Ablage Server für Daten der Workorder Geschäftsstellenwechsel

lws-xen01

- Administrative Tools für die Standortserver in den Geschäftsstellen (statusboard). Alle GeGis (Geschäftsstellen Gefährliche Incidents) werden darauf aufgelistet und von HP-Mitarbeitern bearbeitet.

Das CMS Typo3 stellt Seiten zur Verfügung zur Überwachung Rsync und DaSi Groupshare Support durch Helpdesk)

- Nachstarten und überwachen von rsync Prozessen (MLP Backup und zen_pakete / zen_images)
- Tool zum löschen von lock und archive files auf den Standortservern
- Tool zum Zurücksetzen von Samba User Passwörtern
- Projektwebseiten (z.B. Rolloutdatenbank für Serverupdate und 802.1x Rollout)
- Subversion (Versionierungssoftware für skripte/dokumente)

tomcat-xen01

- Druckerdatenbank für die Standorte (PrintDB.mlp-ag.com)
- Notes ID für Neuinstallation von Notes Clients

rsync-xen01

- ZEN Paket, tftpboot und ZEN Image - Verteilung an die Standortserver
- Verteilung von nachzuinstallierender Software an die Standortserver (nach Bedarf)
- Server UpTime Reporting
- ERM (European Resource Model) Slave (neue angedachte Funktion)

dns-xen01

- DHCP, DNS für die Außenstellen und den Tagungsstandort

proxy-xen01

- Proxy-chain für mlp.de und films.mlp.de
- Proxy für Außenstellen und den Tagungsstandort

Während der Planungsphase wurde ein wichtiger Punkt erwähnt: der Verbrauch an Hauptspeicher. Die Prozessorbestückung der Xen-Server (4 Intel Xeon mit 2,8 GHz) ist bei weitem ausreichend, der Hauptspeicher ist uns allerdings als zu knapp aufgefallen (2,5 GB).

Zwei Forderungen von MLP bedingten unser Urteil:

- der Betrieb muss gewährleistet werden

- eine Verringerung der Performance wird von MLP akzeptiert

Diese Verringerung der Performance bedeutet aber nicht, dass das Swapping erlaubt ist. Die Services dürfen langsamer laufen, im Swapping-Fall wird aber die Performance so sinken, dass der Kunde das nicht akzeptieren könnte.

Der Verbrauch vom Hauptspeicher wurde der Erfahrungen der Mitarbeiter nach wie folgt gerechnet (eine präzise Kalkulation war unmöglich, da das Proxy-Programm Squid Speicher belegt und erst wieder freigibt, wenn andere Anwendungen Speicher anfordern):

Im normalen Betrieb

xenka01 (Karlsruhe):

Name der Maschine	Hauptspeicher	Storage
xenka01 (Gast-OS)	256 Mb	50 Gb
lws-xen01	512 Mb	20 Gb
dasi-xen01	2048 Mb	715 Gb
tomcat-xen01	768 Mb	15 Gb
Summe	3584 Mb	770 Gb

Tabelle 3: Schätzung des Speicherverbrauchs für xenka01

xenwsl01: (Wiesloch)

Name der Maschine	Hauptspeicher	Storage
xenwsl01 (Gast-OS)	256 Mb	50 Gb
proxy-xen01	1792 Mb	10 Gb
dns-xen01	512 Mb	10 Gb
rsync-xen01	1024 Mb	15 Gb
Summe	3584 Mb	770 Gb

Tabelle 4: Schätzung des Speicherverbrauchs für xenwsl01

Im Desasterfall (auf xenka01)

Name der Maschine	Hauptspeicher
xenka01 (Gast-OS)	128 Mb
lws-xen01	512 Mb
dasi-xen01	1024 Mb
tomcat-xen01	512 Mb
proxy-xen01	512 Mb
dns-xen01	256 Mb
rsync-xen01	512 Mb
Summe	3456 Mb

Tabelle 5: Schätzung des Speicherverbrauchs für xenka01

2. Die Xen Technologie

2.1 Einführung

2.1.1 Allgemeines

Xen ist eine unter GPL (GNU General Public License) lizenzierte freie Software, die es erlaubt, mehrere Instanzen eines Betriebssystems auf einem einzigen Rechner laufen zu lassen.

Sie wurde ursprünglich in der University of Cambridge vom Prof. Ian Pratt, der das Unternehmen XenSource Inc. gegründet hat, entwickelt. Die XenSource Inc. unterstützt die Entwicklung des open-source Projekts und verkauft Enterprise-Versionen von Xen.

Xen ist auf einem Hypervisor basiert. Dieser Hypervisor kontrolliert und verteilt alle Ressourcen des Rechners und wird von der sogenannten Dom0 kontrolliert. Es handelt sich um eine Linux Distribution (in unserem Fall, SuSE Linux Enterprise Server 10), dessen Kernel verändert wurde, um Gäste-OS (DomU) erstellen zu können.

In der Praxis bedeutet das, dass der Bootloader GRUB während des Bootvorgangs die Wahl zwischen einem normalen Kernel (z.B. Linux-2.6.22.1-smp) und dem von Xen veränderten Kernel (z.B. Linux-2.6.22.1-smp-xen).

Die Dom0 ist das Betriebssystem, das als Container für die virtuellen Maschinen dient. Es wird als erstes gebootet und kann den Betrieb der anderen VM teilweise steuern (Hoch- und Herunterfahren, Speicher vergrößern oder verkleinern, usw.).

Der Xen-Hypervisor, stellt eine Schicht zwischen der Hardware und den VM dar. Er

kümmert sich um die Verteilung der physikalischen Ressourcen, die er vollständig kontrolliert.

Diese DomU's sind in unserem Fall ebenso SuSE Linux Enterprise Server 10. Der Kernel dieser DomU's ist ebenso leicht verändert. Sie sind sich "bewusst", dass sie nur in virtuellen Maschinen laufen. Diese Art der Virtualisierung nennt sich "Paravirtualisierung" (Abbildung 2.1).

Eine andere Variante der virtuellen Maschinen, ist es, die Full-Virtualization (komplette Virtualisierung) einzusetzen. Dies erfordert eine kompatible Hardware (Prozessoren die bei AMD Pacifica-fähig sind oder bei Intel IVT-fähig sind). Diese Lösung ist aber wesentlich leistungsschwächer als die Paravirtualisierung und wird aufgrund der Homogenität der Umgebung und der zur Verfügung gestellten Mitteln (alle Servern werden mit SLES betrieben) nicht betrachtet.

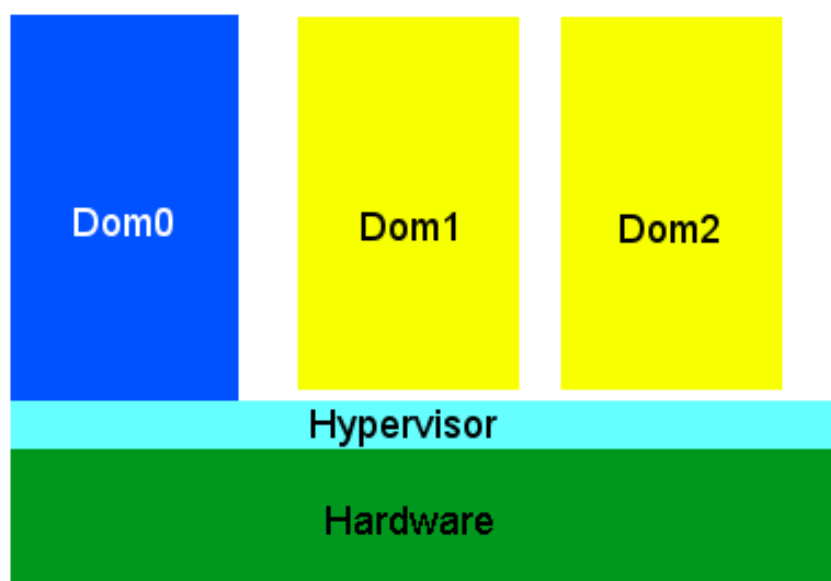


Abbildung 2.1: das Prinzip der Paravirtualisierung

Zwar wird die Leistung der verschiedenen Maschinen vermindert, dieser Verlust ist aber begrenzt und diese Lösung bleibt performant.

Vorteile der Virtualisierung sind vor allem:

- Der Verbrauch an Strom wird begrenzt. Zum Beispiel : Statt 4 Servern zu betreiben, davon 2, die nachts nicht aktiv sind, braucht man nur einen Top-Server. Darüber hinaus kann die Klimaanlage heruntergedreht werden.
- Der Wartungsaufwand wird gesenkt.
- Der Platz im Rechenzentrum (RZ) wird gespart. Dies kann die Kosten senken, wenn der Platz im RZ gemietet wurde.
- Da die kritischen Dienste in einer virtuellen Maschine "eingekapselt" sind, sind sie strikt voneinander getrennt. Wenn ein Dienst ausfällt und seine ganze VM einfriert, werden die anderen VM von diesem Problem nicht beeinträchtigt und die kritischen Dienste können weiterlaufen.
- Die Kosten für die Lizenzen werden reduziert: MLP kauft Novell Lizenzen für die Wartung von SLES (Patches, Support, usw.). In unserem Fall wurden Lizenzen für die zwei physikalischen Maschinen erworben: die 6 virtuellen Maschinen konnten direkt auf die Repository von Patches zugreifen, ohne sich bei Novell anmelden zu müssen.

2.1.2 Xen steuern

Basis für die Erstellung einer VM ist eine Konfigurationsdatei, die sich im Verzeichnis `/etc/xen/vm` befindet.

Der Name der Datei entspricht dem Namen der Virtuellen Maschine aus Sicht von Xen (es handelt sich nicht um den Hostnamen!).

In dieser Datei können sehr viele Parameter geändert werden, wie z.B. die Anzahl der Prozessoren, die der VM zugeordnet sind, die Größe des zugewiesenen Speichers, wie viele Netzwerkkarten es gibt und mit welcher Bridge sie verbunden sind, usw.

xend ist ein Deamon, der innerhalb der Dom0 läuft. Er bildet eine Schicht zwischen dem Hypervisor und dem Dom0 und kann mittels des Kommandos xm die virtuellen Instanzen verwalten.

Xenstore ist die Konfigurationsdatenbank aller virtuellen Instanzen. Sie befindet sich auf dem Domain0. Sie speichert, z.B. welche VM es gibt, wieviele NIC sie besitzen, usw. Sobald eine Änderung an einer VM vorgenommen wird (z.B. Änderung des Speichers einer VM) wird der entsprechende Eintrag in der Datenbank ebenso verändert.

Das Tool xm (für Xen Manager) ist das Werkzeug, das den Deamon xend und somit die virtuellen Maschinen kontrollieren kann.

```
root@xenserver # xm create xen_vm
```

fährt die virtuelle Maschine xen_vm hoch. Die Konfigurationsdatei /etc/xen/vm/xen_vm muss existieren und syntaktisch korrekt sein.

```
root@xenserver # xm destroy xen_vm
```

stoppt die virtuelle Maschine „xen_vm“ unsauber. Dieses Kommando entspricht dem langen Drücken des Knopfes auf einem physikalischen Rechner, bis er angehalten wird.

```
root@xenserver # xm list
Name           ID   Mem VCPUs      State    Time(s)
Domain-0       0   537    2    r----- 31675.2
dasi-xen01     8  2048    2    -b----- 15656.2
lws-xen01      2   768    1    r----- 419002.9
tomcat-xen01   3   512    1    r----- 418979.4
```

Auflisten aller aktiven virtuellen Maschinen (diejenigen, die runtergefahren sind, werden nicht angezeigt). Das Listing enthält auch wichtige Informationen, wie die ID der VM, die Größe seines Speichers, die Anzahl der virtuellen Prozessoren, der Zustand der VM (b – blocked, r – running, p – paused, s – shutdown, c – crashed, d – dying).

2.2 Verwaltung vom Netz

2.2.1 Booten der Domain0

Xen ist lediglich für die Bereitstellung intern verbundener virtueller Netzwerkinterfaces verantwortlich.

7 Paare virtueller Schnittstellen werden in dem Domain 0 am Start erstellt. Sie dienen dazu, die physikalischen Netzwerkkarten der Domain 0 auf die virtuellen Schnittstellen der Domains U abzubilden:

Domain 0

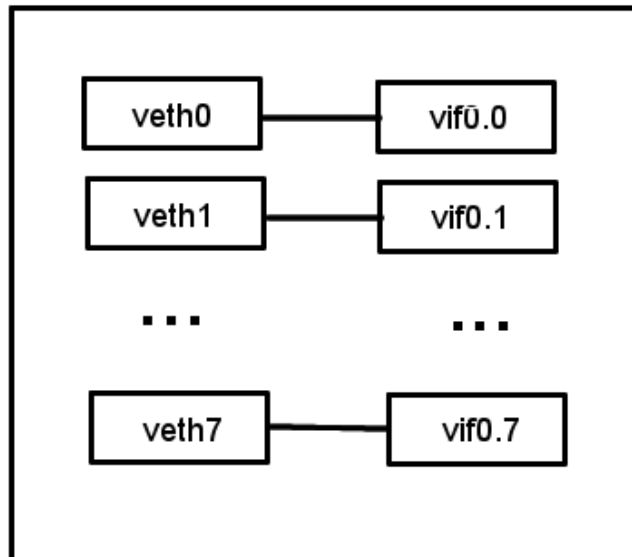


Abbildung 2.2: Virtuelle Interfaces innerhalb der Dom0

Die Skripte, die für die Einstellung der virtuellen Netzwerkumgebung zuständig sind, befinden sich im Verzeichnis `/etc/xen/scripts`. Es handelt sich um einfache Bash- bzw Python-Skripte, die ganz normale Linux-Kommandos beinhalten.

2.2.2 Booten des Domains U

Während des Bootvorgangs wird jeder neuen Domain eine neue inkrementelle ID zugeordnet (#1 für das erste hochgefahrenene Domain, #2 für das zweite hochgefahrenene Domain, auch wenn das erste schon heruntergefahren wurde)

Jeder zur Verfügung gestellten `ethX` Schnittstelle der Domains U ist eine virtuelle Interface `vifY.X` in dem Domain 0 zugeordnet. Diese Y Nummer entspricht der Xen-ID der Domains U.

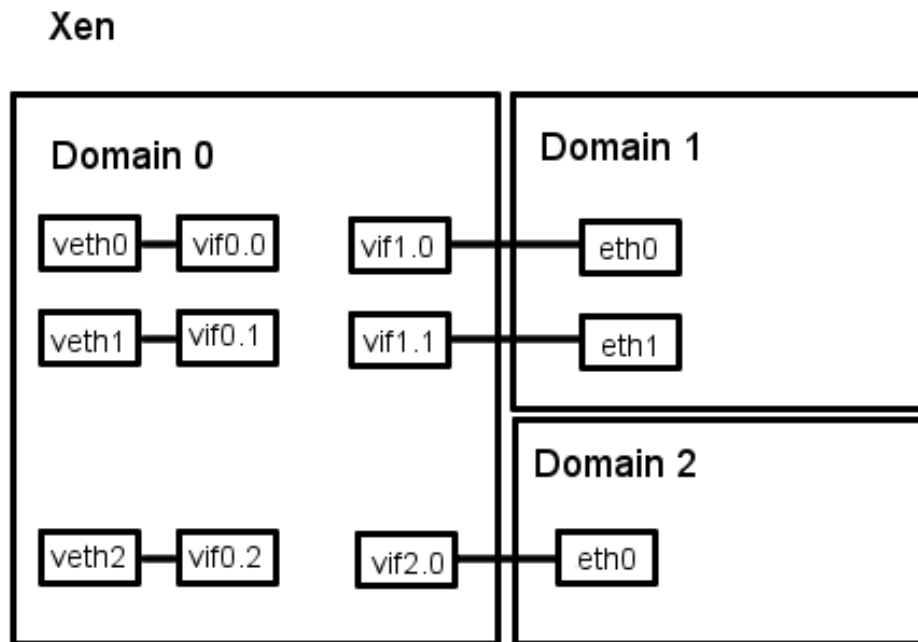


Abbildung 2.3: Virtuelle Interfaces im ganzen Xen-System

2.2.3 Bridged Networking

Das Bridged-Networking ist die Standardeinstellung für Xen3. Zwar ist es ein komplexes Verfahren, doch es ermöglicht eine sehr Hohe Anzahl an Konfigurationsmöglichkeiten.

In Abbildung 2.4 ist ein neues Gerät zu sehen : peth0, das einfach die physikalische Netzwerkkarte ist.

Der Aufbau der Bridge läuft durch die folgenden Schritte:

- 1) Die physikalische Netzwerkschnittstelle eth0 wird in peth0 umbenannt.
- 2) Die virtuelle Interface veth0 (siehe Abbildung 2.4) wird in eth0 umbenannt.

- 3) eth0 bekommt die Eigenschaften von peth0 (MAC- sowie IP-Adressen). peth0 bekommt die MAC-Adresse FF:FF:FF:FF:FF:FF und seine IP-Adresse wird entfernt.
- 4) Das ARP (Address Resolution Protocol), das auf eine Anfrage für eine bestimmte IP-Adresse die MAC-Adresse zurückgibt, wird für peth0 deaktiviert.
- 5) Das Skript erstellt die Bridge xenbr0 und fügt vif0.0 hinzu.

Somit werden alle Pakete, die ursprünglich an die Netzwerkkarte peth0 geschickt waren über die Bridge xenbr0 an die virtuelle Netzwerkkarte eth0 weitergeleitet.

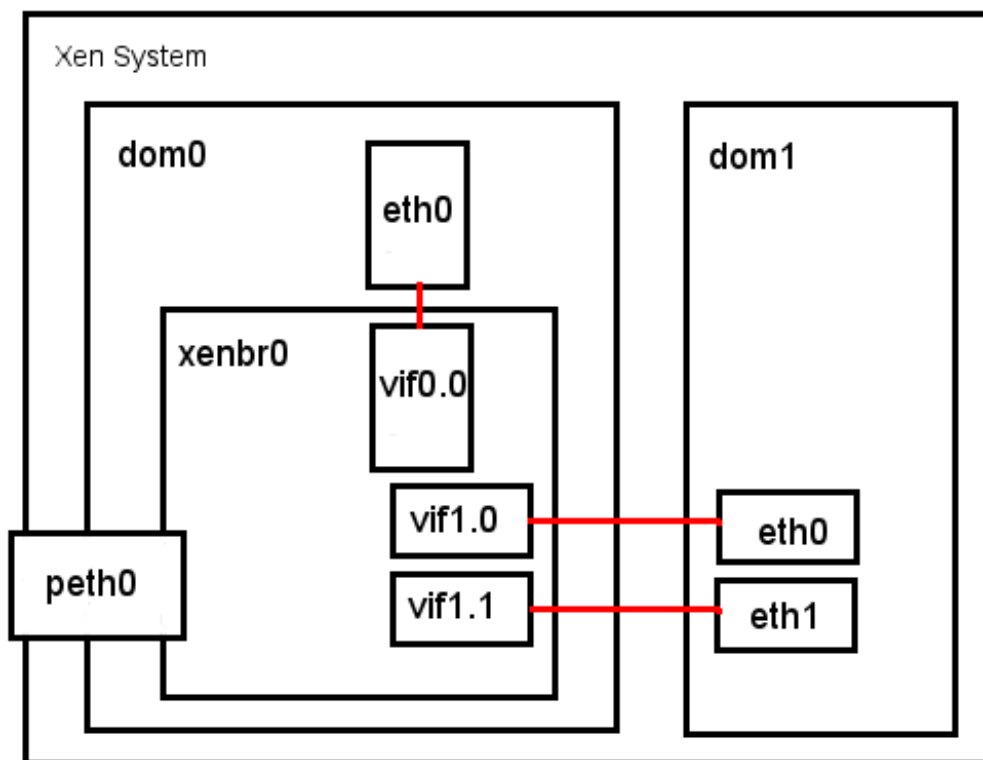


Abbildung 2.4: Bridging-Verfahren in einem Xen-System

Da sich alle Interfaces an der selben Bridge befinden, sind sie verbunden, als ob sie an

einem Hub verbunden wären und können direkt miteinander kommunizieren.

2.3 Lösung unserer Netzproblematik

Jede virtuelle Maschine soll 2 Netzwerkschnittstellen besitzen:

- die erste für die Anwendungen und die Remote-Verwaltung
- die zweite für die Backups.

Die erste Karte ist physikalisch mit dem so genannten User-LAN verbunden und die zweite mit dem sogenannten Backup-LAN.

Diese Zuordnung der Karten zu einem bestimmten LAN hat seinen Grund: Es gibt nämlich ACL's (Access Control List), die den Zugriff z.B. auf Anwendungen je nach Netzwerk (LAN) aus Sicherheitsgründen kontrollieren.

Die Lösung des Problems ist also die folgende (siehe Abbildung 2.5):

- die Backup-Interface der virtuellen Maschine muss an die Bridge der Netzwerkkarte, die physikalisch mit dem Back-up-LAN verbunden ist, angeschlossen sein.
- die User-Interface der virtuellen Maschine muss an die Bridge der Netzwerkkarte, die physikalisch mit dem User-LAN verbunden ist, angeschlossen sein. ie Datei `/etc/xen/scripts/network-bridge-wrapper` wurde neu erstellt, damit eine neue Bridge Namens `xenbr1` den virtuellen Interfaces zur Verfügung gestellt werden kann.

Die folgende Zeile wurde hinzugefügt:

```
/etc/xen/scripts/network-bridge vifnum=1 netdev=eth1 bridge=xenbr1 start
```

In den jeweiligen Konfigurationsdateien der virtuellen Maschinen wurden zwei virtuelle Netzwerkkarten hinzugefügt, die an einer der Bridges angeschlossen sind, damit sie mit dem entsprechenden LAN verbunden sind.

```
vif=[ 'mac=00:16:3e:29:fe:2d,bridge=xenbr0',  
      'mac=00:16:3e:12:fb:79,bridge=xenbr1', ]
```

Listing 2.1 : Konfigurationsdatei einer VM für die Netzwerkkarten

Auf dem Listing 2.1 ist z.B. die Konfigurationsdatei einer VM zu sehen. Die Netzwerkkarte mit der Mac-Adresse 00:16:3e:12:fb:79 ist an der Bridge xenbr1 angeschlossen. Sie wird mit dem Backup-LAN verbunden und erhält eine entsprechende IP.

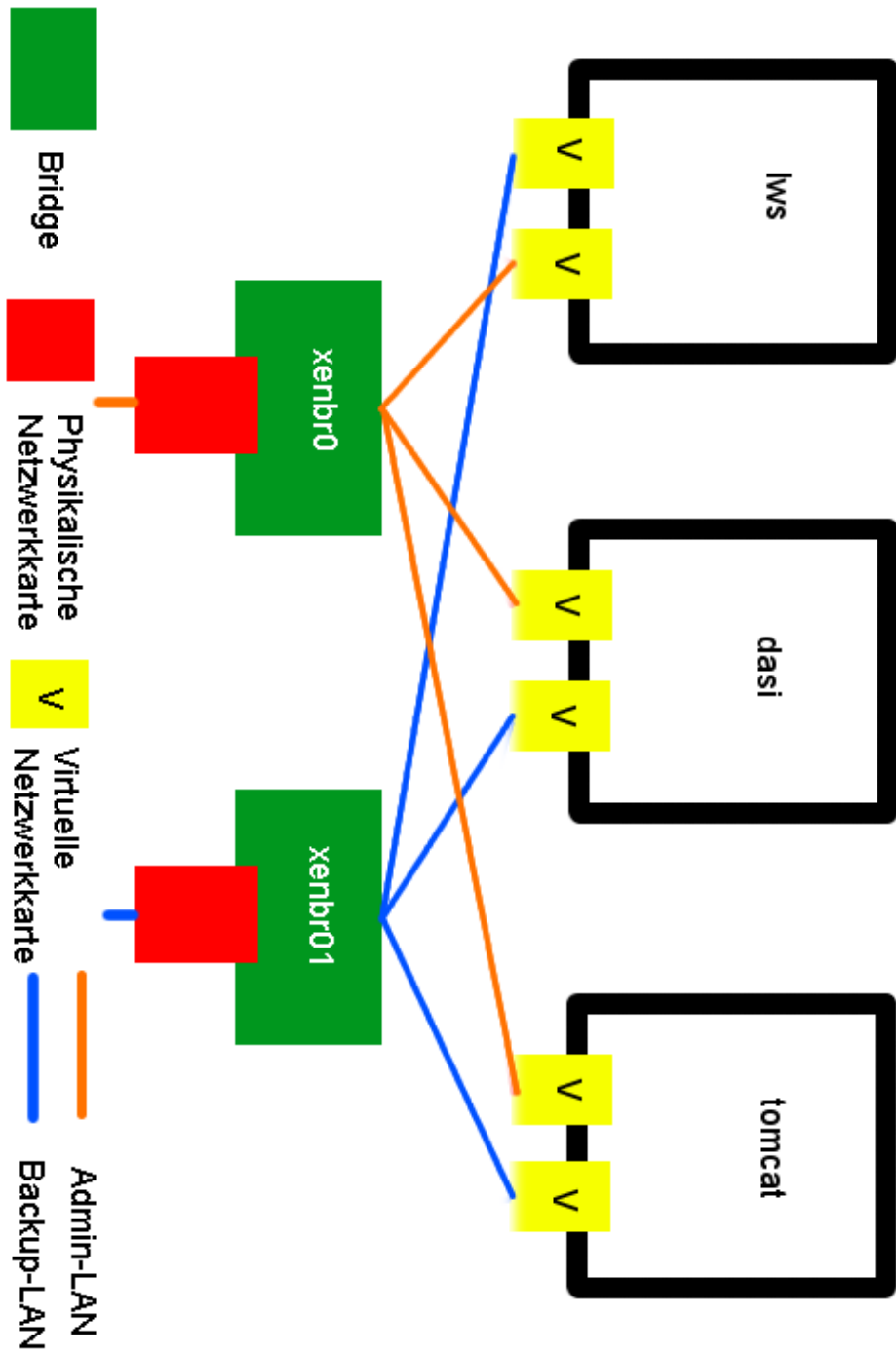


Abbildung 2.5: Lösung des Bridging-Verfahrens

3. Implementierung und Ergebnis des Programms

3.1 Implementierung

3.1.1 Installation von Themis

„Themis“ ist die Test-Maschine des Linux/Novell-Teams im OCH. Sie wird als Übergang zur Erstellung der VM benutzt. (siehe Abbildung 3.1)

Typ des Servers : HP ProLiant ML370 G4 X3,4

Physical Diskspace (GB) : 350

CPU-Type: Intel Xeon G4 3,4

Clockspeed (Mhz): 3400

Installed Memory (Mb): 1024

Number of CPU's: 1

Dieser Server verfügt über 4 Netzwerkschnittstellen:

- eine für den Administrator-Zugang
- eine für die Backups
- eine für die Users
- eine für die Remote Console

Es wurde SuSE Linux Enterprise Server 10 Service Pack 1 neu installiert:

Die Größe der Volume Group physical extend's beträgt 4MB.

Die Festplatte wurde in 3 Partitionen geteilt:

- das /boot-Verzeichnis
- das Swap-Bereich

- das LVM-Bereich, das vg00 benannt wird.

Das logische Laufwerk (Hardware RAID 1 Software) wurde nach dem folgenden Modell partitioniert.

Device	Size	Mounted on
/dev/cciss/c0d0p1	500M	/boot
/dev/cciss/c0d0p2	2G	swap
/dev/cciss/c0d0p3	1G	/
/dev/vg00/lvol1	3G	/usr
/dev/vg00/lvol2	3G	/var
/dev/vg00/lvol3	2G	/opt
/dev/vg00/lvol4	500M	/home
/dev/vg00/lvol5	1G	/tmp
/dev/vg00/lvol6	20	/local/xen/lws-vm01
/dev/vg00/lvol7	10	/local/xen/tomcat-vm01
/dev/vg00/lvol8	20	/local/xen/proxy-vm01

Paketauswahl: Server base System, Xen host

Einzelne Pakete : mc, iptraf, sysstat, kernel-xen, xen-doc-ps, xen-tools, xen, xen-doc-html, xen-libs, arptwatch, ippl

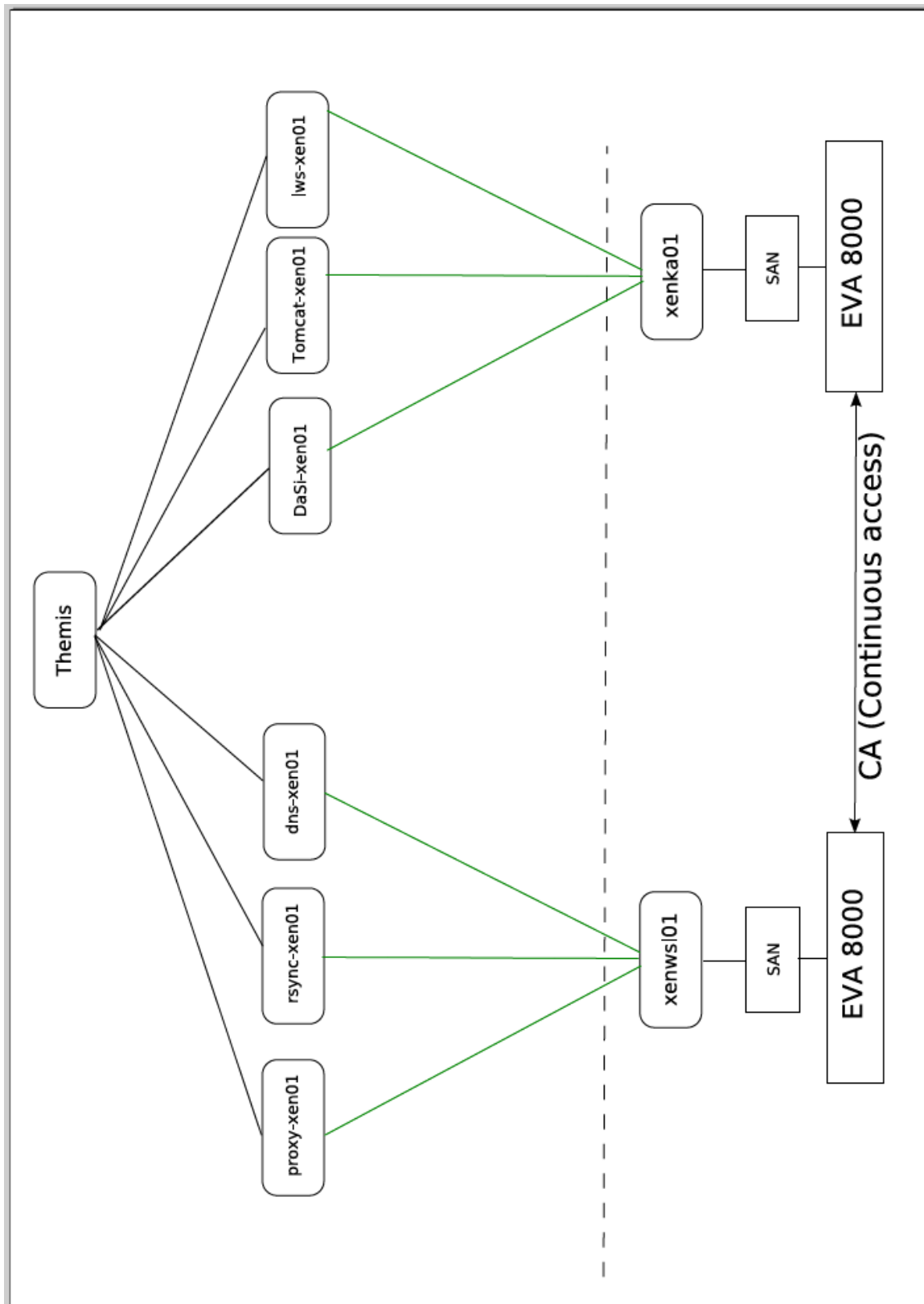


Abbildung 3.1: Schema der Installation der virtuellen Maschinen

Probleme während der Installation:

- Problem mit der Netzwerkschnittstelle : Das Bridging vom Interface eth0 hat nicht sofort geklappt. Es hat sich herausgestellt, dass die Hardware (eine Broadcom BCM5703 Gigabit-Ethernet Netzwerkkarte) nicht offiziell unterstützt wird.

```
## Aenderungen am Skript damit die Gigabit-Karte Broadcom
5703 funktioniert

    ## Herve Marcy herve.marcy@hp.com 11/07/2007
    ## Frueher:
    ##ip link set ${bridge} up
    ##add_to_bridge  ${bridge} ${vif0}
    ##add_to_bridge2 ${bridge} ${pdev}
    ##ip link set ${netdev} up
    ##ifup ${hwddev}

    ip link set ${bridge} up
    ip link set $(vif0) up
    ip link set $(pdev) up
    sleep 5
    add_to_bridge  ${bridge} ${vif0}
    add_to_bridge2 ${bridge} ${pdev}

    ## Ende der Aenderungen
```

Listing 3.1 : Verändertes Skript für die NIC von Themis

Nachdem ich in der Mailing-List von Xen gesucht habe, hat die folgende Lösung (siehe Listing 3.1) geklappt (Änderung an der /etc/xen/scripts/network-bridging Datei):

- Wir haben das Interface eth0 am Bridge xenbr0 manuell anschließen müssen:

```
root@themis # brctl addif xenbr0 eth0
```

Installation einer virtuellen Maschine

Bei der Installation der virtuellen Maschinen haben wir uns entschlossen, LVM zu installieren.

Dieses Programm stellt eine Abstraktionsschicht zwischen den Festplatten und dem Filesystem dar und erlaubt eine dynamische Verwaltung der Partitionen.

Das gestellte Problem war, dass die virtuellen Maschinen ebenso auf ein LVM-System zugreifen sollten. Dazu mussten noch die LVM-Einheiten auf eigenen Partitionen liegen, damit sie mit dem Kommando dd (Disk Dump) direkt auf einen anderen Rechner kopiert werden konnten.

Die folgende Lösung wurde eingesetzt:

- Auf dem Host-Betriebssystem wurden LVM-Einheiten in der folgenden Form erstellt: /dev/v_maschine/lvolX , wobei "v_maschine" der Name der VM und "X" die Partitionnummer ist.
- Damit der Gast (z.B. die VM lws-xen01) diese Partitionen "sehen" kann, wurde die Konfigurationsdatei /etc/xen/wm/lws-xen01 entsprechend verändert.

```
Disk=[
'file:/local/data/iso/SLES-10-SP1-i386-DVD1.iso,xvdb,r',
  'file:/local/data/iso/DP6Lx.iso,xvdc,r',
  'phy:/dev/vg_lws01/lvol1,xvda1,w',
  'phy:/dev/vg_lws01/lvol2,xvda2,w',
  'phy:/dev/vg_lws01/lvol3,xvda3,w',
  'phy:/dev/vg_lws01/lvol4,xvda4,w',
  'phy:/dev/vg_lws01/lvol5,xvda5,w',
  'phy:/dev/vg_lws01/lvol6,xvda6,w',
  'phy:/dev/vg_lws01/lvol7,xvda7,w' ]
```

Listing 3.2 : Host-Konfigurationsdatei

Dieser Vorgang hat einen wichtigen Vorteil: Als die erste VM fertig wurde, wurde der Inhalt der jeweiligen Partition kopiert, so dass die Erstellung der virtuellen Maschinen wenig Zeit gedauert hat (siehe Abbildung 3.1). Einige Veränderungen sind aber trotzdem notwendig gewesen (Änderung der jeweiligen Hostnamen).

Auf allen virtuellen und physikalischen Maschinen wurde das Paket sysstat installiert. Es ist wichtig, um die Performance zu messen, und um die Engpässe bei den jeweiligen Rechnern zu entdecken.

Probleme

Das folgende Problem ist aufgetreten:

Wenn die folgende Meldung regelmäßig auf dem Standard Output erscheint:

```
INIT: Id "x0" respawning too fast: disabled for 5 minutes
```

muss die folgende Linie in der Datei `/etc/inittab` mit “#” auskommentiert werden

```
x0:12345:respawn:/sbin/agetty -L 9600 xvc0 xterm
```

3.1.2 Installation von xenka01 und xenwsl01

Aufgerüstet wurden :

- 1570 MB RAM zusätzlich
- eine zusätzliche Fibre Channel-Karte

Pro Server stehen 4 SAN Ports zur Verfügung:

- Port 4 ist nicht angeschlossen
- 1 für Backup Reserviert (Port 5)
- 2 für Zugriff auf das Storage (Port 2 und 3)

Nachdem wir den Server xenka01 neu installiert hatten, konnten wir ihn nicht booten. Problem war, dass wir ein PAE-Kernel gewählt hatten. Dieser Kernel ist für Servern, die ab 4GB RAM besitzen, geeignet. Da unser Server genau 4096 MB RAM enthält, wurde diese Option von SLES standardmäßig gewählt. Wir haben den Server ohne PAE-Kernel neu installiert. Der Fehler ist auf Themis nicht aufgetreten, weil er nur 3 GB RAM hat.

Damit die virtuellen Instanzen wie geplant die Bridges benutzen, müssen die Interfaces auf xenka01 und xenwsl01 die gleichen Namen haben.

Sie müssen umbenannt werden, um dem folgenden Schema zu entsprechen:

Dom0:

eth0 User/ZSS LAN

xenka01

IP-Adresse: 10.96.30.28

MAC-Adresse: 00:02:A5:4F:8D:16

eth1 Backup LAN

xenka01

IP-Adresse: 10.96.181.11

MAC-Adresse: 00:08:02:28:DC:4E

eth2 Admin LAN (wird in der Zukunft abgebaut)

xenka01

IP-Adresse: 10.96.180.11

MAC-Adresse: 00:08:02:C5:63:63

Die Dateien `ifcfg-eth0`, `ifcfg-eth1` sowie `ifcfg-eth3` im Verzeichnis `/etc/sysconfig/network` sind für die Zuordnung von Namen zu den Mac-Adressen und wurden also angepasst.

Beispiel für die Karte eth1:

Ergebnis des Kommandos „`lspci`“:

```
root@xenka01 # lspci
[...]
0a:02.0 Ethernet controller: Intel Corp. 82546EB Gigabit
Ethernet Controller (Copper) (rev 01)
```

In der Datei `/etc/sysconfig/network/ifcfg-eth1` wurde der Eintrag hinzugefügt:

`_nm_name='bus-pci-0000:0a:02.0'`

So entspricht der Interface eth1 die physikalische NIC .

Nach seiner Installation wurde der Server aus Wiesloch nach Karlsruhe umgezogen und an den SAN angeschlossen.

3.1.3 Installation von den produktiven virtuellen Maschinen

Die produktiven virtuellen Maschinen wurden mit Hilfe des Kommandos dd (Disk-dump) aus den logical volumes von Themis auf die neuen volumes von xenka01 kopiert und je nach Bedarf konfiguriert.

Die virtuellen Maschinen, für die ich zuständig war, waren:

3.1.3.1 lws-xen01

lws heißt Linux Web Services. Auf diesem Server wurden die folgenden Anwendungen mit dem SuSE-Tool „Yast“ installiert : PHP (Version 5.1.2) MySQL (5.0.26) sowie Apache2 (Version 2.2.3), die für die Entwicklung von Web-Anwendungen sehr beliebt sind.

Aufgabe dieses Servers ist es, den HP-Mitarbeitern (Administratoren sowie Helpdesks) Tools zur Verfügung zu stellen, um die täglichen Probleme innerhalb des MLP-Netzes zu lösen. Dies erfolgt mit Web-Anwendungen, die auf dem Content Management System (CMS) Typo3 basieren.

Bisher war auf Cerberus die Version 3.8.1 installiert. Mithilfe des Moduls „Full-Backup“ wurde auf Cerberus eine .tar.gz-Datei erstellt.

Dieses Typo3-Modul wurde dann ebenso auf lws installiert, brauchte aber das PHP-Modul „php5-ctype“, das mit Yast installiert wurde.

Die direkte Wiederherstellung der Backup-Datei mit dem Typo3-Modul "Full backup" ist gescheitert, so dass die .tar.gz-Datei manuell in die entsprechende Verzeichnisse entpackt wurde und die MySQL Datenbank (Namens "Typo3") erst aus Cerberus mithilfe des folgenden Kommandos exportiert wurde:

```
root@cerberus # mysqldump -p Typo3 > cerberus_mysql.bak
```

und dann auf lws importiert wurde

```
root@lws # scp root@cerberus:/root/cerberus_mysql.bak .  
root@lws # mysql -p Typo3 < cerberus_mysql.bak
```

Typo3 wurde dann von der Version 3.1.8 auf die Version 4.1.2 upgraded.

Wegen der Sicherheitspolicy der MLP AG musste die Verbindung zwischen dem Server und dem Host mit dem SSL-Protokoll zu verschlüsseln. Ein Certificate Request wurde mit OpenSSL erstellt:

```
root@lws # openssl req -new -nodes -key id_dsa -out cert.csr
```

Dieses Request wurde Mitarbeitern der MLP AG geschickt, damit sie dieses Zertifikat mit dem MLP CA (Certificate Authority) unterschreiben.

Nachdem wir das unterschriebene Zertifikat bekommen haben, wurde die Konfigurationsdatei (/etc/apache2/vhosts.d/vhost-ssl.conf) des virtuellen Hosts von Apache entsprechend verändert, um SSL zu aktivieren.

Es wurde eine Umleitung von den http-Seiten auf die https-Seiten erstellt, damit alle Verbindungen verschlüsselt übertragen werden.

```
<VirtualHost lws:80>
    Redirect permanent / https://lws.mlp-ag.com/
</ VirtualHost>
```

Die CGI- sowie Perlskripte für das Ändern der Samba-Passwörter sowie das Löschen der Unison ID's wurden im Verzeichnis /srv/www/cgi-bin kopiert und angepasst.

Die Typo3-Seiten wurden verändert, um diese Skripte in zu berücksichtigen (Änderungen von den „cerberus“-Einträge in „lws“).

Das Tool Statusboard wurde ebenso von Cerberus auf lws kopiert. Da aber die Verbindung mit von MLP unterschriebenen SSL-Zertifikaten schon eingesetzt wurde, wurde die Installation mit den folgenden Kommandos durchgeführt:

```
root@cerberus # mysqldump -p mlpincident > statusboard.bak
```

```
root@lws # scp root@cerberus:/root/statusboard.bak .
root@lws # mysql -p mlpincident < statusboard.bak
```

Im Verzeichnis /home/sysad von Cerberus befinden sich zahlreiche wichtige Skripte, die für das Senden von Mails und automatisierte Aktionen zuständig sind. Es wurde auf lws ebenfalls kopiert, um einen reibungslosen Betrieb von Statusboard zu gewährleisten.

```
root@lws # scp -r root@cerberus:/home/sysad /home/
```

Die SSL-Zertifikate und die Apache-Konfigurationsdatei

/etc/apache2/vhosts.d/statusboard.conf

wurden auf lws kopiert. Die Apache Konfigurationsdatei wurde ebenfalls verändert, um

die mit http angefragten Seiten mit SSL-Verschlüsselung zu übertragen

```
<VirtualHost statusboard:80 >  
    Redirect permanent / https://statusboard.mlp-  
ag.com/  
</VirtualHost>
```

Da die HP-Mitarbeiter eine große Zahl von Skripten pflegen sollen, wurde die Versionierungsanwendung Subversion (Version 1.4.4 aus einer .tar.gz Datei) ebenfalls auf lws installiert. Die Dokumentation bezüglich der Installation von SVN würde die Rahmen dieser Diplomarbeit sprengen und wurde von daher nicht hinzugefügt, sie steht aber den HP-Mitarbeitern auf dem Sharepoint des Linux-Novell-Teams zur Verfügung.

3.1.3.2 tomcat-xen01

Tomcat ist der Name eines von der Apache Foundation entwickelten Web-Anwendungen Servers.

Aufgrund der Spezifikationen des Entwicklers der Anwendungen wurden folgende Programme in den folgenden Versionen installiert:

- JDK (Java Development Kit) Sun 1.5.0_12 per RPM-Paket installiert.
- Tomcat 5.5.23 wurde im Verzeichnis /usr/local/tomcat installiert.

Auf Anfrage unseres Entwicklers sollte Tomcat am Port 8081 und nicht am üblichen Port 8080 lauschen. die Konfigurationsdatei /usr/local/tomcat/conf/server.xml wurde wie folgt verändert (nur der Wert von Connector Port wurde verändert):

```
<!-- Define a non-SSL HTTP/1.1 Connector on port 8080 -->  
<Connector port="8081" maxHttpHeaderSize="8192"  
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"  
    enableLookups="false" redirectPort="8443" acceptCount="100"  
    connectionTimeout="20000" disableUploadTimeout="true" />  
<!-- Note : To disable connection timeouts, set connectionTimeout value  
to 0 -->
```

Listing 3.3: Tomcat-Konfigurationsdatei

Damit Tomcat als Unix Daemon läuft, wurde das folgende Skript in /etc/init.d/tomcat geschrieben.

```
#!/bin/bash
#
# Startup script for the Tomcat server
#
# chkconfig: - 83 53
# description: Starts and stops the Tomcat daemon.
# processname: tomcat
# pidfile: /var/run/tomcat.pid

# See how we were called.
case $1 in
start)

export JAVA_HOME=/usr/java/
export CLASSPATH=/usr/local/tomcat/common/lib/servlet-
api.jar
export CLASSPATH=/usr/local/tomcat/common/lib/jsp-
api.jar
sh /usr/local/tomcat/bin/startup.sh
/usr/local/tomcat/jsvc -Djava.endorsed.dirs=/usr/local/
tomcat/common/endorsed -cp
/usr/local/tomcat/bin/bootstrap.jar -outfile
/usr/local/tomcat/logs/catalina.out -errfile
/usr/local/tomcat/logs/catalina.err
org.apache.catalina.startup.Bootstrap
;;
stop)
sh /usr/local/tomcat/bin/shutdown.sh
;;
```

```
restart)
sh /usr/local/tomcat/bin/shutdown.sh
sh /usr/local/tomcat/bin/startup.sh
;;
*)
echo "Usage: /etc/init.d/tomcat start|stop|restart"
;;
esac
exit 0
```

Listing 3.4: Skript zum Starten von Tomcat als Unix-Deamon

Ein Link wurde ebenfalls in `/etc/init.d/rc3.d/` erstellt, damit die Mysql-Datenbank als Service gestartet wird, nachdem der Server hochgefahren wird.

Das folgende Kommando ist dazu erforderlich gewesen, um die Datenbank zum Laufen zu bringen:

```
root@tomcat # mysql : chown -R mysql:mysql /var/lib/mysql/mysql
```

Um Klarheit in der DB zu schaffen wurden alle Datenbanken außer „dbprinters“ gelöscht. „dbprinters“ ist nämlich die einzige Datenbank, die von der Java-Anwendung benutzt wird.

Der User `dbprinters@localhost` wurde gelöscht, denn es stellte ein Problem der Kompatibilität mit dem User `dbprinters`.

Das Skript `checkservices.pl`, das die Verfügbarkeit der Dienste auf dem Server überprüft, wurde im Verzeichnis `/opt/HP/scripts` kopiert und an die installierten Dienste angepasst.

Die Notes ID's wurden im Verzeichnis `/srv/www/notes` kopiert. `htaccess`-Dateien gewährleiten die Sicherheit der ID's.

Die Synchronisierung der ID's wird durch das Skript /opt/HP-zentrale/scripts/notes-wget-sync.pl ausgeführt. Das Skript wurde ebenfalls an den neuen Server angepasst.

Die Perl-Tools von MLP wurden im Verzeichnis /usr/lib/perl5/5.8.8/MLP kopiert.

3.2 Tests und Ergebnis

3.2.1 Tests der virtuellen Maschinen

Dieser Testplan wurde von dem Linux-Novell-Team im OCH vorbereitet. Der Kunde wurde von seiner Durchführung nicht informiert. Er kann davon ausgehen, dass der Betrieb durch die virtuellen Maschinen im Desaster-Fall weiterlaufen wird.

Der folgende Testplan für die verschiedenen VM's wurde durchgesetzt:

lws-xen01	Zugriff https://lws.mlp-ag.com Admin/FDL Netz? -> SSL?	ok
	Zugriff https://statusboard.mlp-ag.com Admin/FDL/BNK Netz? -SSL?	ok
	Erstellen neuer Gegis & Mailversand möglich	Freischaltung für Mailversand von Gegi eMails smtprelay -> 25
	Nachstart Rsync über lws funktioniert?	ok
	Nachstart Dasisync über lws funktioniert?	unmöglich zu erfahren
	Samba PW reset	ok
	Rollout Webseite	ok
	unison key files löschen	ok
	sieht hub db einträge (fehlgeschlagene rysnacs)	ok
	Subversion aktiv & installiert	ok

Tabelle 3.1: Testplan für lws-xen01

tomcat-xen01	Zugriff auf PrinterDB über tst02001?	down
	wget von NotesID's aus den Standorten	ok
	Transfer von NotesID von mlp01admin auf tomcat-xen01? -> samba mapping	freischaltung zss -> mlp01admin samba

Tabelle 3.2: Testplan für tomcat-xen01

3.2.2 Tests der Performance

Die Performance der virtuellen Maschinen sowie der Hosts wurden gemessen. Die folgenden Grafiken sind die von dem Tomcat-Server. Man kann hier sehen, dass, ausser einige hochbelastete Zeitpunkte, der Betrieb der VM einwandfrei ist. Darüber hinaus wurde kein Swapping von Linux eingesetzt.

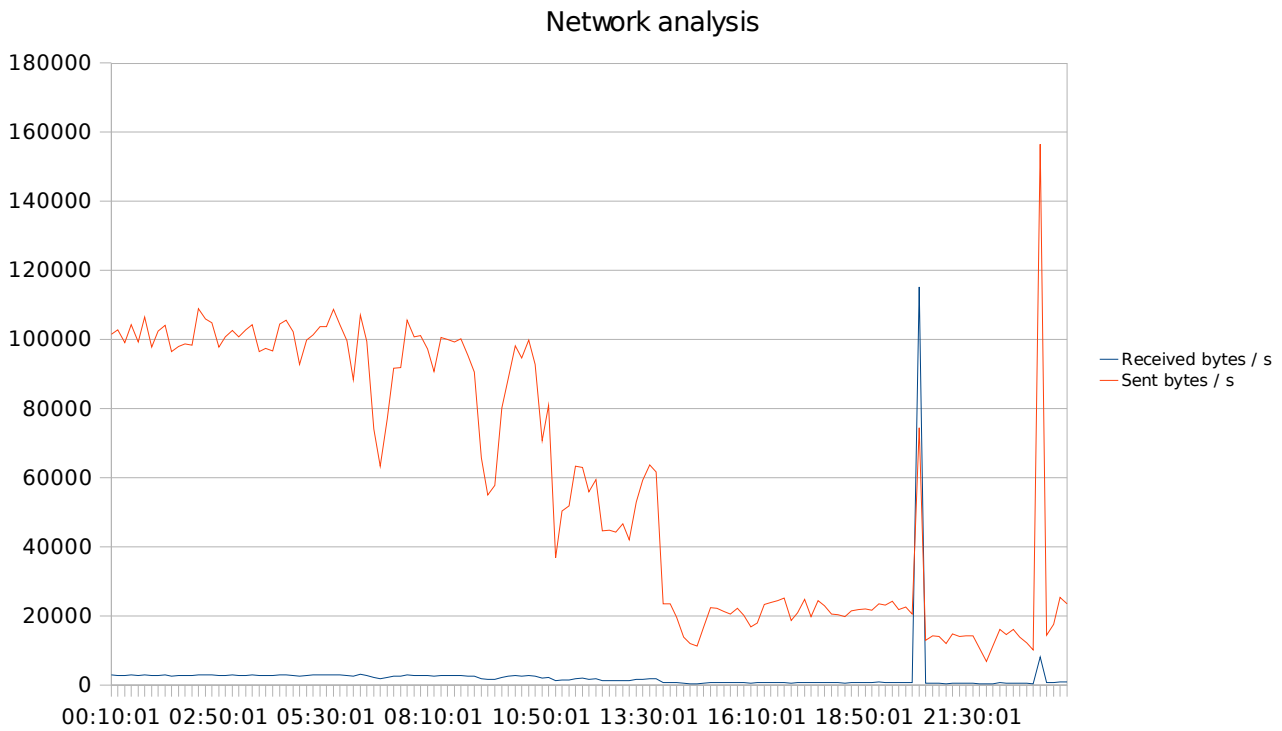


Abbildung 3.2: Performance des Netzwerks

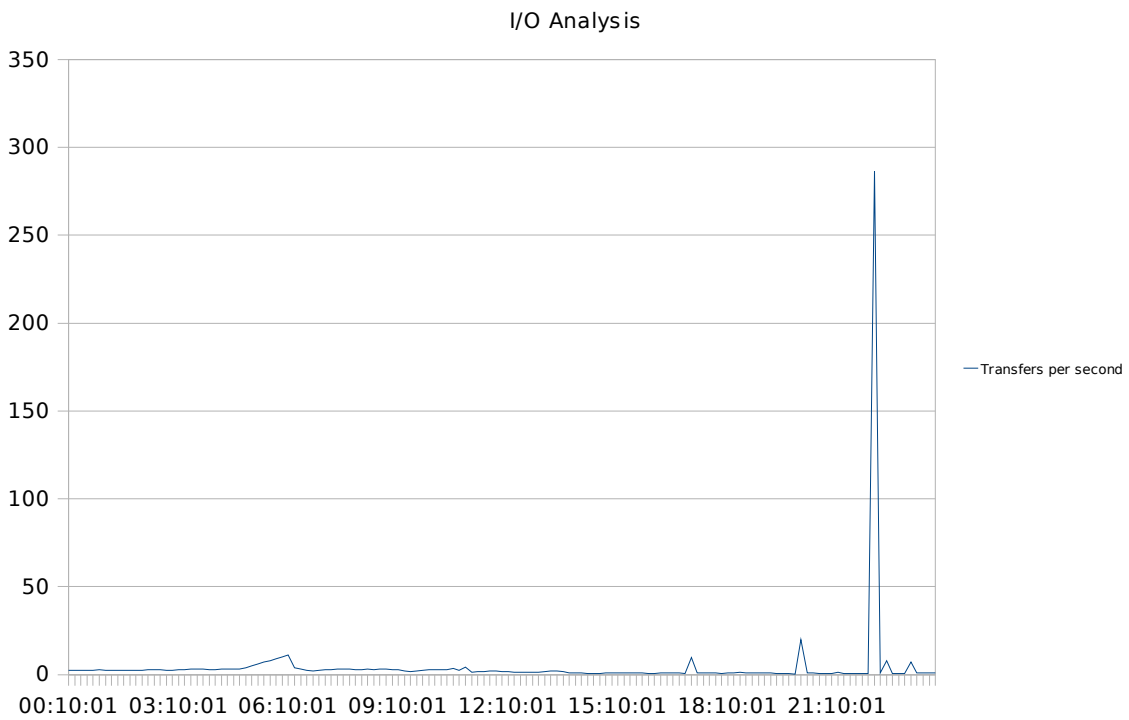


Abbildung 3.3: Performance des I/O

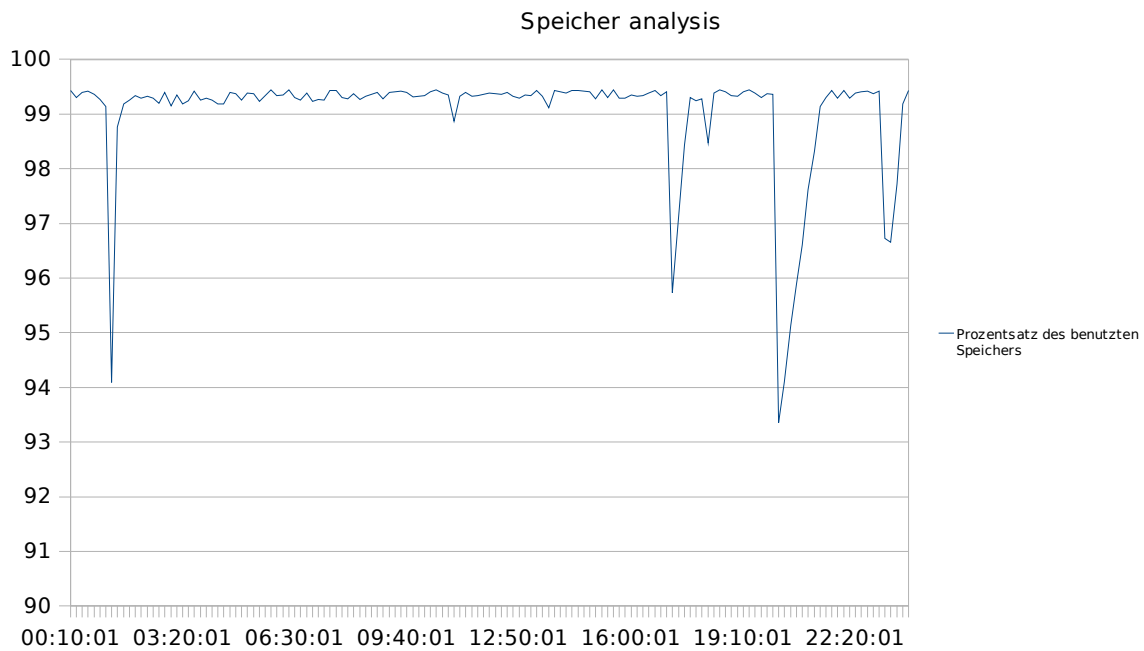


Abbildung 3.4 : Performance des Speichers

3.2.3 Tests des ganzen DR-Programms

Voraussetzungen für den Test des ganzen Programms und für einen erfolgreichen Einsatz des DRP sind:

1	CA – Spiegelseite, konsistent und verfügbar
2	XEN Host Server (domain0) im Ausweichrechenzentrum mit Anbindung an die EVA
3	Netzwerkverbindungen zum Operation Center und in die Standorte vorhanden.

Tabelle 3.4: Bedingungen für das DRP

	Maßnahmen	Min.
1	Feststellung welche virtuellen Maschinen sich bereits im Ausweich-RZ befinden.	5
2	Für die verbleibenden VM's, drehen der DR Gruppen in das Ausweich-RZ	30
3	Integritätscheck der Daten im SAN KA	30
4	Anpassung der Hauptspeicherkonfiguration der existierenden VM's auf den DR Wert	15
5	Start der verbliebenen VM's mit der DR Hauptspeicherkonfiguration (default)	15
6	Funktionstest der virtuellen Instanzen	30
		125

Tabelle 3.5: Recovery-Zeiten

3.3 Akzeptanz beim Kunden und Weiterentwicklung

3.3.1 Akzeptanz beim Kunden

Die Implementierung des Projekts wurde -unter anderem- aufgrund der Verzögerung beim Backups von zbs001 ein bisschen verspätet. Der Server musste neuinstalliert werden und der Name musste von zbs001 in xenwsl01 geändert werden. Das Backup von zbs001 ist aber gescheitert. Da wir uns in einer produktiven Umgebung befinden, war es nicht denkbar, einen Server zu installieren, ohne sich auf eine vernünftige Backup-Möglichkeit verlassen zu können.

Das DRP Projekt ist aber bei den Tests erfolgreich vom Kunden abgenommen worden. Die Xen-Umgebung befindet sich also im Einsatz.

3.3.2 Weiterentwicklung

Der Anteil von Linux-Servern im Rechenzentrum der MLP AG ist noch gering. Noch werden zahlreiche Netware-Server betrieben. Die Firma Novell will seinen Kunden die Möglichkeit geben, Netware weiterzubetreiben. Der Kunde darf das Betriebssystem betreiben so lange wie er möchte.

Doch alle Dienste, die auf Netware liefen wurden nun auf Linux portiert und Novell definiert sich unter anderen als „Linux-Firma“. Die Innovationskraft um Linux ist sehr stark. Beweis dafür ist dieses DRP, das sich mit Netware erheblich schwerer implementieren lassen würde. Der Anteil von Linux-Servern in den Data-Centers wird in den nächsten Jahren vermutlich wachsen. Da die Xen-Technologie jetzt zum Kompetenz-Spektrum der Mitarbeiter des OPC gehört, kann sie wieder eingesetzt werden, um die Rahmen des DR- Projekts z.B. auf das Monitoring des Netzes zu erweitern.

Glossar

Disaster Recovery

Der Begriff Disaster Recovery (englisch für Notfallwiederherstellung) bezeichnet Maßnahmen, die nach einem Unglücksfall in der Informationstechnologie eingeleitet werden. Dazu zählt sowohl die Datenwiederherstellung als auch das Ersetzen nicht mehr benutzbarer Infrastruktur und Hardware.

Virtualisierung

Technik zum Verbergen der physikalischen Eigenschaften eines Rechners, damit andere Systeme, Anwendungen, oder Endbenutzer mit diesen Ressourcen umgehen können. Eine einzige physikalische Ressource (wie ein Server, ein Betriebssystem, eine Anwendung oder ein Speichergerät) scheint wie mehrere logische Ressourcen, zu funktionieren, oder mehrere physikalische Ressourcen (wie Speichergeräte oder Server) scheinen wie eine einzige Ressource zu funktionieren.

Storage Disk Array

Ein Disk Array ist ein Gerät, welches mehrere Festplatten beinhaltet und diese Servern zur Verfügung stellt. Funktionalitäten wie RAID, Storage-Virtualisierung, Kopien oder Spiegelungen innerhalb des selben oder auch zwischen Disk-Arrays werden direkt auf diesen ohne Beteiligung der Server ausgeführt.

Fibre Channel

Fibre Channel ist ein Standardprotokoll aus dem Bereich der Speichernetzwerke. Es ist für serielle, kontinuierliche Hochgeschwindigkeitsübertragung großer Datenmengen konzipiert worden. Die erreichten Bandbreiten liegen heute bei 4 Gb/s (4GFC), was im Vollduplex-Betrieb für Datentransferraten von 800 MB/s ausreicht.

Tomcat

Apache Tomcat stellt eine Umgebung zur Ausführung von Java-Code auf Webservern bereit. Es handelt sich um einen in Java geschriebenen Servlet-Container, der mithilfe des JSP-Compilers Jasper auch JavaServer Pages in Servlets übersetzen und ausführen kann. Dazu kommt ein kompletter HTTP-Server.

LUN

LUN bezeichnet in der EDV eine Logical Unit Number und wird zur Zuordnung für die Ansteuerung von Geräten im SCSI-Bus verwendet.

In modernen Storage Area Networks spielt die LUN-Adressierung eine große Rolle, da hier ein Disk Array viele virtuelle Festplatten zur Verfügung stellen kann.

Samba

Samba ist eine freie Software-Suite, die das Server-Message-Block-Protokoll (SMB) für Unix-Systeme verfügbar macht.

Samba ist damit in der Lage, Funktionen eines Windows-Servers zu übernehmen.

Swap

Dieses Wort beschreibt in der Informatik das Schreiben von Daten, die sich im schnellen, aber kleinen Hauptspeicher des Computers befinden, auf den langsamen, aber großen Hintergrundspeicher (wie z.B. eine Festplatte) und umgekehrt das Laden solcher Daten aus dem Hintergrund- in den Hauptspeicher.

Abkürzungsverzeichnis

CA	Continuous Access
CMS	Content Management System
DaSi	Datensicherung
DRP	Disaster Recovery Project
EVA	Enterprise Virtual Arrays (HP Storage Disk Array)
GPL	GNU General Public License
HP	Hewlett-Packard
ILO	Integrated lights out
ITIL	IT Infrastructure Library
LUN	Logical Unit Number
LVM	Logical Volume Manager
NIC	Network Interface Card
OCH	HP Operation Center Heidelberg
RZ	Rechenzentrum
SAN	Storage Area Network
SLES	SuSE Linux Enterprise Server
USV	Unterbrechungsfreie Stromversorgung
VM	Virtuelle Maschine

Abbildungsverzeichnis

1.1: Physikalische Einstellung in den Rechenzentren.....	Seite 10
1.2: Implementierungsplan	Seite 13
1.3: Maßnahmenabfolge	Seite 15
1.4: Ist- und Soll-Zustand	Seite 21
2.1: das Prinzip der Paravirtualisierung	Seite 27
2.2: virtuelle Interfaces	Seite 30
2.3: virtuelle Interfaces im ganzen Xen-System innerhalb der Dom0	Seite 31
2.4: Bridging-Verfahren in einem Xen-System	Seite 33
2.5: Lösung des Bridging-Verfahrens	Seite 35
3.1: Schema der Installation der virtuellen Maschinen	Seite 38
3.2: Performance des Netzwerks	Seite 53
3.3: Performance des I/O	Seite 53
3.4 : Performance des Speichers	Seite 54

Literaturverzeichnis

- [SprBenZdrDeh2007] Henning Sprang, Timo Benk, Jaroslaw Zdrzalek,
Ralph Dehner
„Xen, Virtualisierung unter Linux“
OpenSource Press, 2007
- [WikiWeb] Ehrenamtliche Autoren
„XenNetworking“
[http://wiki.xensource.com/xenwiki/XenNetworking?
highlight=%28networking%29](http://wiki.xensource.com/xenwiki/XenNetworking?highlight=%28networking%29)
- [HP2007] HP Marketing Division
„HP StorageWorks XP disk array software“
[http://h20195.www2.hp.com/V2/GetDocument.aspx?
docid=0900a5a580d7d64a&cc=de&lc=de](http://h20195.www2.hp.com/V2/GetDocument.aspx?docid=0900a5a580d7d64a&cc=de&lc=de)
- [WikiWeb] Ehrenamtliche Autoren
„Wikipedia – Die freie Enzyklopädie“
„<http://www.wikipedia.org>“, 2007

Diese Diplomarbeit wurde mit den folgenden Programmen erstellt :

- OpenOffice.org
- the GIMP
- Inkscape

Vielen Dank an ihre Autoren !



„Design und Implementierung eines Disaster-Recovery Programms für Xen-virtualisierte Linux-Server im Falle eines kompletten Ausfalls eines Rechenzentrums“
by Hervé Marcy is licensed under a [Creative Commons Attribution-Share Alike 3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/).