HOCHSCHULE DER MEDIEN

Medieninformatik

Bachelorthesis

zur Erlangung des akademischen Grades
Bachelor of Science

Open-Source-basierte Server-Infrastruktur für das Convergent Media Center der Hochschule der Medien Stuttgart

Eingereicht von: **Ingo Ebel**

ingo.ebel@ingoebel.de

Betreut von: **Prof. Roland Kiefer**
Prof. Dr. Wolfgang von Keitz

Eingereicht am: 15. Dezember 2008

Eidesstattliche Erklärung

Ich erkläre hiermit, dass ich die vorliegende Bachelorthesis „Open-Source-basierte Server-Infrastruktur für das Convergent Media Center der Hochschule der Medien Stuttgart“ selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel verfasst habe.

Außerdem versichere ich, dass ich die Inhalte dieser Arbeit in keinem anderen als diesem Prüfungsverfahren angemeldet habe.

Stuttgart, den 15. Dezember 2008

Ingo Ebel

Danksagung

Diese Thesis ist komplett mit Freier Software entstanden. Daher möchte ich an erste Stelle allen danken, die Freie und Open-Source-Software möglich machen, allen Entwicklern, Denkern, Evangelisten, Designern, Musikern, Anwendern und so weiter. Ihr seid spitze und es ist schön, dass es soviel gute Produkte und Ideen durch euch gibt!

"human knowledge belongs to the world"
-"milo hoffmann" in antitrust

Mein persönlicher Dank geht an:

- Daniel Schneider
- Frank Hoffmann
- das RadioTux-Projekt
- Prof. Dr. Wibke Weber
- Michaela Stumberger
- David Prüm
- Helena Lauber

Ein großer Dank geht außerdem an das Rechenzentrum der HdM, das mir bei allen Problemen immer geholfen und Tipps gegeben hat, manchmal auch zu Tageszeiten, an denen sonst niemand mehr an der HdM war. Insbesondere sind dabei Hans-Joachim Czech und Janosch Andrews zu nennen.

Kurzfassung

Diese Arbeit beschreibt den Aufbau einer Infrastruktur für das Convergent Media Center an der Hochschule der Medien in Stuttgart auf Basis von Open Source-Komponenten. Dabei wird auf die wichigsten Dienste und Einstellungen eingegangen. Es werden die eingesetzten Technologien und Konzepte beschrieben. Ein Überblick über Groupware wird gegeben sowie die Umsetzung einer Ausgewählten im Rahmen der Infrastruktur. Das Thema Datensicherheit und Hochverfügbarkeit wird am Beispiel von Backup und Failover des Servers beschrieben. Abschließend wird ein Ausblick auf anschließende Projekte gegeben.

Schlagwörter: CMC, HdM, Convergent Media, Medien, Open Source, Linux, SSO, Backup, DRBD, Heartbeat, Windows, Mac OS X, LAMP, Groupware

Abstract

This thesis describes the architecture based on open source components used for the Convergent Media Center at the university of applied science in Stuttgart. It demonstrates the assigned technologies and concepts. An overview of groupware is given and it is explained how the chosen one was applied to the CMC's infrastructure. "Data security" and "high availability" are also discussed using the example of backup and failover for the server. The last part describes feature projects related to the architecture.

Tags: CMC, HdM, Convergent Media, Media, Open Source, Linux, SSO, Backup, DRBD, Heartbeat, Windows, Mac OS X, LAMP, Groupware

Inhaltsverzeichnis

Danksagung II

Abbildungsverzeichnis VII

Tabellenverzeichnis VIII

1 Einleitung: Medienproduktion an der HdM 1
- 1.1 Das Convergent Media Center . . . 1
- 1.2 Erste Ideen: IT-Infrastruktur CMC . . . 5
- 1.3 Ziele der Thesis . . . 5
- 1.4 Motivation . . . 5
- 1.5 Aufbau der Arbeit . . . 6

2 Aufbau 7
- 2.1 Netz . . . 7
- 2.2 Hardware . . . 10
- 2.3 Betriebssystem . . . 11
  - 2.3.1 Anmerkungen zum OS und Konvention . . . 12
  - 2.3.2 Risiken beim Einsatz von Open Source . . . 13
  - 2.3.3 Partitionierung und SSL-Zertifikate . . . 13

3 Serverdienste 15
- 3.1 OpenLDAP: Zentrale Authentisierung . . . 15
- 3.2 Mailserver: Rückgrat jeder elektronischen Kommunikation . . . 17
  - 3.2.1 MTA Postfix . . . 17
  - 3.2.2 IMAP/POP3-Server Cyrus . . . 19
  - 3.2.3 Antispammaßnahmen . . . 20
    - 3.2.3.1 Restrictions . . . 20
    - 3.2.3.2 Greylisting . . . 23
    - 3.2.3.3 Policyd-weight . . . 24
    - 3.2.3.4 Viren und andere Krankheiten . . . 25
- 3.3 Samba: Windows-Dienste auf Linux . . . 26
  - 3.3.1 Versionen . . . 26
  - 3.3.2 Domain Controller . . . 27
- 3.4 Nagios: Netzwerk-Monitoring . . . 29
  - 3.4.1 Nagios-Plugins . . . 30

3.4.2 Nagios-Objekte und -Benachrichtigungen . . . 31
3.4.3 Vorteile, Nachteile und mehr Plug-Ins . . . 32
3.5 Apache: HTTP-Server . . . 33
3.5.1 Konfiguration und Sicherheit . . . 33
3.5.2 LAMP . . . 35
3.5.3 Anwendungen auf LAMP . . . 36
3.6 DHCP: Automatische Netzwerkeinstellungen . . . 37
3.7 FTP: Datentransfer über weite Strecken . . . 38

4 Backup: Datensicherung und Failover 41
4.1 Allgemeine Überlegungen . . . 41
4.2 Strategien . . . 41
4.2.1 Rsync über ssh . . . 42
4.2.2 LVM . . . 43
4.2.3 Failover mit DRBD/Heartbeat . . . 43
4.3 Umsetzung . . . 44
4.3.1 DRBD . . . 44
4.3.2 Heartbeat . . . 47

5 Groupware 50
5.1 Auswahl: Kriterien . . . 50
5.2 Auswahl: Software . . . 52
5.3 Umsetzung und Installation Open Xchange . . . 54
5.4 Betrieb und Nutzung von Open Xchange . . . 57

6 Single Sign On 61
6.1 Vor- und Nachteile von SSO . . . 63
6.2 SSO im CMC . . . 63
6.2.1 Mac OS X mit LDAP-Authentifikation . . . 64
6.2.2 SSO mit Apache und Firefox unter Windows . . . 66

7 Open Source Software auf den Clients 68

8 Zukunft/Mögliche Anschlussprojekte 71
8.1 Sicherheit . . . 71
8.2 Kerberos . . . 72
8.3 Ausbau Netz auf Glasfaser oder 1000MB Ethernet . . . 73
8.4 Automatische Software-Verteilung . . . 74
8.5 OpenVPN . . . 75
8.6 SyncML Funambol . . . 76

Literaturverzeichnis 78

Glossar 81

Lizenz 85

Abbildungsverzeichnis

1.1 CMCLogo . . . 1
1.2 Arbeiten im CMC . . . 3
1.3 Das Audio- und das Videostudio im CMC . . . 4

2.1 Schematische Darstellung aller wichtigen Komponenten . . . 9
2.2 Beispiel einer fehlgeschlagenen Verbindung, weil die RootCA nicht importiert wurde im Firefox . . . 14

3.1 UCS-Domänen-Konzept[10] . . . 16
3.2 LDAP-Browser: JXplorer . . . 17
3.3 Statistik über eingesetzte Mailserver[19] . . . 18
3.4 Angenommene und abgelehnte E-Mails innerhalb eines Monats . . . 20
3.5 Eingebundene Samba Shares unter Windows Vista (User redakteur) 27
3.6 Nagios-Statusmap und ein Teil der Service-Übersicht . . . 31
3.7 NagVis mit einer Map eines Serverraumes als Hintergrund (Quelle: http://nagvis.org/screenshots) . . . 33
3.8 Website der Redaktion Zukunft . . . 37

4.1 Separates Netz für DRBD/Heartbeat . . . 45
4.2 DRBD beim Syncronisieren . . . 47

5.1 Ein Groupware-Server mit verschiedenen Anbindungen [3] . . . 51
5.2 Open-Xchange-Logo . . . 54
5.3 Verteiltest Open-Xchange-System[20] . . . 55
5.4 Schematische Darstellung OX4UCS mit Clients, die im CMC eingesetzt werden . . . 57
5.5 Infostore über SSL auf verschiedenen Systemen . . . 58
5.6 Kontakt- und Kalenderverwaltung . . . 60

6.1 Lösungsansätze für SSO[39] . . . 61
6.2 SSO mit Tickets bzw. Token[17] . . . 62
6.3 “SSO” an einem LDAP[17] . . . 64
6.4 Mac OS X, Verzeichnisdienste-Programm . . . 65
6.5 LDAP-Pfade konfigurieren für Mac OS X . . . 66

8.1 Marktanteile von Smartphones . . . 77

Tabellenverzeichnis

3.1 Beispiele für Befehle bei der Windows-Anmeldung 28

5.1 Vergleich von Groupware-Lösungen 53

7.1 Links zu eingesetzter Software 70

1 Einleitung: Medienproduktion an der HdM

Wurde vor einigen Jahren noch von Multimedia gesprochen, tauchen heute verstärkt die Schlagworte Convergent Media und Crossmedia auf. Im Folgenden wird beschrieben, wie die Hochschule der Medien (HdM) in Stuttgart damit umgeht und was diese Thesis dazu leistet.

1.1 Das Convergent Media Center

Das Convergent Media Center (CMC) ist ein neues fakultäts- und studiengangsübergreifendes Ausbildungscenter für Studierende der Hochschule der Medien (HdM) in Stuttgart; es ist sowohl Forschungslabor für Medienkonvergenz als auch Think Tank für die Medienwirtschaft[5].

Das Herzstück des CMC ist der 170 qm große Newsroom, bestehend aus einem großen Redaktionsraum, einem Audiostudio und einem Videostudio. In diesem Arbeits- und Lehrraum arbeiten und lernen ca. 100 Studierende pro Semester aus verschiedenen Studiengängen, von Mediapublishing über Informationsdesign bis hin zu Medienwirtschaft und Electronic Media. Das CMC soll Studierende optimal auf eine spätere Berufstätigkeit in der Medienbranche vorbereiten. Das prozessorientierte crossmediale Lernen ergänzt dabei die bestehende produktorientierte Lehre (vgl. [8]).

Schwerpunkte der Convergent-Media-Strategie sind:

- Konzentration auf Medienkonvergenz

Abbildung 1.1: CMCLogo

- Konzentration auf Work-Flow und Arbeitsprozesse in der Medienproduktion
- Interdisziplinarität durch fakultäts- und studiengangsübergreifende Lehre: Vernetzung von Medientechnologie, Journalismus, Design und Medienwirtschaft
- Entwicklung einer neuen Lehr- und Lernarchitektur
- Erforschung und Entwicklung von neuen crossmedialen und medienkonvergenten Strategien

Im Mittelpunkt steht das medienkonvergente und prozessorientierte Arbeiten für Print, Online, TV, Radio, Mobile.

Im Newsroom wird der Arbeitstag einer Redaktion simuliert. „Die Studierenden recherchieren und redigieren, schreiben Artikel für Print und Online, produzieren Audio- und Video-Beiträge, layouten und gestalten Infografiken, programmieren Webseiten und Widgets. Sie übernehmen dabei verschiedene Rollen: die des redaktionellen Planers, des Reporters, des Redakteurs, des Audio-, Foto- oder Videojournalisten, des Layouters und Screen-Designers. Unter Zeitdruck müssen die Studierenden Geschichten schreiben und mit Blick auf das spezifische Medium die jeweiligen Stärken identifizieren und unmittelbar umsetzen.“[5] Die Studierenden arbeiten wenn möglich tagesaktuell, bei größeren Projekten auch wochen- oder monatsaktuell. Die Zielplattform ist vorrangig das Online-Journal `http://www.redaktionzukunft.de`; eine Printausgabe befindet sich gerade in der Entwicklungsphase, ebenso die Konzeption für Mobile-Geräte und Embedded systems.

Das CMC ist eine der ersten Lehrredaktionen in Deutschland, die explizit auf konvergentes, prozessorientiertes, multimediales Arbeiten wert legt, bei dem also der „Convergent Media Journalism“ im Vordergrund steht. Die HdM verfolgt dabei eine arbeitsmarktnahe und eine an der aktuellen Wirtschaftspraxis orientierte Lehre. „Durch das CMC wird diese Idee weiter vorangetrieben und intensiviert, indem bereits bestehende aber auch neue wirtschaftliche Kooperationen zunehmend in innovative Lehrkonzepte übergehen.“[8]

HoRadS/stufe

An der HdM existieren einige Projekte, die Medienproduktion schon eine ganze Weile betreiben. Die Studierenden können in mehreren dieser Projekte arbeiten. HoRadS und stufe sind zwei Beispiele, die im Besonderen mit dem CMC vernetzt sind.

HoRadS, das HochschulRadio Stuttgart, ist das Campusradio der Hochschulregion Stuttgart-Ludwigsburg. HoRadS ist ein nichtkommerzielles Lokal-Radio (NKL) und

(a) Der CvD des Tages (b) Gruppe von Studierenden (c) Studentin schneidet ein Interview

(d) Arbeitsplatz während der Mittagspause (e) Studentinnen beim Text schreiben (f) Plasmabildschrim mit offener Redaktion Zukunft-Seite

Abbildung 1.2: Arbeiten im CMC

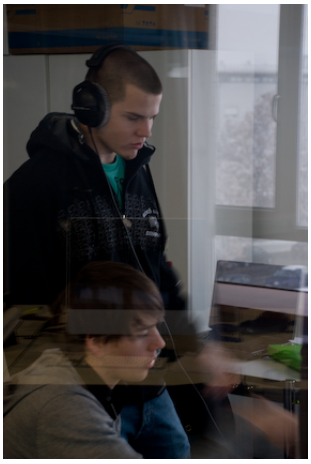
wird getragen vom HoRadS e.V., an dem mehrere Hochschulen und Universitäten aus Stuttgart und Umgebung beteiligt sind. Studenten können das Medium Radio praxisnah kennen lernen und sich zum Beispiel an der Programmplanung, dem Producing, als Moderator, Reporter oder der Musikredaktion beteiligen. HoRadS sendet seit dem 1. Januar 2004. Angefangen hat es mit einem kleinen Produktionsstudio an der Fakultät für Information und Kommunikation der Hochschule der Medien in Stuttgart, Standort Wolframstraße. Als abzusehen war, dass der Platz nicht ausreichte, wurde am Standort Nobelstraße der Hochschule der Medien ein Studio in Betrieb genommen, das den kompletten Sendeablauf übernahm. 2005/2006 wurden dann zwei weitere Studios bzw. Redaktionsräume an der Nobelstraße errichtet und die Wortredaktion zog in diese Räume ein. HoRadS ist auf der UKW-Frequenz 99,2 MHz und im Kabel auf 102,1 MHz zu empfangen und sendet wöchentlich 32 Programmstunden. Auf der Website http://www.horads.de ist der Sender rund um die Uhr als Live-Stream zu hören.

Stufe – das HdM webcast TV – ist das Studentenfernsehen der Hochschule der Medien und existiert seit dem WS 05/06. Es ist ein selbst organisiertes studentisches Projekt, welches allen Studierenden offen steht und ihnen die Chance bietet, sich redaktionell und technisch mit der Produktion einer Fernsehsendung auseinanderzusetzen. Mehrmals pro Semester entsteht eine TV-Sendung, die abgerufen werden kann unter http://stufe.tv.

(a) Produktion der stufe-Sendung

(b) Weißabgleich für die Kamera

(c) Blick vom Audio- ins Videostudio



(d) Studenten bei Aufnahmen im Audiostudio

Abbildung 1.3: Das Audio- und das Videostudio im CMC

Die Studenten können sowohl im CMC als auch bei HoRadS und stufe beteiligt sein, Beiträge können sich in unterschiedlichen Kanälen wiederfinden, so kann ein im CMC produzierter Videobeitrag auch bei stufe laufen oder ein Audiobeitrag bei HoRadS, ebenso ist der umgekehrte Weg möglich, dass ein Audio- oder Videobeitrag von HoRadS oder stufe auch als Podcast[1] auf dem Online-Journal redaktionzukunft.de benutzt wird. Ein weiterer wichtiger Punkt ist der Erfahrungsaustausch zwischen den Studierenden und Projekten, um Wissen oder bewährte Verfahrensweisen weiterzuvermitteln.

[1] Auch wenn der Begriff Podcast hier nicht korrekt ist, Podcasts sind eine Reihe von Medienbeiträgen (Episoden), die über einen RSS-Feed automatisch bezogen werden können; heute wird das Wort Podcast aber auch synonym für einen on demand abrufbaren Audio-/Videobeitrag verwendet.

1.2 Erste Ideen: IT-Infrastruktur CMC

Damit das CMC die Arbeit aufnehmen kann, muss eine Vernetzung aller beteiligten Medien geschehen, außerdem wird ein Server zur Datenablage benötigt. Eine Windows-Domäne, in der alle Rechner zusammen geschaltet sind, wird den späteren Administrationsaufwand verringern. Daher soll es auch möglichst nur einen Authentisierungsdienst geben, damit Single Sign On möglich wird. Eine Groupware kann als Kommunikationsplattform dienen. Um Ausfallsicherheit und Sicherheitsaspekte im Allgemeinen zu gewährleisten, müssen Pläne gemacht werden, außerdem müssen die bestehenden Strukturen von HoRadS und stufe berücksichtigt werden und ggf. eingebunden werden.

1.3 Ziele der Thesis

Mit dieser Thesis soll der Aufbau der IT-Infrastruktur für das Convergent Media Center der Hochschule der Medien dokumentiert werden. Erklärt werden sollen die wichtigsten Entscheidungen, Konzepte und Änderungen. Wenn möglich werden weiterführende Literaturhinweise oder Links gegeben, in denen sich der geneigte Administrator weiter einarbeiten kann. Diese Arbeit ist zum einen als Dokumentation für Administratoren gedacht, die eine ähnliche Problemstellung zu bearbeiten haben, daher werden gewisse Grundkenntnisse vorausgesetzt. Auf der anderen Seite richtet sich die Arbeit auch an IT-Entscheider, die die Möglichkeiten von Open Source in der Medienbranche kennenlernen wollen.

1.4 Motivation

Die Motivation zu dieser Bachelorarbeit resultiert aus den interessanten und spannenden Möglichkeiten, die sich aus einem konvergenten Medienprozess und Lernprozess ergeben, aber auch aus dem Wunsch, das mit einem möglichst großen Anteil von FLOSS (Free/-Libre/Open Source Software) zu gestalten. Open Source ist mittlerweile “Mainstream”, d. h. in vielen Unternehmen, bei vielen Benutzern präsent, ob nun in Form von Programmen auf dem eigenen Rechner, ob als Set-top-Box unter dem Fernseher, als DSL-Router daheim, als Fenster zum Internet und als großer Träger des Internets in Form von Servern, manchmal mehr, manchmal weniger offensichtlich.

Mit dieser Arbeit soll ein Grundstein gelegt werden, wie eine IT-Infrastruktur für medienkonvergentes und prozessorientiertes Arbeiten im Lehrbereich aussehen kann und wie dies mit Open-Source-Komponenten fast völlig zu realisieren ist.

1.5 Aufbau der Arbeit

Der Aufbau der vorliegenden Bachelor Thesis gliedert sich wie folgt:

Am Anfang stehen der Aufbau des Netzes, generelle Einstellung wie IP und Hostname, SSL-Zertifikate sowie die Entscheidungen für Hardware und Betriebssystem. Im Kapitel 3 werden die einzelnen Serverdienste, die wichtig sind für den Betrieb, beschrieben, und es werden Abweichungen von der Standardinstallation des Betriebssystems dokumentiert. Darauf folgt die Beschreibung der Backup-Lösung. Kapitel 5 geht auf die Entscheidung für die Groupware-Lösung sowie dessen Umsetzung ein.

Single Sign On (SSO) ist auch ein Buzzword und wird meistens auf Basis eines Verzeichnisdienstes realisiert. Kapitel 6 geklärt, was SSO ist und wie es zur Zeit in der CMC-Infrastruktur eingesetzt wird.

Eingeschoben wurde das Kapitel 7 über Open Source Software auf den Clients, welches auf die Vorteile von Freier Software allgemein eingeht sowie welche Software von den Studenten auf den Windows- und Macclients verwendet wird.

Abschließend findet sich ein Blick in die Zukunft der Infrastruktur sowie möglicher Anschlussprojekte im Kapitel 8.

2 Aufbau

Bevor in den nächsten Kapiteln auf die Dienste und Projekte eingegangen wird, soll an dieser Stelle erst geklärt werden, für welche Umgebung die Serverstruktur entstehen soll, welche Netzkomponenten berücksichtigt werden müssen, welche Hardware benötigt wird und welches Basisbetriebssystem eingesetzt wird.

2.1 Netz

Das Rechenzentrum der Hochschule der Medien stellt dabei den Platz für die Server sowie alle Switches (hauptsächlich von der Firma Cisco, aber auch einige von 3Com). Außerdem werden die Leitungen zwischen allen Rechnern und Servern, ebenso die VoIP-Telefone, von der Haustechnik betreut und werden hier nicht extra betrachtet. Auch die Verkabelung in den Räumen wird als gegeben angesehen.

Die Switches sind größtenteils mit ihrer IP-Adresse bekannt und können auch überwacht werden (siehe Abschnitt 3.4 dazu), sie sind hier aber vollkommen transparent und unterliegen nicht unserer Kontrolle, genauso wie die Firewalls.

Die Hochschule betreibt außerdem ein eigenes WLAN-Netz, welches über das gesamte Gebäude verteilt ist. Dennoch musste ein extra WLAN-Accesspoint mit eigener SSID im Raum 148 aufstellen werden, da sonst die Windows-Domain-Anmeldung nicht funktioniert hätte. Dies ist ein Linksys-WRT-WLAN-Router, der auf einer Frequenz funkt, auf den er möglichst wenig Störung gegenüber dem HdM-WLAN verursacht.

Der wesentlich größte Teil des neuen CMC ist der Raum 148, der Newsroom. Hierfür wurden fünf Desktop-Rechner beschafft sowie fünf Laptops von Dell, außerdem ein iMac und zwei MacMinis der Firma Apple. Hinzu kommt der Drucker, der ebenfalls als Netzwerkkomponente zählt und seine Dienste über verschiedene Protokolle anbietet. Diskutiert wurde der Einsatz von Thin Clients, dieser Ansatz wurde jedoch verworfen, da Audio- und Videoschnitt, welcher viele Ressourcen braucht, auf allen Rechnern möglich sein sollte.

Für das CMC wurde vom Rechenzentrum der öffentliche Adressbereich 141.62.96.0/24 zugewiesen. Der Router ist 141.62.96.254. Im Zuge der Vereinfachung würde der vorher

separate IP-Adressbereich für das Studentenfernsehen stufe entfernt und in das CMC-Netz aufgenommen. Neben diesem existiert noch ein weiterer Bereich, der dem HochschulRadioStuttgart zugewiesen ist; dies betrifft das Netz 141.62.53.160/27 mit den nutzbaren Adressen von 141.62.53.161 - 141.62.53.188, da die .189 vom RZ belegt wird sowie die .190, die den Router darstellt – in diesem Bereich sind kaum noch freie Adressen verfügbar. Alle Hauptserver befinden sich jedoch in diesem Adressbereich, so hat der neuaufgebaute Server die IP 141.62.53.165 und bietet unter dieser IP bzw. dem Domainnamen media.hdm-stuttgart.de seine Dienste auch im Internet an. Um ebenfalls das CMC-Netz direkt zu bedienen, was für alle Dienste wichtig ist, die auf Broadcasts lauschen sollen, wurde dem Server als VLAN nach IEEE 802.1q[1] auf demselben Interface die IP-Adresse 141.62.96.1 zugewiesen. Dazu ist das Paket vlan nötig, außerdem muss das Modul 8021q geladen (`modprobe 8021q`) und in `/etc/modules` eingetragen werden. Damit können alle Netzwerkgeräte innerhalb des 141.62.53.160/27- und 141.62.96.0/24-Netzes direkt angesprochen werden. Der WLAN-Accesspoint hängt ebenfalls im 141.62.96.0/24-Netz daher können alle Serverdienste auch über das WLAN erreicht werden, es wird nach den besten Möglichkeiten mit WPA2 gestützt.

Insgesamt besteht das Netz aus:

- 22 Windows Clients, davon
  - 13 Windows XP
  - 9 Windows Vista
- 3 Mac OS X Clients
- 1 WLAN Access Point
- 1 Color Laser Drucker
- 6 Server

Der neue Server muss auch Dienste für verschiedene Laptops von Studenten und Professoren anbieten, die im Newsroom einen der freien Netzzugänge benutzen.

Das Projekt soll außerdem zur Konsolidierung beitragen. Bei Beginn des Projektes war für die Dateiablage bei HoRadS ein Windows-2000-Server zuständig, ein Domaincontroller existierte nicht, die Daten wurden per rsync auf einen Linux-Server (RHEL)

[1] Virtual Local Area Network, als IEEE 802.1q standardisiert, auch tagged VLAN genannt, dazu werden in den Ethernet-Frame vier zusätzliche Bytes eingeführt: eine zusätzliche Typangabe und das TCI-Feld (Tag Control Information). Letzteres enthält die Priorität, das Format und die VLAN-ID des 802.1q-Frame, siehe auch http://de.wikipedia.org/wiki/VLAN und http://www.linux-magazin.de/heft_abo/ausgaben/2006/11/patchen_ohne_kabel

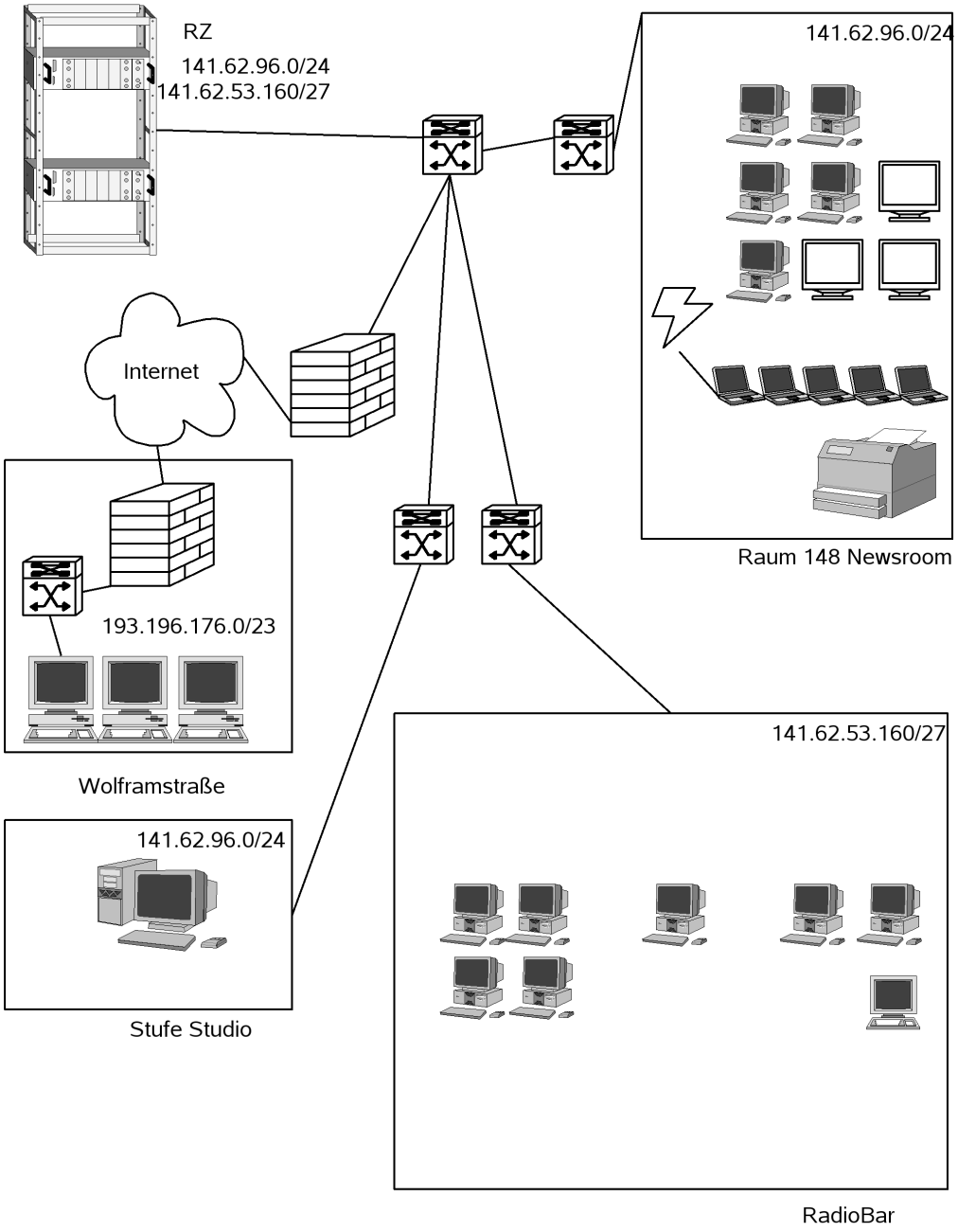


Abbildung 2.1: Schematische Darstellung aller wichtigen Komponenten

gezogen, außerdem existierte ein Mailserver am Standort Wolframstaße der Hochschule (SW), der Großteil der Server stand aber im Rechenzentrum des Standortes Nobelstraße (SN). Das Studenten-Fernsehen war nicht daran angeschlossen und sicherte seine Daten nur lokal. Mit der Intrastruktur des CMC sollte eine zentrale Datenspeicherung entstehen, bei der alle Beteiligten, die ihre Daten untereinander austauschen können, sowie die zurzeit benutzen HoRadS-Server für die Windowsfreigabe und der Mailserver auf einer Maschine untergebracht werden. Auf die anderen Server wird nicht weiter im Einzelnen eingegangen, einige werden noch konsolidiert, andere sind für das Streaming von HoRadS notwendig.

2.2 Hardware

Für die Serverhardware wurde ein CALLEO-300-Server der Transtec AG[2] aus Tübingen gewählt. Dies war das beste Angebot in Bezug auf das Preis-Leistungs-Verhältnis. Der Server wurde folgendermaßen konfiguriert:

- 1 x AMD Dual-Core Opteron 2212, 2.0 GHz (max. 2 Opteron-Socket-F-Prozessoren)
- NVIDIA nForce MCP55-Chipsatz
- 8 GB DDR2 ECC
- 3ware 9650SE-8LPML RAID-Controller:
  - 5x 750 GB Serial ATA-2 Festplatte, 7200 U/min, 3.5"
  - als RAID 5 konfiguriert = 3TB Speicherplatz
- 2x PCI-Express x8 low-profile Slots
- 2x 64-bit 133/100 MHz PCI-X low-profile Slots
- 2x 64-bit 100 MHz PCI-X low-profile Slots
- onboard ATI-ES1000-Grafik
- onboard dual MCP55 Pro Chipsatz Gigabit Ethernet Controller
- 2 HE Rackmountgehäuse inkl. Einbauschienen
- slimline DVD-ROM und slimline Floppy-Laufwerk

[2] http://www.transtec.de/

- 560 Watt Netzteil
- ohne Betriebssystem
- 5 Jahre Vor Ort Service

Als Backupserver wurde ein ähnlicher Server aus demselben Hause genommen mit nur 1,8 Ghz AMD Dual-Core Opteron und 2 GB DDR2 ECC RAM, jedoch ebenfalls mit 3ware-RAID-Controller und 3 Terabyte Speicherplatz.

2.3 Betriebssystem

Das Operation System (OS) sollte ein GNU/Linux werden. Die Lizenzkosten sind wesentlich geringer als bei einem Windows-Server, es gibt unzählige Software für diesen Betriebssystem-Typ, außerdem kann auf die Hilfe von Tausenden von Entwicklern und Benutzern zurückgegriffen werden(Community). Dadurch, dass der Quellcode (Source Code) verfügbar ist, können Änderungen notfalls auch selbst daran vorgenommen werden, d. h. auch Investitionsschutz; selbst wenn eine Software nicht weiter entwickelt würde, könnte man diese Aufgabe selber übernehmen, außerdem soll der Server ein heterogenes Netz aus Windows-, Mac- und ggf. zukünftig auch Linux-Clients betreuen können. Da Linux auf dem Server kein Einzelphänomen mehr ist, durch die gefallenen Rootserverpreise heute viele junge Leute einen eigenen Linux-Rootserver betreiben oder auf anderem Weg mit Linux in Kontakt gekommen sind, ist es auch kein Problem mehr, passende Administratoren für dieses Betriebssystem zu finden. Es gibt natürlich noch wesentlich mehr Gründe, auf Open Source zu setzen; einige davon sind im Kapitel 7 nachzulesen. Ebenso gibt es auch Nachteile, z. B. dass auf einem Linux noch kein vollständiger Active Directory Domain Controller nachgebildet werden kann (siehe dazu Abschnitt 3.3), diese Nachteile wiegen uns aber nicht die Vorteile auf.

Auch wenn GNU/Linux in vielen Varianten/Distributionen[32] komplett kostenlos zu benutzen ist, sollte bei diesem Projekt auf eine Enterprise-Distribution gesetzt werden, d. h. es gibt einen Maintenance-Vertrag mit dem Distributor, der dafür Sorge trägt, dass Updates für Sicherheitslücken zeitnah zur Verfügung gestellt werden, der eine langjährige Produktpflege verspricht und im Problemfall auch Support bietet.

Der Transtec-Server hätte die SUSE Linux Enterprise Server 10 (SLES) mitliefern können, eine andere große Enterprise-Distribution wäre Red Hat Enterprise Linux (RHEL) gewesen, die Entscheidung fiel aber für eine Debian-basierte Distribution aus dem Hause Univention, Bremen. Diese Distribution nennt sich Univention Corporate Server (UCS)

und zeichnet sich durch ein zentrales Server- und Client- sowie ein plattformübergreifendes Managementsystem aus. Sie bietet ein zentrales Identitymanagement auf Basis von OpenLDAP und eine einfache Administration über ein Webinterface. Das System kann somit auch von einem Administrator ohne spezielle Linux-Kenntnisse betreut werden. Dieses Konzept, alles in ein LDAP zu speichern und darum eine geschickte Webadministrationsoberfläche zu bauen, gefiel auf Anhieb, auch deckten sich die angebotenen Dienste/Softwarekomponenten mit vielen, deren Einsatz bei dem Projekt geplant wurden. Univention stellt alle Eigenentwicklungen unter die GPL[3] , damit ist auch die oben genannte Investitionssicherheit gegeben. Diese Vorteile sprachen für die Distribution. Der Server hat 8 GB an RAM; um diese voll nutzen zu können, wird auf eine 64bit-Variante von UCS 2.1 gesetzt.

2.3.1 Anmerkungen zum OS und Konvention

Da UCS als Betriebssystem eingesetzt wird, erleichtert das bei der Einrichtung einiger Dienste die Arbeit. Diese Thesis beschreibt Software-Pakete, die nicht bei UCS Standard sind, dabei genauer und gibt auch Konfigurationshinweise, geht jedoch nicht auf das Selbererstellen und Kompilieren von Debian-Paketen ein; siehe dazu http://forum.univention.de/viewtopic.php?f=20&t=553. Alle Beschreibungen sind möglichst so gefasst, dass diese auch auf anderen Linux-Distributionen angewendet werden können, wenn der Administrator weiß, wo Pakete für seine Distribution zu finden sind bzw. wie er selbst Software kompiliert. Pakete für UCS finden sich auf der Installations-DVD oder unter http://apt.univention.de/. Diese Thesis ist also keine Anleitung, wie die Dienste von Univention zu verwenden sind. Insbesondere wird zwar oft die entwickelte WebGUI von UCS angesprochen; wie damit umzugehen ist, sollte aber im Handbuch zur Distribution nachgelesen werden unter http://univention.de/download_doku.html. Auch die Univention Configuration Registry wird nicht erwähnt oder benutzt, obwohl hier viele Einstellungen, die per Hand hinzugefügt wurden, auch über diese hätten erledigt werden können. Ebenso werden immer die direkten Pfade angegeben, in der sich die Konfigurationsdateien befinden, auch wenn Univention Templates angelegt hat und diese an anderer Stelle liegen. In jeder Konfigurationsdatei ist jedoch der Templatename vermerkt. Änderungen, die an einem laufenden Univention-System gemacht werden, sollten also auch immer ins Template geschrieben werden, bei anderen Linux-Distributionen ist dies nicht nötig. Neben den Dokumentationen, die Univention zur Verfügung stellt, wie das Handbuch, sei auch das Forum unter http://forum.univention.de/ sowie die

[3] die GNU General Public License siehe http://www.gnu.org/copyleft/gpl.html und zu Univentions Eigenentwicklungen siehe http://univention.de/oss.html

E-Mailadresse `feedback@univention.de` erwähnt, über die Fragen beantwortet werden.

2.3.2 Risiken beim Einsatz von Open Source

Der Einsatz von Open-Source-Software birgt auch einige Risiken. Eine der größten ist sicherlich, wenn eine Lösung, auf die gesetzt wird, nicht mehr existiert bzw. von der Community oder dem Unternehmen nicht geflegt und weiterentwickelt wird. Dem kann man nur in gewissem Maße begegnen, indem man auf Tools zurückgreift, die von einer breiten Community entwickelt werden; sollte doch einmal dieser Fall eintreten, bleibt der Vorteil von Open Source, dass die Entwicklung selbst in die Hand genommen oder ggf. ein anderes Unternehmen mit der Weiterentwicklung beauftragen werden kann.

Die meiste Open-Source-Software, die in dieser Arbeit genannt wird, ist jedoch lange erprobt und reif für den Unternehmenseinsatz; dies belegt auch der Open-Source-Katalog 2009 von Optaros[23].

2.3.3 Partitionierung und SSL-Zertifikate

Der Server erhielt eine 90 GB große Rootpartition, auf ihr sind alle wichtigen Systemdateien gespeichert; diese hätte man allerdings auch kleiner wählen können. Eine 1,9 TB große Homepartition, auf der alle User Ihre Daten ablegen werden, außerdem alle Sambashares werden hier die Daten haben, sowie eine 735 GB große /var-Partition, auf der alle Logfiles liegen, alle E-Mails und Daten für den Webserver. Als Dateisystem wird ext3 verwendet, da mit diesem Access Control Lists (ACLs) sowie benutzer- und gruppenspezifische Speicherplatzbeschränkungen, sogenannte Quotas, gesetzt werden können.

Die SSL-Zertifikate, welche unter `/etc/univention/ssl/media.hdm-stuttgart.de` abgelegt sind und für die die verschiedenen unter Kapitel 3 genannten Serverdienste benutzt werden, sind von CAcert[4] signiert worden. CAcert ist eine gemeinschaftsbetriebene, nicht-kommerzielle Zertifizierungsstelle, im Gegensatz zu kommerziellen Root-CAs werden die Zertifikate kostenlos ausgestellt. Leider ist das CAcert Rootzertifikat noch nicht in allen Browsern, Mailclients und Betriebssystemen verankert, daher muss das Zertifikat `http://www.cacert.org/certs/class3.crt` noch manuell bei den Clients hinzugefügt werden, da sonst eine Fehlermeldung angezeigt wird, die bei neueren Browsern auch nicht mehr so einfach weggeklickt werden kann (vgl. Abb. 2.2, es muss beim Firefox über mehrere Schritte eine Ausnahme hingefügt werden). Alternativ könnten die Zertifikate auch von der HdM Root CA unterschrieben werden, bei der das gleiche Problem auftauchen würde, außerdem ist der gemeinschaftliche Gedanke bei CACert wie

[4] `http://www.cacert.org`

Abbildung 2.2: Beispiel einer fehlgeschlagenen Verbindung, weil die RootCA nicht importiert wurde im Firefox

bei vielen Open-Source-Produkten faszinierend und es bleibt zu hoffen, dass das Root CA von CACert bald weit verbreitet ist und mit den Browsern mitkommt.

3 Serverdienste

Nachdem die Vorüberlegungen getroffen sind und es grob umrissen ist, für welche Anzahl von Clients der Server zur Verfügung stehen soll, widmet sich dieses Kapitel den eigentlichen Diensten, die angeboten werden. Nicht alle Dienste werden bis ins Detail erklärt, einige wie der Zeitserver (NTP) oder Secure Shell (SSH) werden einfach als gegeben hingenommen, andere wie z. B. das Common Unix Printing System (CUPS) werden ebenfalls nicht behandelt, da sie nicht aktiv eingesetzt werden. Auch der Domain Name System (DNS) Server Bind wird auf dem Server zwar ausgeführt, spielt aber kaum eine Rolle, da für Domains wie redaktionzukunft.de und convergentmedia.de die DNS-Server des HdM-Rechenzentrums zuständig sind. Bind ist so konfiguriert, dass er alle Anfragen an den DNS-Server des Rechenzentrums 141.62.1.5 weiterleitet.

3.1 OpenLDAP: Zentrale Authentisierung

Schon bei Beginn des Projektes (vgl. 1.2) stand fest, dass es einen Authentisierungsdienst geben soll, sprich einen zentralen Verzeichnisdienst. Die Benutzer und Diensteverwaltung für unterschiedliche Betriebssysteme auf der Grundlage einer zentralen Datenbasis schafft außerdem die Voraussetzung für die Realisierung von SSO[16](siehe Kapitel 6). Eine Vielzahl von Anwendungen können heute das Lightweight Directory Access Protocol (LDAP) verwenden.

Um einen solchen Verzeichnisdienst, auch LDAP-Server genannt, unter Unix oder Linux zu betreiben, wird oft die freie Implementierung des LDAP, OpenLDAP, verwendet. Andere Implementierungen sind z. B. Novells eDirectory oder Microsofts Active Directory. OpenLDAP ist dabei als einziges System in der Lage, auf einem 64bit-Betriebssystem bis zu 150 Millionen Einträge zu verwalten[35].

Das Univentionbetriebssystem setzt stark auf OpenLDAP und führt ein plattformübergreifendes Domänenkonzept ein. Innerhalb dieser Domäne ist ein Benutzer mit seinem im UCS-Managementsystem hinterlegten Benutzernamen und Passwort auf allen Systemen bekannt und kann für ihn freigeschaltete Dienste nutzen[10]. Da in diesem Konzept OpenLDAP die zentrale Rolle spielt und dies auch ein Grund ist, weshalb die

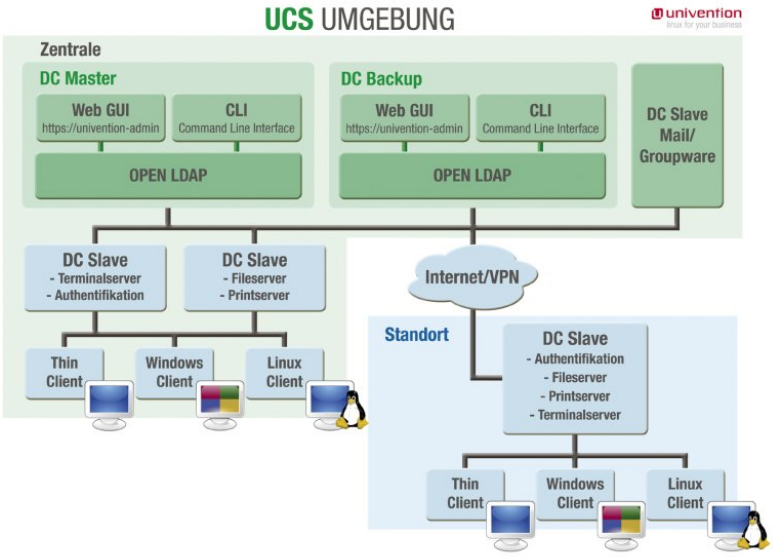


Abbildung 3.1: UCS-Domänen-Konzept[10]

Entscheidung für dieses Betriebssystem fiel (siehe 2.3) muss OpenLDAP nach der Installation nicht mehr weiter konfiguriert werden. Alle Einstellungen können über die WebGUI geschehen, erst bei der Installation der Groupware müssen Schemaerweiterungen vorgenommen werden. OpenLDAP ist auch schon für SSL/TLS vorbereitet. Das Konfigurationsdateien für OpenLDAP sind unter `/etc/ldap` zu finden.

Wer die Daten, die im LDAP gespeichert werden, genauer betrachten oder auch Änderungen daran vornehmen will und dazu nicht das Kommandozeilentool ldapsearch benutzen möchte, dem sei der JXplorer[1] empfohlen; dieses in JAVA geschriebene und daher für alle Betriebssysteme zur Verfügung stehende Programm ist leicht zu bedienen und zeigt schön die LDAP Strukturen. Für ein Programm, das sich auf einem Webserver installieren und von überall bedienen lässt, sei der phpLDAPadmin[2] empfohlen.

[1] http://www.jxplorer.org/
[2] http://phpldapadmin.sourceforge.net/

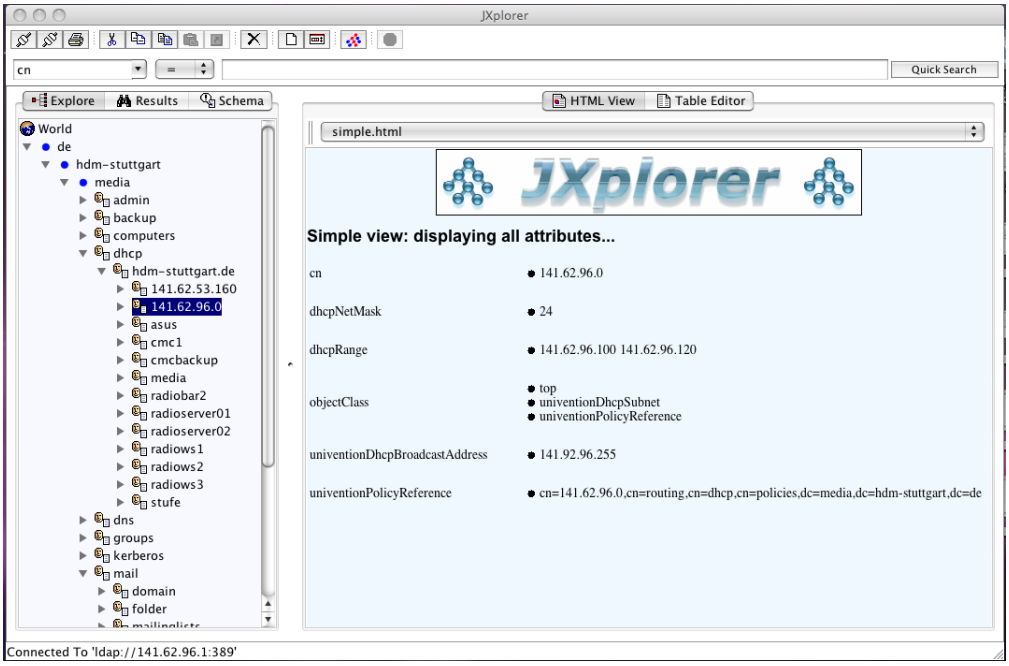


Abbildung 3.2: LDAP-Browser: JXplorer

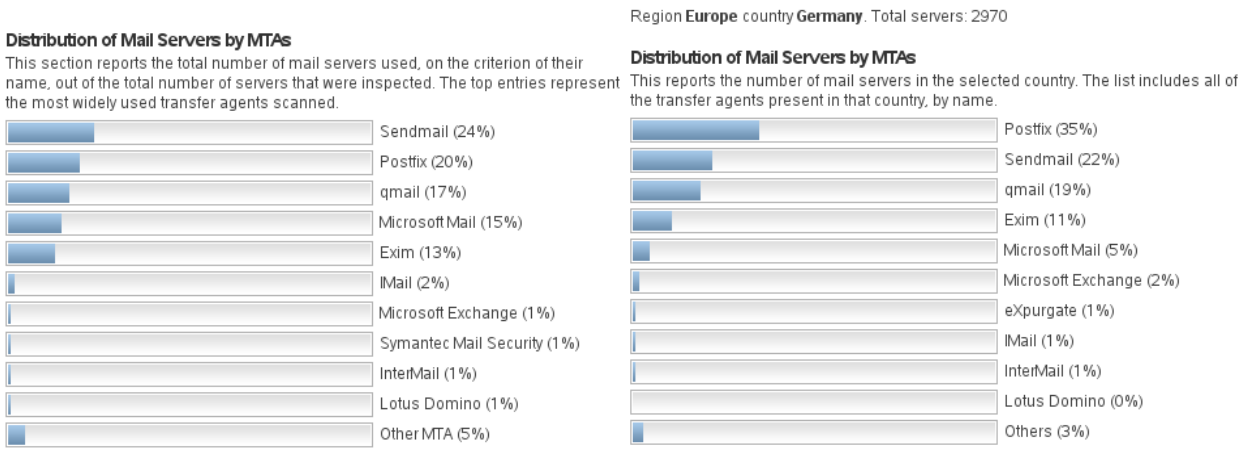
3.2 Mailserver: Rückgrat jeder elektronischen Kommunikation

Wenn von einem Mailserver gesprochen wird, sind meist zwei unterschiedliche Dienste gemeint. Zum einen gibt es den Mail Transfer Agent (MTA), also den SMTP-Mailserver, der E-Mails annimmt, diese weiterleitet oder verschickt, zum anderen gibt es einen Dienst mit dem die User Ihre E-Mails abholen können, Mail Delivery Agent (MDA), dies geschieht meist über POP3, heute sogar verstärkt über IMAP.

3.2.1 MTA Postfix

Die Entscheidungen für einen MTA fiel auf Postfix[37], welcher seit 1998 von Wietse Zweitze Venema bei IBM entwickelt wird. Postfix ist ein modular aufgebautes, schnelles, sicheres und leicht zu administrierendes System, außerdem bietet Postfix eine Aufrufkompatibilität zu dem ehemaligen Standardmailserver von unixoiden Betriebssystemen, Sendmail, so dass alle Tools, die auf Sendmail zugreifen können, auch mit Postfix umgehen können.

Es gibt auch andere weit verbreitete Open-Source-MTAs für Linux wie z. B. Exim, welches der Standardmailserver unter Debian ist, oder das eben angesprochene Sendmail; ebenso beliebt ist qmail. Postfix war jedoch die logische Entscheidung, da dieser



(a) Mailserver weltweit (b) Mailserver in Deutschland

Abbildung 3.3: Statistik über eingesetzte Mailserver[19]

aktiv weiterentwickelt wird, modular ist und sehr viele Features bietet, auch ist er der wahrscheinlich häufigst eingesetzte Mailserver in Deutschland (vgl. Abb. 3.3). Solche Statistiken sind zwar mit Vorsicht zu genießen, denn es gibt sicher wesentlich mehr Mailserver in Deutschland als die hier getesteten knapp 3000, jedoch entspricht diese Statistik auch der Wahrnehmung des Verfassers dieser Arbeit. Da Postfix der Standardmailserver von SUSE Linux ist, kamen viele heutige Systemadministratoren schon mit diesem Mailserver in Kontakt, außerdem existiert eine vitale Postfix-Community und einige sehr gute Postfix-Bücher stammen von deutschen Autoren.

Einen MTA zu betreiben ist keine leichte Aufgabe, daher wurde bei der Konfiguration auch viel Arbeit aufgewendet, um diesen möglichst sicher zu betreiben. Ein falsch konfiguriert Mailserver kann gefährlich sein, denn im Gegensatz zu einen schlecht konfigurierten Webserver, der im schlimmsten Fall einfach nicht funktioniert, wird der Mailserver auch im Internet aktiv, verbindet sich mit anderen Mailservern und kann ein schlechtes Licht auf das Unternehmen oder die Organisation werfen und ggf. von Spammern missbraucht werden.

Postfix wird über zwei zentrale Konfigurationsdateien gesteuert, das sind zum einen die main.cf und zum anderen die master.cf. Diese und andere wichtige Dateien finden sich unter `/etc/postfix`. Postfix nimmt E-Mails für mehrere Domains entgegen für redaktionzukunft.de, convergentmedia.de sowie für horads.de, E-Mails für die Domain hdm-stuttgart.de werden relayed, d. h. diese werden angenommen und an den Mailserver der HdM übergeben. Die Userdaten und angelegten E-Mailadressen werden aus dem

eben beschrieben LDAP gezogen. Über die Webadministrationsoberfläche für den UCS können diese bearbeitet werden. Ist eine E-Mail nicht an eine dieser Domains gerichtet, nimmt Postfix diese nicht an (also er ist kein Open Relay), jedoch sollen die User des Servers auch E-Mails an die Außenwelt schicken dürfen, hierfür müssen sie sich jedoch authentisieren, die Userdaten sind wieder im LDAP gespeichert, die Authentisierung geschieht über die Cyrus SASL Library.

3.2.2 IMAP/POP3-Server Cyrus

Bei dem MDA fiel die Entscheidung zu Gunsten von Cyrus[29] aus. Cyrus wird an der Carnegie Mellon University entwickelt, ursprünglich für das Campus-Mail-System der Universität. Eine der großen Stärken von Cyrus ist die Cyrus SASL Library, eine Implementierung von Simple Authentication and Security Layer (SASL), um mehrere Authentifizierungsmethoden zur Verfügung zu stellen. Außerdem kann Cyrus mit Sieve-Skripten[3] umgehen, dabei werden E-Mails direkt auf dem IMAP-Server gefiltert und nicht erst wie früher auf dem Mailclient; so können E-Mails direkt in verschiedene Ordner geschoben werden oder gelöscht werden, sogar Abwesenheitsmitteilungen sind möglich. Cyrus ist der Standard-MDA auf UCS und Postfix/Cyrus ist eine vielfach bewährte Kombination, andere POP3/IMAP-Server sind z. B. Dovecot, maildrop oder Courier, wobei es von Courier mittlerweile auch einen MTA gibt, also einen kompletten Mailserver.

Der MTA Postfix gibt die E-Mail über das Local Mail Transfer Protocol (LMTP) über einen Unix Socket an Cyrus weiter. Dieser sortiert die E-Mails in Maildirs ein, die sich unterhalb von `/var/spool/cyrus/mail` befinden. Die Konfigurationsdateien von Cyrus liegen unterhalb von `/etc/imapd/`.

Die User können sich per POP3 oder IMAP zum Cyrus-Mailserver verbinden und ihre E-Mails dort abholen, besser ist jedoch, und dies wird alles Nutzern empfohlen, eine TLS- oder SSL-Verbindung zu benutzen, dabei wird der Verkehr zwischen Mailclient und Mailserver verschlüsselt. Dazu werden neben den Standardports 143 für IMAP und IMAP über TLS sowie 110 für POP3 und POP3 über TLS die Ports 993 und 995 bereitgestellt für IMAPs und POP3s, also Verbindungen über SSL. Die User werden wie auch bei Postfix über SASL authentifiziert. Am IMAP-Server wurden die wenigsten Änderungen vorgenommen, er wird „Out-of-the-box“ so benutzt, wie er von Univention für die Distribution gebaut wurde.

[3] Sieve ist in RFC 5228 beschrieben; mehr siehe: http://de.wikipedia.org/wiki/Sieve

Abbildung 3.4: Angenommene und abgelehnte E-Mails innerhalb eines Monats

3.2.3 Antispammaßnahmen

In einer Zeit, in der die meisten E-Mails, die auf unseren Mailserver einprasseln, Spam sind, reicht es nicht, diesen einfach in einer Standardkonfiguration zu fahren. Viele kleine Einstellungen sind nötig, damit Postfix im besten Fall nur E-Mails durchlässt, die auch wirklich gewollt sind. Wie Abbildung 3.4 zeigt, werden knapp 90 % der E-Mails schon beim Einlieferungsversuch abgelehnt.

Postfix bietet dafür eine Reihe von Restrictions; an dieser Stelle wird nur auf eine Art näher eingegangen, sonst würde das den Rahmen dieser Thesis sprengen, außerdem ist der Autor der Thesis der Meinung, dass nur an dieser Stelle die wirklich wichtigen Dinge gefiltert werden können. Für eine genaue Erklärung der Restrictions in Postfix, welche es außerdem gibt, wie eigene entwickelt werden können und vieles mehr, siehe [13, 14].

3.2.3.1 Restrictions

Für die Annahme von E-Mails ist das Modul smtpd von Postfix zuständig. Daher werden diese Restrictions auch mit smtpd_*_restrictions gekennzeichnet. Hier wird speziell auf Restrictions eingegangen, die nach dem RCPT TO: prüfen, also nach dem Empfänger, diese werden daher auch smtpd_recipient_restrictions genannt.

Folgendes Set an Einstellungen wird verwendet:

Listing 3.1: Einstellungen in der main.cf

```
smtpd_recipient_restrictions =
reject_non_fqdn_sender,
reject_non_fqdn_recipient,
reject_unknown_sender_domain,
reject_unknown_recipient_domain,
permit_mynetworks,
permit_sasl_authenticated,
reject_unauth_pipelining,
reject_non_fqdn_hostname,
reject_invalid_hostname,
reject_unauth_destination,
reject_multi_recipient_bounce,
reject_rbl_client ix.dnsbl.manitu.net,
reject_rbl_client dul.dnsbl.sorbs.net,
reject_rbl_client bl.spamcop.net,
check_policy_service inet:127.0.0.1:12525,
check_policy_service inet:127.0.0.1:10023,
reject_unverified_recipient,
permit
```

Diese hier aufgeführten sind keinesfalls der Weisheit letzter Schluss. Es gibt unzählige Möglichkeiten, Postfix zu tunen, um evtl. noch mehr unerwünschte Post herauszufiltern, es sind nur eine Reihe von Anweisungen, die sich bewährt haben. Die Anweisungen stehen natürlich aus gutem Grund in dieser Reihenfolge, so stehen oben einfache Tests, die wenig Ressourcen brauchen, weiter unten kommen dann Tests die z. B. DNS-Anfragen generieren und damit wesentlich „teurer“ sind. Manche Restrictions machen auch an anderen Stellen keinen Sinn.

Die Bedeutung der Restrictions von oben nach unten:

- reject_non_fqdn_recipient, reject_non_fqdn_sender – die Sender- und Empfangsadresse muss als Fully Qualified Domain Name (FQDN) angegeben werden, d. h. eine E-Mail kann nicht einfach an webmaster geschickt werden, sondern muss an webmaster@convergentmedia.de gehen

- reject_unknown_sender_domain, reject_unknown_recipient_domain – E-Mails

von unbekannten, nicht vergebenen Domains werden nicht angenommen

- permit_mynetworks – weist Postfix an, E-Mails aus seinem eigenen Netz anzunehmen, falls diese vorher nicht schon abgelehnt wurde, die E-Mail wird jetzt angenommen, Tests danach werden nicht ausgeführt
- permit_sasl_authenticated – E-Mails von richtig authentisierten Benutzern von außen sollen durchgelassen werden, auch hier wird jetzt die E-Mail angenommen
- reject_unauth_pipelining – in SMTP können mehrere Anfragen gebündelt werden, manche Spammer machen dies sofort, ohne dass der Mailserver dies erlaubt hätte, Postfix unterbindet dies
- reject_non_fqdn_hostname – Clients von richtigen Mailservern senden im HELO einen FQDN mit z. B. mail.hdm-stuttgart.de; sollte nur mail oder pc123218 gesendet werden, lehnt das Postfix ab
- reject_invalid_hostname – ein HELO-Hostname muss nicht nur ein FQDN sein, sondern darf auch bestimmte Zeichen nicht enthalten; dies wird hier getestet
- reject_unauth_destination – soll eine E-Mail an eine Domain geschickt werden, für die Postfix nicht zuständig ist, wird diese E-Mail abgelehnt
- reject_multi_recipient_bounce – mit diesem Parameter werden sogenannte Bounces, also E-Mails, die nicht zugestellt werden konnten, abgelehnt, wenn diese mehr als einen Empfänger haben
- reject_rbl_client – E-Mails, die auf einer der DNSBL-Blacklists (DNS-based Backhole List) gelandet sind, werden abgewiesen

Ob man Blacklists verwendet, sollte jeder Postmaster selber entscheiden. Es gibt sowohl Vorteile als auch Nachteile. Auf Blacklists können natürlich auch Clients landen, die nichts „böses“ getan haben, das kann z. B. alle Kunden eines kleineren Providers treffen oder Ähnliches. In der Regel sollte es aber einfach möglich sein, wieder von einer Blacklist gelöscht zu werden, wenn das Problem gelöst wurde. Neben der Möglichkeit, die E-Mail sofort abzulehnen, gibt es auch mehrstufige Prüfungen, die eine E-Mail erst ablehnen, wenn ein bestimmter Grenzwert erreicht ist, z. B. auch wenn sie auf mehreren Blacklists gelandet ist und weitere Protokollverstöße. Siehe dazu auch Policyd-weight.

Die `check_policy_service` werden in den folgenden Abschnitten näher erläutert und `reject_unverified_recipient` überprüft, ob ein Empfänger auf dem Server (als z. B.

im LDAP) eingetragen ist bzw. bei einer E-Mailadresse, die relayed werden soll, ob diese E-Mailadresse auf dem Relay existiert. Der letzte Parameter `permit` sagt nur, dass wenn alle Tests negativ ausgefallen sind und die E-Mail nicht abgelehnt wurde, sie jetzt endgültig zugelassen wird.

3.2.3.2 Greylisting

Postfix bietet auch an, die Entscheidung, ob eine E-Mail angenommen wird oder nicht, an ein anderes Programm abzugeben, sogenannte Policy Delegation; dies kann über einen Unix-Socket oder eine TCP-Verbindung geschehen. Alle bekannten Merkmale der E-Mail werden an den Policy Daemon übergeben und die Entscheidung (z. B. OK, REJECT, DISCARD etc) wird abgewartet.

Eine Art dieser Policy Delegation ist Greylisting. Es wurde im Jahr 2004 entwickelt und macht es sich zu Nutze, wie Spammer Ihre E-Mails versenden, nähmlich möglichst schnell und viele auf einmal; schlägt ein Versuch fehl, ist das egal, denn einer der vielen Millionen Mails wird schon ankommen. Greylisting geht nun wie folgt vor:

- Noch bevor die E-Mail komplett übertragen wird, also vor dem DATA-Kommando des SMTP-Dialogs, schaut sich der Mailserver ein Triple aus der IP-Adresse, der Absenderadresse (MAIL FROM) und der Empfängeradresse (RCPT TO) an.
- Dieses Triple wird zusammen mit einem Zeitstempel in einer Datenbank gespeichert, ist das Triple neu, wird die E-Mail mit einem temporären 4xx-Fehler ablehnt
- Ein echter Mailserver als Client wird nach einer kurzen Zeit erneut versuchen, die E-Mail zuzustellen
- Diesmal ist das Tipple schon bekannt und die E-Mail wird akzeptiert, falls nicht noch andere Filterregeln wie die oben genannten Restrictions dagegensprechen.

Mit diesem Verfahren ist also sichergestellt, dass der einliefernde Client (Mailserver) sich um seine verschickten Mails kümmert, denn temporär kann ein Server immer mal ein Problem haben, z. B. einen Konfigurationsfehler, eine volle Festplatte, zuviel Last oder Ähnliches. Der andere Mailserver muss dann dafür Sorge tragen, dass die E-Mail zu einem späteren Zeitpunkt erneut zugestellt wird . Spammer versuchen das in der Regel nicht, auch wenn der Aufwand heute nicht mehr so groß wäre. Da die Rechner, die in einem Botnetz sind, durch DSL fast 24 Stunden am Tag im Netz sind, gehen die meisten Spammer immer noch nach dem Muster vor: soviel rausschicken wie möglich, und das was durchkommt, kommt durch. Ein Problem löst Greylisting natürlich nicht,

wenn die E-Mails über einen „echten“ Mailserver eingeliefert werden, z. B. über den gekaperten Account bei einem Mailprovider, über Webformulare oder über einen schlecht konfigurierten Mailserver.

Auf dem Server läuft die Greylisting-Implementation von David Schweikert[4] namens postgrey. Diese ist einfach zu installieren:

```
wget http://postgrey.schweikert.ch/pub/postgrey-1.32.tar.gz
tar -xvzf postgrey-1.32.tar.gz
cd postgrey-1.32/
cp postgrey /usr/local/sbin/
cp contrib/postgreyreport /usr/local/sbin/
cp postgrey_whitelist_* /etc/postfix/
useradd -r -s /bin/false postgrey
mkdir /var/spool/postfix/postgrey
chown postgrey /var/spool/postfix/postgrey/
```

Danach kann postgrey gestartet werden; benutzt wird hier die Variante über TCP statt über einen UNIX-Socket, da dies meistens unkomplizierter ist.

```
postgrey -d --inet localhost:10023
```

Gegebenenfalls müssen vorher noch einige Perl-Module installiert werden, dies kann entweder über das Paketmanagement der Distribution geschehen, also z. B. apt-get wenn die Pakete zur Verfügung stehen, oder mittels CPAN[5]. Auf der Kommandozeile kann `cpan` aufgerufen werden und mittels “install Modulname” können die nötigen Module kompiliert werden. Benötigt werden Net::Server, IO::Multiplex und BerkeleyDB.

Zu guter Letzt muss `check_policy_service inet:127.0.0.1:10023` noch in die main.cf unter `smtpd_recipient_restrictions` eingetragen werden. Nach einem `postfix reload` ist Greylisting aktiv, außerdem sollte noch ein Startscript angelegt werden, damit Greylisting auch nach einem Server reboot wieder mitgestartet wird.

3.2.3.3 Policyd-weight

Auch ein Policy-Daemon ist policyd-weight von Robert Felber[6]. Er führt eine Reihe von Tests auf den Angaben des Clients (bzw. einliefernden Mailserver) durch, z. B. ob der HELO plausibel ist, ob die Client-IP auf Blacklists steht, ob die DNS-Einträge stimmen

[4] http://postgrey.schweikert.ch/
[5] Comprehensive Perl Archive Network, ist ein weltweit gespiegeltes Online-Repository für Perl-Module, -Anwendungen und Dokumentationen
[6] http://policyd-weight.org/

und vieles mehr. Jedem dieser Tests werden bestimmte Werte zugewiesen, z. B. wenn der Client nicht auf einer Blacklist steht, gibt es Minuspunkte, sollte er aber beim HELO patzen, gibt es Pluspunkte. Aus allen Tests wird ein Gesamt-Score errechnet und danach wird entschieden, ob die E-Mail abgelehnt wird oder nicht.

Auch policyd-weigt lässt sich einfach installieren. Die einzelnen Schritte sind in der Dokumentation auf den policy-weight.org-Seiten nachzulesen. Dabei ist zu beachten, dass auch dieser Daemon bestimmte Perlmodule braucht, wie z. B. Net::DNS aus CPAN. Per Default lauscht policyd-weight auf dem Port 12525, daher steht in der main.cf in den `smtpd_recipient_restrictions` siehe Listing 3.1 folgendes: `check_policy_service inet:127.0.0.1:12525`; und dies am besten vor greylisting, denn wenn der Client schon grundlegende Dinge falsch macht oder er auf Blacklists steht – wozu soll die E-Mail dann überhaupt angenommen geschweige denn das Triple gespeichert werden, um ihn später wiederzuerkennen?

3.2.3.4 Viren und andere Krankheiten

Nicht nur Spam ist ein großes Thema, sondern auch Viren, Würmer, Trojaner und weitere Schadprogramme. Die schon vorgestellten Maßnahmen liefern einen guten Schutz vor Viren, denn indem so wenige E-Mails wie möglich angenommen werden, also die meisten schon aussortiert werden, bevor diese überhaupt von Mailserver angenommen und weiterverarbeitet werden, wird eine wichtige Maßnahme ergriffen. Knapp 90 % lassen sich auf diese Weise bekämpfen, was geschieht aber mit dem Rest? Hier setzt AMaViS (A Mail Virus Scanner) an. AMaViS kann mehrere Virenscanner einbinden, darunter kommerzielle wie von Kaspersky oder Avira oder den freien ClamAV[7], außerdem kann AMaViS den mächtigen Spamfilter SpamAssassin (SA) einbinden. Es gibt mehrere AMaViS-Ableger, heute wird meisten der amavis-new[8] eingesetzt, da er sich am besten entwickelt hat.

AMaViS wird hier nicht ausführlich mit Installationsanleitung behandelt, da der Autor der Arbeit der Meinung ist, dass soviel wie möglich schon vorher gefiltert werden muss, außerdem kostet ein Virenfilter ziemlich viele Ressourcen, darüber hinaus setzt AMaViS in diesem Beispiel erst an, nachdem die E-Mail komplett übertragen wurde und damit unser Mailserver dafür zuständig ist. Hieraus ergeben sich Problematiken, was mit einer E-Mail geschieht, die im Nachhinein als Spam oder als virenverseucht abgelehnt wird (Backscatter) sowie rechtliche Probleme (vgl. Kapitel 21.3 in [13]).

Zur Funktionsweise: AMaViS öffnet einen eigenen kleinen SMTP-Server, meistens auf

[7] siehe http://www.clamav.net/
[8] siehe http://www.ijs.si/software/amavisd/

Port 10024. Eine eingehende E-Mail wird von Postfix komplett an diesen übergeben, d. h. es wird nicht nur eine Entscheidung abgewartet wie bei einem Policy-Daemon. Amavisnew filtert die E-Mail und kann diese, falls sie in Ordnung ist, an Postfix zurück geben oder in eine Quarantäne verschieben. AMaViS kann die E-Mail nicht über Port 25 an Postfix zurück geben, da dadurch eine Endlosschleife entstehen würde, sondern in der master.cf von Postfix muss ein eigener Port definiert werden, der den content_filter nicht enthält.

3.3 Samba: Windows-Dienste auf Linux

„Samba ist eine freie Software-Suite, die das Server-Message-Block-Protokoll (SMB) für Unix-Systeme verfügbar macht“[38]. Samba wird von einem 25- bis 30-köpfigen Team entwickelt. Ursprünglich wurde es von Andrew Tridgell programmiert.

Mit Samba ist es möglich typische Funktionen wie Datei- und Druckdienste für Windows-Clients anzubieten. In TCP/IP-Netzen läuft SMB ursprünglich über den NetBIOS-Port 139 und die Namensauflösung erfolgte mittels Windows Internet Naming Service (WINS). Heute wird SMB auch als Dienst microsoft-ds bezeichnet und über den Port TCP/UDP 445 angesprochen, auch der Samba-Server bietet beide Möglichkeiten an. Samba ist außerhalb der Windows-Welt das Mittel der Wahl, wenn es um das Anbieten von SMB geht. Samba gilt als stabil und leistungsfähig und wird von vielen Unternehmen eingesetzt, hat eine große Community und von verschiedenen Firmen gibt es kommerziellen Support. Mit der SerNet - Service Network GmbH ist außerdem eine der wichtigsten Firmen, die an der Entwicklung von Samba beteiligt ist, in Deutschland beheimatet, ebenso findet in Göttingen regelmäßig die SambaXP-Konferenz statt, auf der sich Entwickler und Anwender treffen. [6]

3.3.1 Versionen

Zurzeit gibt es zwei Samba-Versionen, Samba 3 und Samba 4. Samba 4 ist eine noch nicht fertige komplette Neuentwicklung, die einen integrierten LDAP-Server bietet, dies ist allerdings kein OpenLDAP, sondern eine Eigenentwicklung; ob oder wann es auch möglich ist, OpenLDAP statt den integrierten LDAP zu nutzen, ist noch nicht bekannt. Der integrierte LDAP-Server ist nötig, um eine volle Active-Directory- (AD) Umgebung zu schaffen. Samba 3 ist die stabile Version, die zurzeit nur in der Lage ist, eine Windows-NT4-Domain nachzubilden. Samba 3 und 4 werden zur Zeit parallel entwickelt, Entwicklungen und neue Technologien werden teilweise von Samba 4 in Samba 3 zurück portiert.

Anfang 2009 soll jedoch Samba 4 erscheinen, die jahrelange parallele Entwicklung von Samba soll langsam beendet werden. Bis sich das neue Samba durchsetzt, wird sicher noch einige Zeit vergehen.

3.3.2 Domain Controller

Samba mit einem LDAP als Primary Domain Controller (PDC) aufzusetzen ist keine leichte Aufgabe. Diese Aufgabe wurde daher zum Glück auch von Univention schon übernommen. So wird das Samba out of the Box benutzbar, selbst schwierigste Aufgaben wie die add-machine-Skipte, d. h. ein Rechner, der eine Windows-Domain joined, bekommt ein Maschinenkonto, welches in den LDAP übernommen werden muss, sind vorkonfiguriert. Ebenso die Möglichkeit, dass User ihr Kennwort über Windows ändern können und dies nicht zwingend direkt im LDAP geschehen muss. Neue Samba Shares, also Verzeichnisse, die über SMB zur Verfügung stehen sollen, können über die WebGUI eingerichtet werden.

Als PDC ist Samba für die komplette Windows-Domain zuständig, für alle Windows-Clients verhält sich Samba wie ein Windows NT4 Domain Controller, nicht wie ein AD Domain Controller. Microsofts Active Directory (AD) ist mit Windows 2000 eingeführt worden und ist eine Kombination aus LDAP, Kerberos, DNS und SMB/CIFS. Da Samba eine LDAP-Anbindung hat, müsste eigentlich gesagt werden, der Samba-PDC ist irgendetwas zwischen einem NT4 PDC und einem AD PDC. Samba wird über die Konfigurationsdateien unterhalb von `/etc/samba` gesteuert.

Die Profile aller Windows-User werden auf dem Server abgelegt, d. h. Profileinstellungen wie Hintergründe, Eigene Dateien und Dokumente, der komplette Desktop; ebenso legen viele installierte Programme wie OpenOffice.org und Adobe Ihre Einstellungen im Windows-Profil ab. Ein User, der sich an verschiedenen Clients anmeldet, erhält damit immer die gleichen Einstellungen. Da in der CMC-Umgebung Windows-Vista- und Windows-XP-Clients gemischt eingesetzt werden, müssen allerdings zwei Profile gepflegt werden; Windows Vista und XP legen die Profile in unterschiedlichen Arten

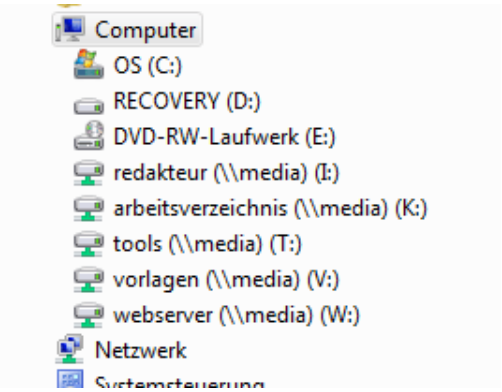


Abbildung 3.5: Eingebundene Samba Shares unter Windows Vista (User redakteur)

Befehl	Aktion
echo Setting Current Time...	Schreibt „“Setting Current Time“ auf die Kommandozeile
net time \\media /set /yes	Überschreibt die Systemzeit des Windows-Clients mit der Zeit des Servers media
net use t: \\media\tools	weist Windows an, das Verzeichnis tools auf dem Rechner media als Laufwerk t einzubinden
net use r: \\141.62.53.183\Daten	weist Windows an, die Windows-Freigabe-Daten auf dem Rechner 141.62.53.183 als Laufwerk r einzubinden
net use k: /DELETE	löst die Netzlaufwerkverbindung k

Tabelle 3.1: Beispiele für Befehle bei der Windows-Anmeldung

ab, daher sollten eigene Dateien bzw. wichtige Dateien nicht unter „Eigene Dateien“ abgelegt werden sondern im Homeverzeichnis, unter Linux ist das `/home/username`, als Samba Share wird das Verzeichnis unter Windows als Netzlaufwerk automatisch eingebunden, als welcher Laufwerksbuchstabe das geschehen soll, kann eingestellt werden. Im CMC ist das das Laufwerk I: (siehe Abb. 3.5). Da alle Windows-Clients sich in der Samba-Domain befinden, können beim Anmelden auch Batch-Skripte übergeben werden, die bei der Anmeldung am Client ausgeführt werden, damit ist es z. B. möglich, weitere Laufwerke zu mappen (einzubinden), diese müssen nicht einmal direkt auf dem Server liegen, sondern können auch andere Windows-Freigaben sein, auch können die Zeit gesetzt oder sogar Programme im Hintergrund installiert werden (siehe 8.4). Tabelle 3.1 zeigt einige Befehle, die ausgeführt werden können. Theoretisch ist es jedoch möglich, jede Art von Programmen auszuführen, die es unter Windows gibt. Abgelegt werden diese Batch-Skripte unter `/var/lib/samba/netlogon`, jede Benutzergruppe erhält dabei ein eigenes Skript, da diese auf unterschiedliche Ordner zugreifen müssen.

Auf den Samba Shares können zum Teil auch Dateien liegen, die wichtig sind, daher sollten die Rechte entsprechend gesetzt werden, welcher Benutzer oder welche Gruppe zugreifen darf und mit welchen Rechten Verzeichnisse oder Dateien angelegt werden kann. Dies kann über die WebGUI des UCS geschehen, jedoch ist es manchmal wünschenswert, dass von vornherein nicht alle Clients zum Samba eine Verbindung aufbauen dürfen. Dazu können in die Global-Sektion der smb.conf oder auf einem UCS in die local.conf, welche in der smb.conf eingebunden ist, Hosts explizit erlaubt bzw. verboten werden. Im folgenden Beispiel werden alle Verbindungen der in Abb. 2.1 zu sehenden Netze erlaubt, dazu die Verbindung vom Host 141.62.52.65. Alle anderen Verbindungen werden abgelehnt, sobald der Client sein erstes Paket sendet. Das könnte ebenfalls

mit Firewallregeln auf die Ports 137,138,139 und 445 erledigt werden (vgl. [25] Seite 247–251).

```
[global]
hosts allow = 127.0.0.1 141.62.96.0/24 141.62.53.160/27
              193.196.176.0/23 141.62.52.65/32
hosts deny = 0.0.0.0/0
```

In der local.conf ist ebenfalls die Zeile

```
[homes] hide files = /?esktop.ini/ntuser.ini/NTUSER.*/?humbs.db/
```

eingetragen, damit die verschiedenen ini-Dateien, in denen Windows Einstellungsinformationen hineinschreibt, nicht angezeigt werden.

Um Samba mittels LDAP anzubinden, sollten schon Erfahrungen mit Samba vorhanden sein, es gibt zahlreiche HowTos[9] zu dem Thema im Internet, allerdings ist es empfehlenswert, einen Kurs[10] zu besuchen, um die Tiefen von Samba richtig zu verstehen. Selbst bei einer Out-of-the-Box-Lösung, wie von Univention angeboten, ist es in größeren Umgebungen angebracht, sich intensiver damit zu beschäftigen. Neben den Kursen gibt es auch Bücher, z. B. das Samba 3 für Unix-/Linux-Administratoren von Volker Lendecke aus dem dpunkt-Verlag, das Samba 3 – Das offizielle Handbuch, welches leider kaum auf LDAP eingeht, dafür viele der Grundbegriffe klärt (siehe [25]), auch das LDAP Buch, LDAP verstehen – OpenLDAP einsetzen [16] geht auf einen PDC mit LDAP und SSO kurz ein.

3.4 Nagios: Netzwerk-Monitoring

Je größere eine Umgebung wird, umso schwieriger ist es für den Administrator, alles im Auge zu behalten. Um auf allen Rechnern die Festplattenkapazität zu wissen, zu ahnen, wann der Netzwerkdrucker keine Tinte mehr hat, oder nur das Ausfallen eines wichtigsten Dienstes mitzubekommen, aber auch um gleich erkennen zu können, wo das Problem liegt, ist ein Switch ausgefallen oder die ganze Internetverbindung der HdM, für solche Fälle ist eine Monitoring-Software unabdingbar.

Nagios ist eine solche Software zur Überwachung komplexer IT-Infrastrukturen. Nagios bietet dazu eine Vielzahl an Plug-Ins und Modulen zur Überwachung von Netzwerken, Hosts und speziell Diensten sowie einer WebGUI zum Anzeigen der gesammelten

[9] siehe z. B. http://download.gna.org/smbldap-tools/docs/samba-ldap-howto

[10] z. B. von Sernet: http://sernet.de/Samba/Training.shtml oder der heinlein akademie: http://www.heinlein-support.de/web/akademie/kurse/samba/

Daten an. Nagios steht in der Version 2.6-2 auch für UCS zur Verfügung; Univention macht es auch hier möglich, dass viele Einstellungen über die WebGUI zu erreichen sind. Für alle im LDAP eingetragenen Rechner kann die Nagios-Überwachung schnell eingeschaltet werden und vorkonfigurierte Checks wie PING eingesetzt werden. Da Nagios normalerweise ohne eine Konfigurationsweboberfläche installiert wird, ist dies eine willkommene Erleichterung. Trotzdem bleibt das System komplett flexibel, unterhalb von `/etc/nagios2` können jeder Zeit eigene Konfigurationen hinzugefügt werden, denn die Integration deckt zwar Standardanwendungszwecke ab, aber sobald größere, verteilte Netze überwacht werden sollen, müssen eigene Kommandos und Checks definiert werden, da die vorkonfigurierten Checks von Univention meist nur lokal funktionieren oder Tests sind, die das Erreichen eines Ports, z. B. Port 22, für SSH überprüfen. Nagios ist aber ebenfalls in der Lage, Tests auf entfernten Rechnern durchzuführen, die lokale Werte wie CPU-Auslastung, Speicherplatz oder Anzahl der eingeloggten User beinhalten.

3.4.1 Nagios-Plugins

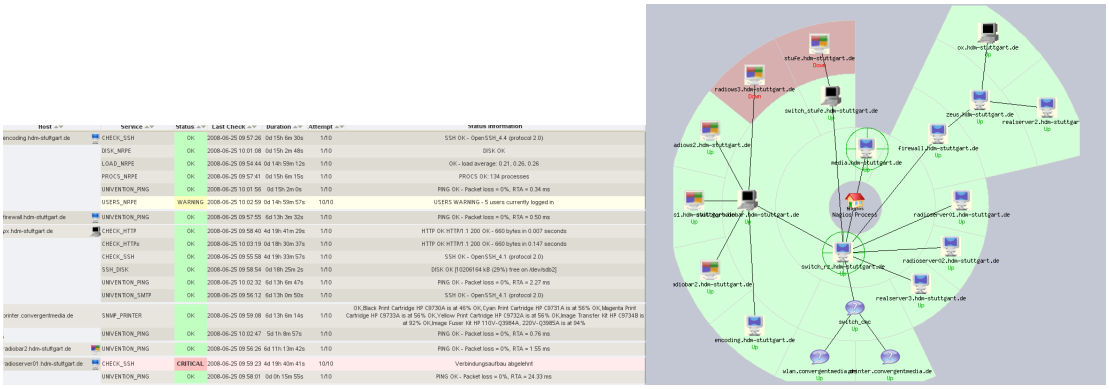
Um Informationen über entfernte Systeme zu bekommen, können verschiedene Methoden angewendet werden. Der einfachste ist ein Plug-In direkt aufzurufen, um zu testen, ob ein SSH-Server, HTTP-Server noch läuft. Dafür stellt Nagios verschiedene Plug-Ins zur Verfügung, die auch testen können, ob hinter dem Port auch wirklich ein HTTP-Server lauscht; es gibt auch generische Plug-Ins, die nur testen, ob ein bestimmter TCP-Port erreichbar ist. All diese Plug-Ins stellt das Paket nagios-plugins bereit, welche auf vielen Distributionen zu finden ist oder über `http://nagios.org` bzw. `http://nagiosplugins.org/` zu bekommen ist. Die zweite Methode ist, dies über SSH zu erledigen. Dazu müssen die nagios-plugins auf dem Zielrechner installiert werden. Auf dem Nagios-Server wird ein SSH-Schlüssel ohne Passwort generiert, damit der Nagios-Server eine SSH-Verbindung zum Client aufbauen kann. Dieser Schlüssel wird dann auf den zu überwachenden Rechner übertragen, sowie Gruppen und User für nagios müssen erstellt werden. Nun können Nagios-Kommandos definiert werden, die über SSH die Plug-Ins auf dem entfernten Rechner ausführen. Der Vorteil dieser Methode ist, das SSH durch viele Firewalls durchgelassen wird und die Verbindung verschlüsselt ist.

Eine weitere Methode, Informationen auf anderen Rechnern zu sammeln, ist, den Nagios-Remote-Plug-In-Executor (NRPE) einzusetzen. Dazu werden NRPE und die Nagios-Plug-Ins auf dem Zielhost installiert. Hierbei sollte darauf geachtet werden, dass die NRPE-Verbindung auch über SSL/TLS gesichert wird. NRPE kann so konfiguriert werden, dass es als Inet-Deamon läuft und so automatisch beim Systemneustart mitgestartet wird. Der Vorteil dieser Lösung liegt darin, dass nur explizite Plug-Ins aufgeführt

werden dürfen und keine komplette SSH-Session aufgemacht werden muss.

Die vierte Möglichkeit ist es, Abfragen über SNMP durchzuführen. Dazu muss auf dem Zielhost ein SNMP-Deamon laufen, z. B. der weit verbreitete NET-SNMPD. Nagios kann diesen dann nutzen, um lokale Ressourcen wie Prozesse, Festplattenkapazität oder Interface-Auslastung abzufragen. Auch hier gibt es wieder ein generisches Standardplugin check_snmp oder spezialisierte Plug-Ins. Auf diese Weise wird z. B. der Füllstand der Patronen des Netzwerkdruckers im Newsroom ermittelt.

Die letzte Methode ist der NSCA (Nagios Service Check Acceptor), dies ist eine eher passive Methode. Hierbei läuft auf dem Nagios-Server ein Daemon. Andere Nagiosinstanzen auf anderen Rechnern können an diesen Server Daten bzw. Resultate schicken. Der Haupteinsatzzweck ist ein verteiltes Monitoring für größere Umgebungen. Eine gute Anlaufstelle für weitere Plug-Ins ist die Austauschplattform http://nagiosexchange.org/.



(a) Serviceübersicht, mit den verschiedenen Zuständen OK, WARNING, CRITICAL

(b) Statusmap

Abbildung 3.6: Nagios-Statusmap und ein Teil der Service-Übersicht

3.4.2 Nagios-Objekte und -Benachrichtigungen

Nagios unterscheidet Hosts, Hostsgroups, Services, Servicesgroups, Kontakte, Kommandos und so weiter, diese sind in unterschiedlichen Konfigurationsdateien gespeichert unterhalb von `/etc/nagios2`. All das sind in Nagios Objekte und die Bezeichnung dafür kommt nicht von ungefähr; selbst Vererbung von Eigenschaften ist bei Nagios möglich. Nagios ist, wie im vorangegangen Abschnitt erläutert, ein mächtiges Werkzeug, standardmäßig wird der Administrator per E-Mail benachrichtigt, wenn eine Komponente nicht erreichbar ist. Es sind aber auch zig andere Wege möglich wie z. B. per SMS,

dazu sind die smstools[11] nötig sowie ein GSM-Modem, z. B. als USB-Stick, damit Nagios auch benachrichtigen kann, wenn die Internetverbindung zur Außenwelt gestört ist. Nagios bietet auch Benachrichtigungen über IM-Messages, Telefonanrufe etc. an, außerdem gibt es zahlreiche Plug-Ins für Browser[12] die den Status von Nagios abfragen können. Außerdem gibt es ein Eskalationsmanagement, dabei besteht die Möglichkeit, festzulegen, in welcher Reihenfolge Meldungen an weitere Kontaktpersonen (Administrator des Dienstes, Administrator der Maschine, RZ-Verantwortlicher...) erfolgen sollen, wenn eine Störung nach den ersten Meldungen nicht behoben wurde. UCS nimmt dem Administrator zwar Arbeit ab mit seiner Integration, so dass selbst Laien damit einigermaßen ihr Netz monitoren können, jedoch ist auch hier für ein tieferes Verständnis Arbeit auf der Kommandozeile nötig. Eine Dokumentation bringt Nagios mit z. B. unter `/usr/share/nagios2/htdocs/docs` oder über die Weboberfläche zu erreichen. Eine andere gute Quelle ist das Buch Nagios von Wolfgang Barth (siehe [2]).[13]

3.4.3 Vorteile, Nachteile und mehr Plug-Ins

Nagios hat seine Stärken bei der Erweiterbarkeit durch unzählige Plug-Ins, der Vielzahl an Benachrichtigungsmöglichkeiten sowie dem Eskalationsmanagement und ist eines der ältesten Open-Source-Monitoringprogramme. Nagios hat eine große und aktive Entwickler- und Anwendercommunity (für die deutschsprachige Community siehe http://www.nagios-portal.org/). Nagios ist weiterhin hoch skalierbar, durch NSCA können auch mehrere Nagios-Server zusammenarbeiten. Der Nachteil, dass Nagios zwar eine WebGUI zum Anzeigen, nicht aber zum Konfigurieren hat, wird durch Univention aufgefangen, ist aber bei normalen Installationen schon ein Hindernis. Dass Nagios keine Daten in einer SQL-Datenbank speichert, kann sowohl Nachteil als auch Vorteil sein, aber hierzu gibt es ebenfalls ein Plug-In.

Nagios sammelt nur Daten über den aktuellen Zustand eines System, OK- oder Fehler-Zustand, keine Performancedaten, es steht also kein Graph zur Verfügung der z. B. verdeutlichen würde, wann ungefähr eine neue Festplatte besorgt werden muss, weil der Festplattenplatz in einem bestimmten Tempo zur Neige geht oder wie die Zuverlässigkeit und die Verfügbarkeit von Diensten bzw. Netzwerkelementen ist. Dazu gibt es aber das Projekt Nagiosgraph, unter http://nagiosgraph.sourceforge.net. Die Perl-Software nutzt die Logging- und Graphing-Fähigkeiten des Open-Source-Werkzeugs RRDtool

[11] http://smstools3.kekekasvi.com/ oder http://smstools.meinemullemaus.de/
[12] Nagios Checker für Firefox: https://addons.mozilla.org/de/firefox/addon/3607
[13] Ein Vergleich zwischen Nagios und dem Tool Cacti sowie der Einrichtung beider auf UCS ist unter http://ingoebel.de/system_netzwerkmonitoring_nagios_cacti.pdf abrufbar.

(Round Robin Database)[14], mit dessen Hilfe auch Abb. 3.4 entstanden ist, um Graphen von Performancedaten zu erstellten. Diese Daten werden in Round-Robin-Datenbanken gespeichert.

Ein weiteres nützliches Projekt ist NagVis.Mit NagVis lassen sich Host- und Service-Zustände mit eigenen Grafiken visualisieren. Dabei ist es egal, ob das eine Landkarte, Zeichnung oder ein Raum voller Server ist, wie ihn Abb. 3.7zeigt. Auf dem Hintergrundbild positioniert man Objekte an beliebiger Stelle, die dann je nach Zustand ein rotes Icon für CRITICAL, ein gelbes für WARNING, ein grünes für OK oder ein blaues für UNKNOWN anzeigen.

Abbildung 3.7: NagVis mit einer Map eines Serverraumes als Hintergrund (Quelle: http://nagvis.org/screenshots)

3.5 Apache: HTTP-Server

Der Apache-Webserver ist der meistverwendete Webserver[15], an ihm führt kaum ein Weg vorbei. Der Apache-Webserver ist modular aufgebaut und kann um viele Module erweitert werden. Oft benutze Module sind z. B. mod_ssl zum Verschlüsseln von Verbindungen, mod_rewrite zum Manipulieren von URLs, außerdem werden viele Scriptsprachen wie PHP, Perl oder Ruby als Module eingebunden. Er läuft auch vielen verschiedenen Betriebssystemen, unter anderem AmigaOS, Novell NetWare und allen Unix-artigen Betriebssystemen wie *BSD, Solaris, Mac OS X und Linux. Unter Linux finden sich die Konfigurationsdateien unterhalb von `/etc/apache2`.

3.5.1 Konfiguration und Sicherheit

Der Webserver wird bei Univention schon beim Aufsetzen des Betriebssystems mit installiert, da die WebGUI des UCS funktionieren muss. Apache nutzt sogenannte Virtuelle Hosts (kurz vhosts), damit lassen sich mehrere Webangebote (z. B. www.convergentmedia.de und www.redaktionzukunft.de) auf einer einzigen Maschine betreiben. Siehe http://

[14] die RRDtools sind auf vielen Distributionen vorkompiliert zu finden, oder unter http://www.rrdtool.org

[15] siehe http://news.netcraft.com/archives/web_server_survey.html

httpd.apache.org/docs/2.0/de/vhosts/ für mehr Informationen zu vhosts. Diese vhosts lassen sich unterhalb von `/etc/apache2/sites-available` einstellen. Danach muss noch ein Symlink in `/etc/apache2/sites-enabled` gelegt werden und der Apache muss neu geladen (reload oder restart) werden.

Beispiel eines vhosts, welcher auf den Port der IP Adresse 141.62.53.165 und dem Port 80 lauscht:

```
<VirtualHost 141.62.53.165:80>
ServerName wiki.horads.de
ServerAdmin webmaster@horads.de
CustomLog /var/log/apache2/access.log combined
ErrorLog /var/log/apache2/error.log
LogLevel warn
DocumentRoot "/var/www/wiki"
Redirect 301 / https://wiki.horads.de/
#<Directory /var/www/wiki>
#  Options Indexes FollowSymLinks MultiViews
#  AllowOverride AuthConfig Limit
#
#  Order allow,deny
#  allow from all
#</Directory>
</VirtualHost>
```

Sobald also eine HTTP-Anfrage für die Domain wiki.horads.de erfolgt, würde dieser vhost benutzt werden. Der Browser würde durch die Redirect-Regel auf https://wiki.horads.de weitergeleitet werden. Für diese ist wieder ein anderer vhost zuständig, welcher auf dem Port 443 für HTTPS lauscht und die SSL-Einstellungen wie Zertifikate etc. enthält. Nicht für alle Dienste ist ein extra vhost eingerichtet worden, einige lassen sich auch einfach über http://media.hdm-stuttgart.de/"softwarename" erreichen, z. B. Nagios oder MRBS.

Sicherheit

In einer UCS-Standardinstallation sendet der Apache viele Informationen, z. B. Version, verwendete Module inkl. deren Version und mehr über sich im HTTP-Header und zeigt diese auch auf z. B. Errorseiten und Dateilistings an. Dies ist zwar im Fehlerfall vielleicht wünschenswert, jedoch ist der Apache heute ein großes Angriffsziel für

Cracker[16] und andere böse Buben siehe auch Abschnitt 8.1, daher sollten so wenige Informationen wie möglich das System verlassen. Um dies zu erreichen, muss in der `/etc/apache2/apache2.conf` der Parameter ServerTokens auf Prod gestellt werden, zusätzlich könnte ServerSignature auch auf Off gesetzt werden. Diese Einstellungen können auch in jedem vhost überschrieben werden, z. B. falls die Server-Signatur nur bei bestimmten Webangeboten angezeigt werden soll und bei anderen nicht.

ServerTokens Full	Apache/2.2.3 (Univention) mod_jk/1.2.18 PHP/5.2.0-8+etch7.64.200807101712 mod_ssl/2.2.3 OpenSSL/0.9.8c Server at media.hdm-stuttgart.de Port 80
ServerTokens Prod	Apache Server at media.hdm-stuttgart.de Port 80

3.5.2 LAMP

LAMP ist ein Akronym für:

- Linux
- Apache
- MySQL
- PHP bzw. andere Scriptsprachen, die ebenfalls mit P beginnen wie Perl oder Python

Diese verschiedenen Komponenten definieren zusammen einen Software-Stack für dynamische Webseiten. MySQL ist ein relationales Datenbankmanagementsystem (RDBMS), in dem viele Anwendungen ihre Daten speichern, es lässt sich auf einem Linux-System leicht installieren und einrichten. Damit auch PHP-Anwendungen ihre Daten in MySQL speichern können, sollte das PHP-MySQL-Modul installiert werden.

„Obwohl die [verschiedenen] Programme ursprünglich nicht darauf ausgelegt waren, miteinander zusammen zu arbeiten, wurde das Bündel schnell erfolgreich, da es einfach verfügbar und preiswert in der Beschaffung war und ist. Mit der Zeit haben sich eine Vielzahl von Community-Projekten rund um LAMP entwickelt, die Dokumentationen und einfache Installationsroutinen für LAMP-Systeme erstellen.“[31]

Es sind ganze LAMP-Distributionen entstanden, manche auch mit einem anderen Betriebssystem, z. B. WAMP für Windows und den anderen Komponenten. Erwähnenswert

[16] hier ist bewusst der Begriff Cracker gewählt, Hacker sind die „Guten“ und wollen in aller Regel keinen Schaden anrichten, sondern nur auf Probleme aufmerksam machen

ist noch die XAMPP, siehe http://www.apachefriends.org/de/xampp.html, welche für verschiedene Betriebssysteme existiert, einfach zu installieren und einzustellen ist. Diese Distribution bringt noch mehr Dienste mit wie z. B. Proftpd (siehe 3.7) und viele kleine Tools und Libraries.

Es gibt viele Software-Pakte, die auf diese LAMP-Komponenten aufsetzen, das geht von Content-Management-Systemen über Zeiterfassung und Wikisysteme bis hin zu professionellen Customer-Relationship-Management-Systemen (CRM). Für beinahe jeden Zweck, welcher sich irgendwie mit einem Browser bedienen lässt, gibt es mittlerweile ein Open-Source-Projekt, welches auf LAMP setzt.

3.5.3 Anwendungen auf LAMP

Open-Source-Anwendungen auf Basis dieses LAMP-Stacks, die für das CMC benutzt werden sind:

- Mediawiki, die Wikisoftware mit dem auch die Wikipedia läuft, siehe http://www.mediawiki.org/
- Das Raum- und Gerätebuchungssystem mrbs, siehe http://mrbs.sourceforge.net/
- die e-learning-Plattform Moodle, die HdM-weit eingesetzt wird, also nicht direkt auf dem CMC-Server läuft, siehe http://moodle.org/
- Zope, wird ebenfalls HdM-weit eingesetzt und läuft auf einem anderen Webserver
- Groupware, siehe Kapitel 5
- Nagios, siehe 3.4

Jedes der eben genanten Programme bietet die Möglichkeit, Userinformationen über LDAP abzurufen, d. h. die Userauthentifikation geschieht gegen den OpenLDAP. Mache Programme bieten das schon von Hause aus, bei anderen sind Extramodule dafür zuständig. Mediawiki wird hauptsächlich zur Dokumentation eingesetzt, mit MRBS lassen sich das Ton- oder Videostudio buchen, ebenso Equipment wie Foto- und Videokameras oder Audioaufnahmegeräte. Die Online-Lernplattformen Moodle wird als Kommunikationsplattform, Forum und Knowledgebase benutzt. Zope ist eigentlich ein kompletter Webanwendungsserver und setzt daher nur auf Linux und Python und ggf. MySQL. Zope bringt einen eigenen Webserver (Zserver), allerdings ist es auch möglich, Zope mit einem Apache zu betreiben. In Zope wurde ein Content-Management-System (CMS)[17] für das

[17] Es gibt auch schon ein fertiges CMS in Zope welches sich Plone nennt siehe http://plone.org

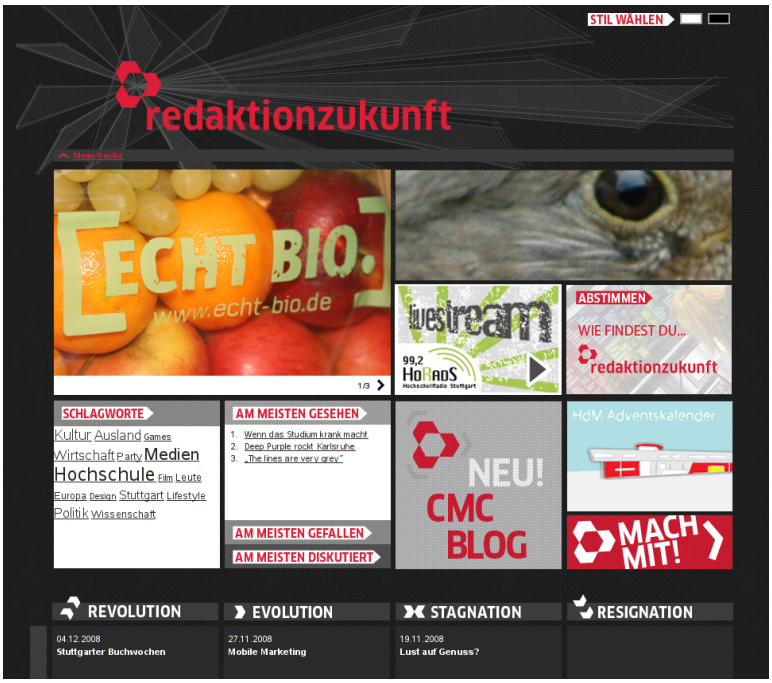


Abbildung 3.8: Website der Redaktion Zukunft

Online-Journal Redaktion Zukunft (http://www.redaktionzukunft.de) geschrieben. Die Studierenden stellen hier ihre Texte, Bilder, Audiobeträge, Infografiken und Videos ein. Das Design von Redaktion Zukunft war Thema einer Bachelorarbeit im Studiengang Infodesign[18] an der HdM siehe Abb. 3.8.

3.6 DHCP: Automatische Netzwerkeinstellungen

Über das Dynamic Host Configuration Protocol, kurz DHCP, werden Netzwerkkonfiguration an Geräte übermittelt. „Das Dynamic Host Configuration Protocol wurde im RFC 2131 definiert und bekam [...] die UDP-Ports 67 und 68 zugewiesen."[30]

Damit Rechner oder Geräte an einem TCP/IP-Netz teilnehmen können, muss jedem mindestens eine IP-Adresse zugewiesen werden. Dies bei jedem Client manuell durchzuführen ist viel Arbeit, daher erlaubt das DHCP eine automatische Einbindung eines neuen Computers in ein bestehendes Netzwerk. Am Client muss im Normalfall lediglich der automatische Bezug der IP-Adresse eingestellt werden. Der Client kann dann von einem DHCP-Server die IP-Adresse, die Netzmaske, das Gateway, DNS-Server und gegebenenfalls WINS-Server und Zeitserver beziehen.

[18] siehe http://www.maxlmedia.com/download/BA_Mollien_screen.pdf

Dazu wird ein Broadcast-Paket, also ein Paket als die IP 255.255.255.255, geschickt, der DHCPDISCOVER. Da solche Pakete nicht über Netzwerkgrenzen hinweg transportiert werden musste der Server auch in verschiedenen VLAN hängen (siehe 2.1). Die DHCP-Server antworten mit einem DHCPOFFER und machen Vorschläge für eine IP-Adresse. Dies geschieht ebenfalls mit einem Broadcast. Nimmt der Client einen der Vorschläge an, sendet er einen DHCPREQUEST wieder per Broadcast, der DHCP-Server bestätigt mit einer DHCPACK-Nachricht (DHCP-Acknowledged) die IP-Adresse.

Rechner im Netzsegment 141.62.96.0/24 erhalten auf eine DHCP-Anfrage automatisch eine IP zwischen 141.62.96.100 und 141.62.96.150 zugewiesen, außerdem den DNS-Server der HdM 141.62.1.5 sowie das default-Gateway 141.62.96.254. Rechner im Netzsegment 141.62.53.160/27 erhalten nur eine IP-Adresse, wenn diese im UCS-Managementsystem mit ihrer MAC-Adresse hinterlegt sind, anderen Clients wird nichts zugewiesen. Auch im CMC-Netz werden Einstellungen für einige Clients manuell zugewiesen, z. B. für alle festen Rechner und anderen Netzwerkgeräte gibt es feste IP-Adressen zwischen 141.62.96.2 und 141.62.96.99, diese sind entweder im Gerät fest eingestellt oder werden vom DHCP-Server anhand der MAC-Adresse vergeben.

Der DHCP-Server kann über `/etc/dhcp3` konfiguriert werden, allerdings werden bei UCS wieder alle Einstellungen über das Webinterface vorgenommen, daher hat auch der DHCP-Server eine vorkonfigurierte LDAP-Anbindung.

3.7 FTP: Datentransfer über weite Strecken

Das File-Transfer-Protokoll ist eines der ältesten Internet-Protokolle überhaupt, obwohl es auch andere Arten gibt, wie Dateien auf den Server gelangen könnten z. B. mit WebDav oder dem im Kapitel 8.5 beschriebenen OpenVPN, wird hier vorerst auf FTP gesetzt. FTP hat einige Vorteile wie einfache Installation und Konfiguration und ein ausgereiftes Chrooting[19], im Gegensatz zu SCP/SFTP[20], welches einen SSH-Server benötigt, bei dem es sehr schwierig ist, ein Change Root für jeden User anzulegen, damit diese nicht auf wichtige Systemdateien zugreifen können. Leider bietet FTP auch einige Nachteile wie die standardmäßige unverschlüsselte Übertragung und die Eigenheiten des Protokolls an sich. Dazu wird ProFTPd[21] eingesetzt, welcher zu den meistbenutzen FTP-Daemons unter UNIX-Systemen gehört. ProFTPd ist für UCS schon gebaut und

[19] Chrooting bietet eine einfache Möglichkeit, nicht vertrauenswürdige, Test- oder sonstwie gefährliche Programme in eine Sandbox zu versetzen.

[20] SSH File Transfer Protocol (SFTP) ist eine Weiterentwicklung von SCP und erlaubt sichere Datenübertragung und Dateizugriffe auf entfernte Systeme über SSH (Port 22); es sollte nicht mit FTPS (Port 21) verwechselt werden, FTPS ist FTP über TLS/SSL und benötigt daher keinen SSH-Server.

[21] Kurzform für Pro FTP daemon URL: http://www.proftpd.org/

kann einfach mit apt-get install proftpd installiert werden, allerdings ist dies nicht die neuste Version; da ein Bug in der SSL-Verarbeitung gefunden wurde, funktioniert nur die Version von der Website http://www.proftpd.org/ richtig mit dem FTP-Client Filezilla zusammen, dazu ist Kompilieren/Selbstbauen von Proftpd nötig. Der FTP-Server ist nicht in die WebGUI von Univention integriert. Per FTP sollen sich nur User mit ihrem eigenen Passwort anmelden können, es werden keine extra Virtuellen Hosts wie bei Apache angelegt. Jeder User darf nur in sein Homeverzeichnis. Damit FTP die User authentifizieren kann, ist eine Anbindung über LDAP nötig, da dies unsere zentrale User- und Passwortdatenbank ist, es gibt zwei Möglichkeiten, dies zu erreichen: entweder über PAM (Pluggable Authentication Modules) oder direkt in die Konfigurationsdateien eintragen. Es wird die zweite Variante genutzt. Die Konfigurationsdatei für ProFTPd liegt unter `/etc/proftpd/proftpd.conf`, damit die User nur auf hier Homeverzeichnis gechangerooted[28] werden ist der Eintrag DefaultRoot ~ nötig. Für die LDAP-Anbindung wurde die Konfigurationsdatei um folgende Einträge erweitert:

```
LDAPServer localhost
LDAPDNInfo cn=admin,dc=media,dc=hdm-stuttgart,dc=de XXXXX[22]
LDAPDoAuth on "dc=media,dc=hdm-stuttgart,dc=de"
```

Nun können sich die LDAP-Benutzer per FTP anmelden, dazu können Sie einen FTP-Client Ihrer Wahl benutzen, ggf. auch ihren Browser.

Da FTP wie oben erwähnt standardmäßig unverschlüsselt ist und das Passwort damit auf dem Weg von FTP-Client zum Server mitgelesen werden kann, müssen noch Maßnahmen ergriffen werden, die auch eine verschlüsselte Kommunikation gewährleisten. Dies ist mit FTP über explizit TLS/SSL (FTPES) möglich. Zwar unterstützen diesen Modus nicht alle FTP-Clients, aber der als Open Source und plattformübergreifend verfügbare Filezilla[23] schon. Damit FTPS benutzt werden kann, sollte überprüft werden, ob ProFTPd mit SSL-Unterstützung kompliert worden ist, in der UCS-Variante ist dies der Fall, daher kann die Konfiguration einfach um folgende Zeilen ergänzt werden:

[22] Für XXXXX muss das entsprechende Passwort gesetzt werden, auch die Basedn muss angepasst werden, zu empfehlen ist es auch einen User im LDAP anzulegen der nicht alle Einträge auch schreiben kann sondern nur Zugriff auf die User und Passwörter hat

[23] http://filezilla.sf.net

```
<IfModule mod_tls.c>
TLSEngine on
TLSProtocol TLSv1
TLSRequired off
TLSVerifyClient off
TLSRSACertificateFile /etc/univention/ssl/media/cert.pem
TLSRSACertificateKeyFile /etc/univention/ssl/media/private.key
</IfModule>
```

Der verschlüsselte Zugriff ist nun möglich. Jeder User wird in sein Homeverzeichnis gechangerootet d. h. kann also dort nicht heraus. Da jedoch einzelne Personen Zugriff auf bestimmte Freigaben benötigen und außerdem eine Standardfreigabe für alle User genutzt werden soll, ist es nötig, die entsprechenden Verzeichnisse im Homeverzeichnis darzustellen. Auf Grund der Problematik, dass der FTP-User in seinem Chroot „gefangen“ ist, können keine Symlinks gesetzt werden, da diese auf einen Bereich zeigen würden, der aus dem Chroot nicht erreichbar ist. Die einzige Möglichkeit dafür ist es, mittels eines bind mounts die Verzeichnisse im Homebereich darzustellen. Das Verzeichnis /daten/webserver ist die zentrale Ablage, diese soll für jeden User zur Verfügung stehen. Also wird ein Ordner /home/username/webserver angelegt und mittels mount –bind /daten/webserver /home/username/webserver eingebunden. Nun kann der User, entsprechende Rechte vorausgesetzt, auch diese Dateien lesen bzw. bearbeiten. Dies muss natürlich für jeden User einzeln gemacht werden, was sich aber mit einem einfachen Bash-Skript lösen lässt.

4 Backup: Datensicherung und Failover

Ein wichtiges Thema ist auch, für ein Backup zu sorgen, damit Daten nicht verloren gehen.

Auf dem Server werden viele wichtige Daten gelagert, er ist das Herzstück der Redaktion Zukunft, von HoRadS und Stufe. Sollte er ausfallen, können an den Windows-Clients keine Anmeldungen mehr durchgeführt, keine Daten gespeichert oder Musik abgespielt werden. Daher ist es wichtig, ein Konzept zur Datensicherung und für einen Failover, d. h. ungeplante Wechsel von einem Primärserver zu einem zweiten Standby-System, zu erarbeiten und umzusetzen.

4.1 Allgemeine Überlegungen

Die Sicherung auf Tape (Band) ist für diese Umgebung nicht geeignet. Bandlaufwerke sind zum einen sehr teuer, ebenso die Bänder. Das Sichern und Wiedereinspielen von Tapes dauert außerdem sehr lange und ist daher nur für die Langzeitarchivierung sinnvoll. Genau diese Art wird hier jedoch nicht gebraucht, eher ist es erforderlich, auf Versehentlich gelöschte Daten schnell zugreifen zu können, auch wird eine Möglichkeit gebraucht, im Fehlerfall schnell ein lauffähiges System zu haben (Failover). CDs/DVDs sind ebenfalls kein Backupmedium für diese Infrastruktur, DVDs lassen sich zwar schneller einlesen als Bänder, können aber, da der Server im Rechenzentrum steht und kein DVD-Wechselautomat zur Verfügung steht, nicht verwendet werden; bleiben nur Festplatten (HDDs). Der Festplattenpreis ist drastisch gefallen, der Preis pro GB bei einer 3,5-SATA-Festplatte bei ca. 0,13 €. Daher sind Festplatten mittlerweile ein sehr beliebtes Backupmedium.

4.2 Strategien

Der Server hat ein RAID (redundant array of independent disks) von 3Ware eingebaut. Mehrere Festplatten sind als RAID 5, der beliebteste RAID-Variante, zusammengeschaltet. Diese Variante bietet sowohl gesteigerten Datendurchsatz beim Lesen von Daten als

auch Redundanz. Ein RAID bietet damit Ausfallsicherheit, bei einem RAID 5 kann maximal eine Festplatte ausfallen, die dann schleunigst ersetzt werden sollte, ohne dass Daten verloren gehen. Ein RAID ersetzt allerdings kein Backup und leistet auch keinen Schutz davor, wenn ein anderes Teil des Servers als die Festplatte ausfällt. Daher gibt es mehrere Möglichkeiten, wie zusätzlich Daten sicher vorgehalten werden können.

4.2.1 Rsync über ssh

Rsync ist ein Programm zur Synchronisation von Daten, meistens über ein Netzwerk. Da Rsync nur die Teile von Dateien überträgt die sich geändert haben und nicht jedes Mal die ganze Datei, kann enorm viel Bandbreite und Zeit gespart werden. Rsync über SSH bietet zudem die Möglichkeit der Verschlüsselung, kostet dafür aber auch etwas Performance. Mit Rsync können Snapshots des kompletten Systems vorgenommen werden

Nachteile dieser Lösung sind, das der erstellte Snapshot manuell gebootet werden muss, es dauert also eine Zeitlang, bis im Falle eines Desasters das Backup lauffähig ist. Außerdem müsste beim Erstellen des Snapshots darauf geachtet werden, dass keine inkonsistenten Daten entstehen, also müssten SQL-Server, Mailserver und weitere, die eine Datenbank pflegen, angehalten werden, und da es eine Weile dauern kann, bis rsync einen kompletten Server gebackuped hat, wäre das eine zu lange Zeit. Zwar können z. B. MySQL-Dumps extra erstellt werden, die rsync dann mit kopiert, allerdings würde das beim Wiederherstellen des Systems ebenfalls Zeit kosten, bis der MySQL-Dump wieder eingespielt ist. Ebenso könnten beim GAU alle Daten zwischen Snapshot und der aktuellen Zeit verloren gehen.

Dennoch reicht dies bei einigen Servern durchaus. Mit einigen Skripten[1] können jede Nacht Snapshots erstellt werden, diese können für mehrere Tage oder Wochen vorgehalten werden, Snapshots von wichtigen Tagen, Monatsanfängen oder Ereignissen können über lange Zeit aufgehoben werden. Falls eine Datei versehentlich gelöscht wurde, kann diese aus einem rsync-Snaptshot wieder hergestellt werden. Diese Methode wird auf dem neuen Backupserver genutzt, um andere Server zu sichern, die keinen schnellen Failover brauchen, hierzu wird jede Nacht ein Snapshot des gesamten Servers über rsync gezogen, unwichtige Dateien oder Verzeichnisse werden ausgenommen. Dieser Snapshot wird in ein Verzeichnis gespeichert. Tagsüber werden die Snapshots rotiert, d. h.. Tag0 wird nach Tag1 verschoben, Tag1 nach Tag2 u.s.w., diese Snapshots sind dabei als Hardlinks angelegt, d. h. in jedem Ordner findet sich der komplette Server an, eine Datei die z. B. in Tag 1 und Tag 2 gleich ist, belegt aber nur einmal den physikalischen Speicherplatz

[1] siehe http://www.heinlein-support.de/web/support/wissen/rsync-backup/

auf dem Dateisystem. Damit ist man in der Lage, täglich eine neue Snapshot-Kopie zu machen, die keinen Speicherplatz kostet, solange sich nichts ändert. Wird eine Datei geändert, wird rsync diese Änderung übertragen und in das Backup einpflegen. Zuvor allerdings löst rsync den Hardlink auf und erzeugt eine neue Kopie der Datei. Erst dann existiert diese zwei Mal physikalisch und belegt auch zwei Mal Speicherplatz.

4.2.2 LVM

Eine weitere Möglichkeit wäre, die Verwendung von LVM (Logical Volume Manager). LVM bietet die Möglichkeit, zur Laufzeit einen Readonly-Snapshot des Dateisystem zu machen. Der statische Readonly-Snapshot kann anschließend auf einen anderen Server kopiert/repliziert werden.

Die ist eine sehr schnelle Variante, das Problem ist allerdings, wie bei rsync müssten Mailserver, SQL-Server und Co für kurze Zeit angehalten werden, um konsistente Datenbanken zu gewährleisten. Im Falle eines Fehlers müssten die Dienste manuell auf dem zweiten Server gestartet werden, außerdem würden nur die Daten des letzten Snapshots zur Verfügung stehen. Daten der vergangenen Zeit zwischen Snapshot und dem auftretenden Problem sind im schlimmsten Fall für immer verloren.

4.2.3 Failover mit DRBD/Heartbeat

Ein Failover ist kein klassisches Backup. Für einen Failover reichen nicht nur die Daten an sich, sondern für alle Teile des aktiven Servers muss es ein Backup geben. Daher spricht man auch davon, dass Daten und Dienste hochverfügbar gehalten werden. Ist ein Server ausgefallen, so initiiert der andere Server automatisch die Übernahme der Dienste. Binnen weniger Sekunden bis Minuten stehen dieser dann den Nutzern wieder zur Verfügung. Für ein System mit Failover würde es auch ausreichen, ein shared-scsi oder NAS/SAN zu haben, allerdings sind diese Dinge meist sehr teuer und sind ein Single Points Of Failure (SPOF), d. h. fallen die Festplatten aus, braucht man auch keinen Server-Failover. Daher wird DRBD verwendet, dies realisiert ein RAID 1, also eine komplette Spiegelung der Daten über ein Netzwerk. Der Herzschlag (Heartbeat) prüft regelmäßig, ob die Server sich noch gegenseitig erreichen und startet im Fehlerfall auf dem Zweitserver die entsprechenden Dienste.

4.3 Umsetzung

Für den Failover wurde die DRBD/Heartbeat-Lösung gewählt. DRBD ist auf UCS verfügbar, auch die Kernelmodule stehen schon zur Verfügung, müssen also nicht extra kompiliert werden. Heartbeat steht zwar für UCS 2.1 nicht zur Verfügung, aus dem unmaintainten Bereich für UCS 2.0 kann es jedoch installiert werden, alternativ kann auch hier das Paket selbst gebaut werden.

Der Backupserver

Wie schon in Abschnitt 2.2 erwähnt, sind beide Server sehr ähnlich und beide aus dem Hause Transtec. Sowohl der aufgebaute Server als auch der Standby-Server für einen Failover haben jeweils zwei Netzwerkkarten. Die erste ist mit öffentlichen IP-Adressen ausgestattet und ist die Verbindung zum CMC-Netz und Internet, auf der zweiten wurden private Adressen aus dem 10.0.0.0-Netz vergeben. Der CMC-Server erhielt die IP 10.0.0.1, der Backup-Server die IP 10.0.0.2 siehe Abb. 4.1. Beide sind direkt, ohne einen Switch über ein (Crossover-)Ethernetkabel verbunden. Auf beiden läuft das gleiche Betriebssystem, ein UCS 2.1 64bit mit Kernel 2.6.24 in der gleichen UCS-Serverrolle.

Der Standby-Server hat fast nicht zu tun und ist nur im Leerlauf. Es gäbe zwar auch die Möglichkeit, diesen mit einzusetzen, z. B. Active/Active-Konfigurationen von Heartbeat oder Loadbalancing zu betreiben, diese Konfigurationen sind jedoch etwas schwieriger. Daher hat der Standby-Server auch die Aufgabe, andere Systeme zu sichern, dafür wurden noch mehr Festplatten besorgt und ein zweites Hardware RAID 5 erstellt. Mit der rsync-über-SSH-Methode werden wichtige Rechner und Server komplett auf diesen gebackuped.

4.3.1 DRBD

Da der Server schon produktiv im Einsatz war, aber die Daten behalten werden sollten, ist äußerste Vorsicht geboten. Eine Sicherungskopie aller sollte in jedem Fall gemacht werden!

Mit `apt-get install univention-drbd` lassen sich die benötigten drbd8-utils installieren. Dazu muss noch das passende Kernelmodul installiert (hier: apt-get install drbd8-2.6.24-ucs8-amd64) bzw., falls nicht vorhanden, kompiliert werden, diese Schritte sind auch im offiziellen DRBD User Guide unter http://www.drbd.org/users-guide/ beschrieben [12].

Danach sollte das Modul geladen werden mittels:

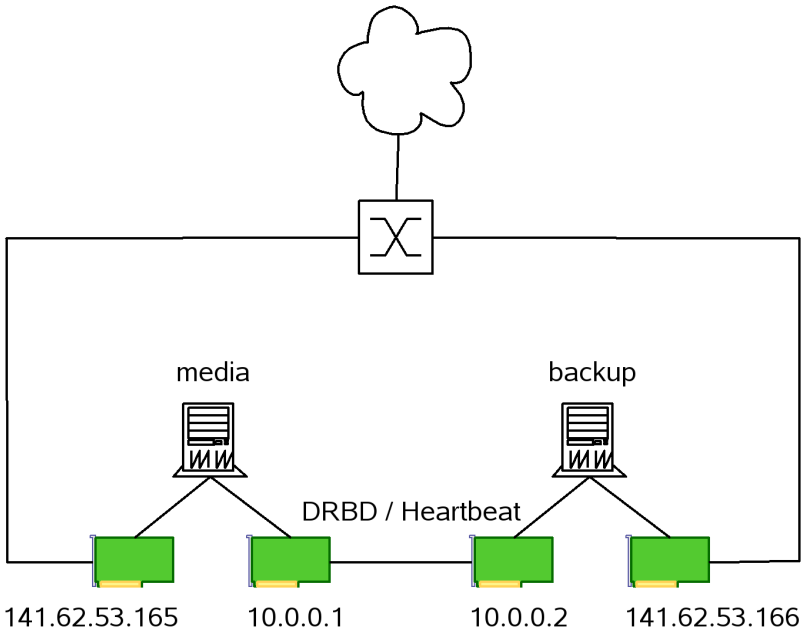


Abbildung 4.1: Separates Netz für DRBD/Heartbeat

```
insmod /lib/modules/2.6.24-ucs8-amd64/kernel/extra/drbd.ko
```

Jetzt sollte `/proc/drbd` zur Verfügung stehen. Ist dies nicht der Fall, müssen vorher noch andere Module geladen werden z. B. cn (`modprob cn`). Auf beiden Servern (Cluster Nodes) müssen ungefähr identische Speicherbereiche für DRBD zur Verfügung gestellt werden. Das können sein:

- eine Festplattenpartition oder die gesamte Festplatte
- ein Software RAID device
- ein LVM Logical Volume oder jedes andere Blockdevice, welches über den Linux device-mapper funktioniert
- sowie jedes Blockdevice auf dem System

In diesem Beispiel ist das auf dem CMC-Hauptserver (media) eine normale Festplattenpartition, auf dem Backup (media2) ein LVM. DRBD wird über die Konfigurationsdatei `/etc/drbd.conf` gesteuert. Im Folgenden wird die drbd.conf für das Home-Verzeichnis gezeigt, auf dem die wichtigsten Daten liegen. Die Datei muss auf beiden Servern gleich sein.

```
global {
usage-count no;
}
common {
    protocol C;
    syncer { rate 20M;
           }
       }

resource r0 {

  on media {
    device    /dev/drbd0;
    disk      /dev/sda3;
    address   10.0.0.1:7788;
    meta-disk internal;
  }
  on media2 {
    device    /dev/drbd0;
    disk      /dev/mapper/vg_ucs-vol2;
    address   10.0.0.2:7788;
    meta-disk internal;
  }
}
```

Es gibt drei unterschiedliche DRBD-Protokolle. A, B und C, wobei C der Standard ist und gleichzeitig das sicherste. Protokoll C wartet ab, bis der Schreibvorgang auf beiden Servern erfolgreich durchgeführt wurde. Der Parameter meta-disk internal gibt an, dass DRBD-Metadaten, die wichtig für den Betrieb sind, am Ende des physikalischen Devices, also z. B. der Partition, speichert. Es gibt auch die Möglichkeit, dies extern an einer anderen Stelle, z. B. einer kleinen Partition, zu speichern. Beides hat Vor- und Nachteile, die unter http://www.drbd.org/users-guide/ch-internals.html nachgelesen werden können.

Da normalerweise das Filesystem den kompletten Platz einer Partition einnimmt, muss es verkleinert werden, damit DRBD seine Metadaten speichern kann. Dazu kann das Programm ext2resize[2] benutzt werden. Unter der eben genannten URL sind auch For-

[2] ext2resize, ist in Debian Etch enthalten, in UCS direkt nicht, es kann auch über http://ext2resize.

```
version: 8.0.12 (api:86/proto:86)
GIT-hash: 5c9f89594553e32adb87d9638dce591782f947e3 build by phil@mescal, 2008-04-24 13:29:44
 0: cs:SyncSource st:Primary/Secondary ds:UpToDate/Inconsistent C r---
    ns:156096 nr:0 dw:0 dr:156096 al:0 bm:9 lo:0 pe:0 ua:0 ap:0
        [>....................] sync'ed:  0.1% (1772381/1772533)M
        finish: 1260:21:36 speed: 384 (320) K/sec
        resync: used:0/61 hits:9746 misses:10 starving:0 dirty:0 changed:10
        act_log: used:0/257 hits:0 misses:0 starving:0 dirty:0 changed:0
```

Abbildung 4.2: DRBD beim Syncronisieren

meln angegeben. mit denen berechnet werden kann, wieviel Platz für die Metadaten gebraucht wird. Mit ext2resize können ext2/3-Filesysteme verkleinert werden, andere Dateisysteme haben ggf. andere Tools. Eine saubere Lösung wäre es auch, ein komplett neues Dateisystem anzulegen, wenn das möglich ist. Nachdem auf dem Device jetzt Platz ist für die Metadaten, können diese mit `drbdadm create-md r0` geschrieben werden. Mit `drbdadm up r0` wird das Device erstellt und mit seinem Gegenüber verbunden. Diese beiden Schritte sind auf Cluster Nodes notwendig. Der letze Schritt muss nur auf dem primären Server durchgeführt werden, also hier nur auf media. `drbdadm -- --overwrite-data-of-peer primary r0` startet die Syncronisation und legt den media als Quelle fest. Nun kann `/proc/drbd` beobachtet werden (z. B. mit `watch cat /proc/drbd`) siehe Abb. 4.2. Das erste Synchronisieren kann mitunter sehr lange dauern ggf. auch Tage, je nachdem, welche Geschwindigkeit für syncer eingestellt ist. Im obigen Beispiel sind das 20Mb/sek. DRBD ist nun fertig eingerichtet. Das Device `/dev/drbd0` kann gemountet und normal benutzt werden, selbst wenn der sync-Prozess noch läuft.

4.3.2 Heartbeat

Mit DRBD steht nun auf beiden Server die gleiche Datenbasis zur Verfügung, nun muss im Fehlerfall ein Programm aber noch die IP-Adresse ändern und die Dienste starten. Das kann Heartbeat aus dem Linux-High-Availability-Projekt (`http://linux-ha.org`) übernehmen.

Heartbeat steht nicht für UCS 2.1 zur Verfügung kann aber aus UCS 2.0 genommen siehe `http://apt.univention.de`. Mittels `apt-get install heartbeat` werden das Paket und die entsprechenden Abhängigkeiten installiert.

Es wird eine Active/Passive- (auch hot standby genannt) Konfiguration vorgenommen, bei der auf einem Server alle Dienste laufen und der zweite nur im Fehlerfall übernimmt. Es können auch Active/Active-Konfigurationen erstellt werden, wo z. B. einige Dienste

`sourceforge.net` heruntergeladen werden.

wie Mailserver auf dem einen Rechner laufen und der Webserver auf dem anderen.

Zum Starten von Heartbeat sind drei Dateien wichtig[24]. Diese müssen erstellt und unterhalb von `/etc/ha.d/` abgelegt werden. Die erste Datei ist die ha.cf, in ihr werden die Cluster Nodes festgelegt sowie das Interface, über welches die Heartbeat-Kommunikation erfolgen soll.

```
ucast eth1 10.0.0.1
logfile /var/log/ha.log
auto_failback off
node media
node media2
```

Dies ist eine sehr minimale ha.cf, welche für den Failover des CMC-Servers aber ausreicht. Als Logdatei wird `/var/log/ha.log` verwendet. Es kann auch syslog benutzt werden. Diese Datei sieht auf dem Backup-Server fast identisch aus, nur die erste Zeile enthält stattdessen `ucast eth1 10.0.0.2`, um auch hier das richtige Interface anzusprechen. Der Parameter auto_failback ist hier auf off gestellt, wenn der CMC-Server wieder online ist, wird nicht direkt wieder auf diesen umgeschaltet, dies muss manuell geschehen.

Die zweite wichtige Datei ist haresources. Hier wird konfiguriert, auf welchem Server welche Dienste laufen; da nur ein Server aktiv (primary) ist, wird auch nur dieser eine hier eingetragen:

```
media drbddisk::r0 Filesystem::/dev/drbd0::/home::ext3
141.62.53.165/27/eth0 141.62.96.1/24/vlan96
slapd heimdal-kdc mysql apache2 nagios2 samba bind9 saslauthd
postfix cyrus2.2 dhcp3-server proftpd
```

Das erste ist der Hostname, wie ihn der Befehl `uname -n` auf der Kommandozeile ausgibt, gefolgt von der Anweisung, bei einem Failover drbddisk für die Resource r0 aufzurufen, damit DRBD auf dem Server primary wird. Danach wird das Filesystem gemountet. Außerdem sind die IP-Adressen angegeben, auf denen die Dienste laufen, diese IP wechselt also im Falle eine Failovers den Server. Danach stehen die Dienste, die gestartet werden müssen. Diese starten in der Reihenfolge von links nach rechts, wie sie angegeben werden. Als Erstes sollte hier natürlich der LDAP-Server stehen. Heartbeat schaut bei den Namen für die Scripte erst in `/etc/ha.d/resource.d` und danach in `/etc/init.d`.

Die letzte wichtige Datei ist authkeys. Sie muss genau eine Authentifizierungsmethode enthalten und ebenfalls auf beiden Servern gleich sein. Es reicht hier die einfachste

Methode, CRC, da die Umgebung, direkte Verbindung über ein Crossover-Kabel, vertrauenswürdig ist.

Listing 4.1: /etc/ha.d/authkeys

```
auth 1
1 crc
```

Ist die Verbindung über ein anderes Netz realisiert, sollte z. B. sha1 benutzt werden.

Es gibt viele verschiedene Möglichkeiten, DRBD/Heartbeat einzusetzen und Dienste zu starten. Es ist sogar möglich, komplette virtuelle Maschinen unter Xen oder KVM auf einen anderen Rechner umzuziehen und zu starten[1]. Die Rootpartition wird in dieser Konfiguration nicht 1:1 gespiegelt mit DRBD, um aber Konfigurationsänderungen an den Diensten wie Samba, Apache etc doch zu übernehmen, läuft jede Nacht ein Rsync.

5 Groupware

Eine Groupware, oder auch kollaborative Software genannt, dient dazu, die Zusammenarbeit in einer Gruppe zu erleichtern. Dieses Kapitel beschäftigt sich mit der Auswahl einer Groupware-Lösung sowie deren Umsetzung.

5.1 Auswahl: Kriterien

War bis vor Kurzem noch die Entscheidung für eine Groupware relativ einfach, da automatisch nur die großen drei, also Microsoft Exchange, IBM Lotus Notes oder Novell Groupware, wirklich in Frage kamen, buhlt heute eine Vielzahl an Software mit unterschiedlichem Funktionsumfang um die Gunst des Users oder Administrators. Immer mehr dieser Groupware-Lösungen sind mittlerweile auch Open Source. Da jeder Hersteller/Entwickler etwas anderes unter Groupware zu verstehen scheint, ist es schwer, die richtige Lösung zu finden. Somit gibt es keine Lösung, die auf alle Anforderungen passt: „There is no one size fits all!“[3]. Minimal sollte eine Groupware allerdings E-Mail- , Termin- und Kontaktverwaltung bieten.

Es lassen sich zurzeit drei Gruppen von Lösungen ausmachen: Die komplett proprietären wie Lotus und Exchange, die halboffenen, bei denen Teile Open Source sind und andere Komponenten lizenzpflichtig, Zimbra, WICE, sowie die komplette freien wie Horde oder Egroupware, wobei gesagt werden muss, dass es zum Glück in den letzten Monaten sehr viel Bewegung gab. Einige, die in dem zweiten Bereich waren, haben mittlerweile alles als Open Source freigegeben. [27, 11]

So sind im Jahr 2007 gleich 2 umfangreiche Werke zum Thema Groupware erschienen. Eines vom Heise-Verlag, unter anderem Herausgeber der c’t und iX, die iX-Studie „Groupware“ (http://www.heise.de/kiosk/special/ixstudie/07/02/), zum anderen von der Linux New Media, Herausgeber des Linux Magazins, das Technical Review 05 Groupware (http://www.linux-magazin.de/heft_abo/ausgaben/technical_review/ltr_05_groupware).

Damit aus dieser Fülle die richtige Auswahl getroffen werden kann, müssen Auswahlkriterien definiert werden. Diese können bei jedem Unternehmen oder jedem Projekt

andere sein. Für diese Umsetzung waren die Auswahlkriterien folgende:

- Open Source/Offene Standards
- Integration in bestehende Intrastruktur
- guter Webclient
- Anbindung an verschiedene Fat Clients (wie Mozilla Thunderbird), Microsoft-Outlook-Anbindung ist nicht nötig
- möglichst Anbindung an mobile Geräte
- Professioneller/kommerzieller Support

Ein Vorteil ist sicher, dass bei der Auswahl der Software nicht auf eine Outlook-Anbindung geachtet werden muss, da die meisten Studenten sowie Mitarbeiter beim CMC/HoRadS/-stufe nicht mit Outlook arbeiten, allerdings bieten die meisten Pakete mit kommerziellen Support auch einen Outlook-Konnektor an.

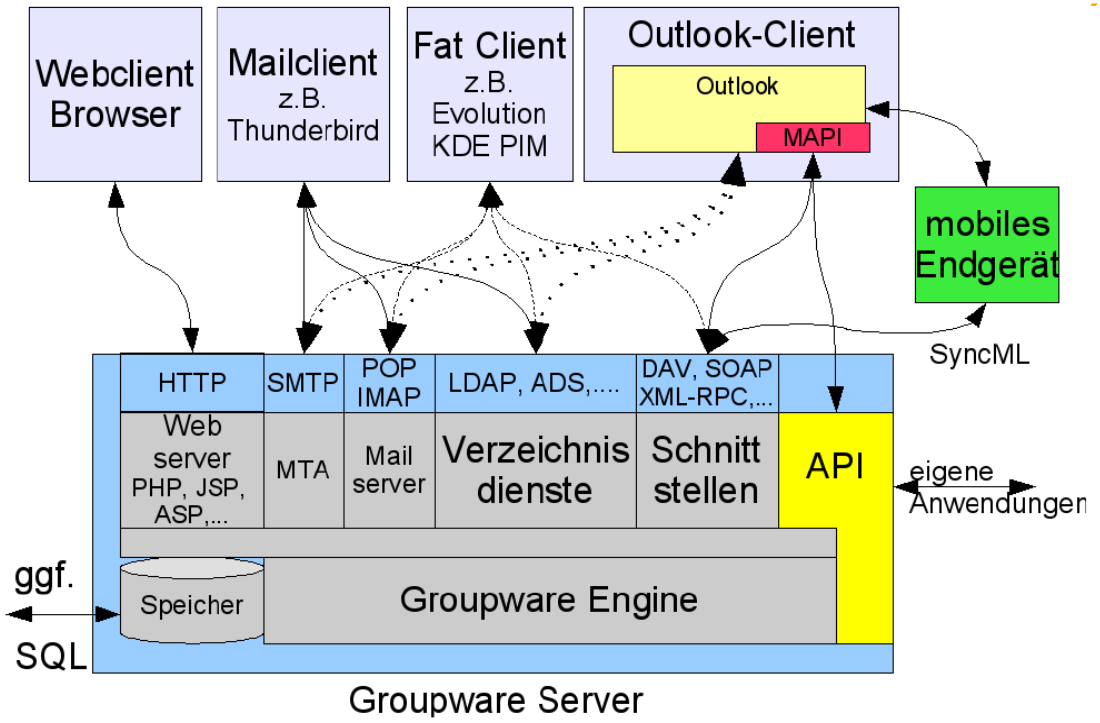


Abbildung 5.1: Ein Groupware-Server mit verschiedenen Anbindungen [3]

5.2 Auswahl: Software

Die Liste der Groupware-Produkte ist ziemlich lang, einige wurden auch eben schon genannt: Lotus Notes von IBM, Groupwise von Novell, Sun ONE von Sun, Scalix, Citadel, Collanos Workplace, OpenGroupware.org, Ipswitch Collaboration Suite, Open-Xchange, Microsoft Exchange, Zimbra von Yahoo, Tobits David, WICE CRM-Groupware, Zarafa, Kolab, eGroupWare, phpGroupWare, GROUP-E und PHProjekt. Diese Liste ist gewiss nicht vollständig, außerdem es gibt auch viele Appliances, also komplett fertig einsetzbare Distributionen mit vielen Funktionen, die eine der oben genannten Groupwares benutzen.

Tabelle 5.1 zeigt die Groupware-Lösungen, die genauer betrachtet wurden. Dabei ist zu beachten, dass sich in dem Markt, wie schon erwähnt, sehr viel tut. Es ist ein sehr dynamischer Markt mit viel Potential. Die Auswahl der Groupware fand zwischen Dezember 2007 und Februar 2008 statt, daher sind einige der Ergebnisse von damals schon wieder überholt.

Name	Hersteller	Vorteile	Nachteile
Open Groupware.org	Skyrix Software AG, http://www.skyrix.com/de/	+ viele offene Schnittstellen + Cyrus / Postfix Anbindung Möglich	- keine Integration in UCS - nachgelassene Entwicklung / Dokumentation von 2004
OpenXchange	Open-Xchange GmbH, http://www.open-xchange.com/de/	+ AJAX-GUI + schon OX 5 im Einsatz erlebt + komplett Open Source (bis auf Outlook-Konnektor) + Anbindung an mehrere Clients	- keine Integration in UCS - auf OX 6 Basis ist das Schreiben auf WebDav-Kalendern nicht möglich
Kolab	Kolab-Konsortium, http://www.kolab-konsortium.de/	+ kein MySQL nötig / alles in IMAP + Integration in UCS von Univention als UGS + Postfix / Cyrus Anbindung + komplett Open Source	- keine eigene WebGUI - richtige Client unterstützung nur für KDE Kontact + Properitär mit Outlook Konnektor - keine Syncro mit Mobilengeräten
Scalix	Xandros Inc, http://www.scalix.com/	+ AJAX-Oberfläche + Robust, Hoch Skalierbar + fertige Integration in UCS erhältlich	- GUI sieht zu sehr Outlook ähnliche - Viele Funktionen nur in Outlook - keine Postfix-/Cyrus-Umgebung - schlecht verschlüsselte Verbindung - nicht komplett Open Source
Zarafa	Zarafa BV, http://www.zarafa.com/	+ postfix möglich + z-push + UCS Integration fertig	- große Teile nicht unter Open-Source-Lizenz - keine Multi-Domain-Unterstützung - keine Fat Clients mit Thunderbird/-Kontact
Zimbra	Zimbra Inc (Yahoo!), http://www.zimbra.com/	+ AJAX-GUI + Postfix möglich	- von Yahoo abhängig, ggf. bald Teil von Microsoft - keine UCS-Integration - nicht komplett OSS

Tabelle 5.1: Vergleich von Groupware-Lösungen

Die Groupware Open Xchange machte das Rennen für dieses Projekt, zum einen wegen bereits bestehender Kontakte zu Open Xchange, zum anderen überzeugte die mit Ajax-Technologien gestaltete WebGUI und die Dokumentenverwaltung. Außerdem ist die Groupware komplett Open Source, bis auf den Outlook-Konnektor, welcher keine Rolle spielt bei dieser Installation und in Kürze ebenfalls unter einer Open-Source-Lizenz freigegeben werden soll[11]. Open Xchange ist trotzdem ein kommerzielles Produkt und für den Support und die Wartung (maintenance) wurde ein Vertrag geschlossen.

5.3 Umsetzung und Installation Open Xchange

Nachdem die Entscheidung zu Gunsten von Open Xchange (OX) gefallen war, wurde die Integration in das bestehende UCS beauftragt. Open Xchange stetzt zwar zum großen Teil auf Open-Source-Komponenten wie OpenLDAP, Postfix, Cyrus, MySQL, die auf dem Server bereits installiert waren, jedoch mussten Mechanismen entwickelt werden, damit sowohl die LDAP-Struktur von Univention als auch die von Open Xchange genutzt werden können, ebenfalls sollte Open Xchange über die WebGUI des UCS bedienbar gemacht werden, damit die zentrale Administration des Systems weiterhin möglich ist. Diese Integration wurde von der iKu Systems & Services (http://www.iku-systems.de/) aus Saarbrücken erstellt. Die ersten Gespräche hierzu begannen im März 2008 auf der CeBIT in Hannover. Open Xchange arbeitete zu der Zeit gerade an der Open-Xchange Server Edition (OX SE) sowie an der für 1&1 MailXchange benutzen Open-Xchange Hosting Edition (OX HE), den Nachfolgeprodukten des, auch immer noch installierbaren, Open Xchange Servers 5. Da beide Produkte die gleiche Codebasis benutzen, wird hier nur von OX geredet. Open Xchange stellt die Debian-Pakete von OXHE für die Installation auf UCS bereit und nimmt Anpassungen und Bugfixes vor, die die Integration gestört hätten, ebenso änderte Univention Teile seines Betriebssystemen falls dies nötig war. OX steht neben Debian auch für SLES und RHEL zur Verfügung.

Abbildung 5.2: Open-Xchange-Logo

Die Integration besteht aus:

- LDAP Schemaerweiterung
- Modulerweiterung für den Univention Directory Manager

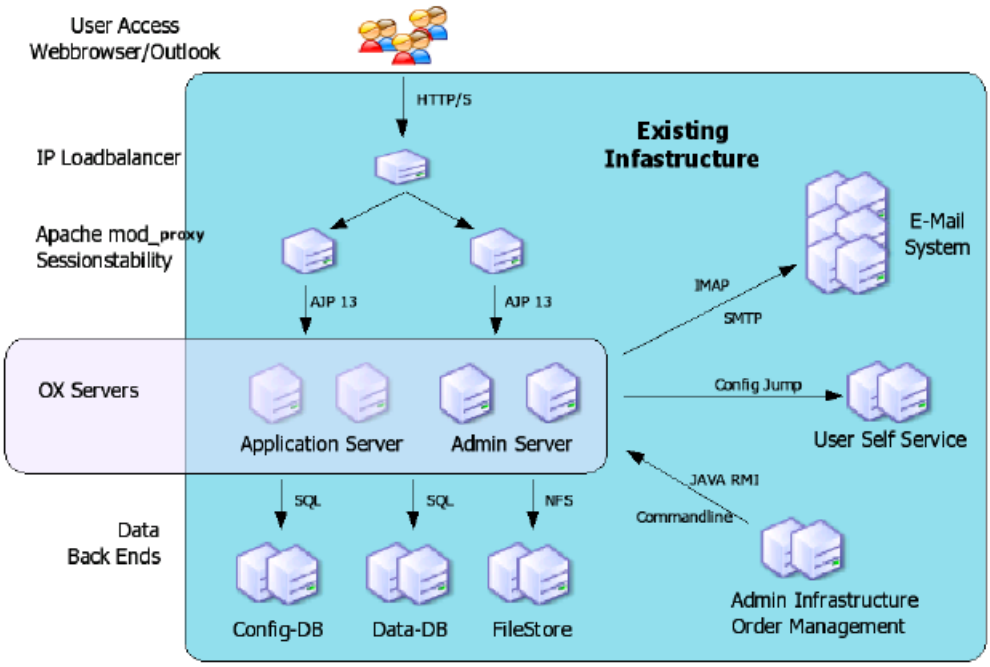


Abbildung 5.3: Verteiltest Open-Xchange-System[20]

- Listener-Mechanismus, der alle OX-spezifischen Änderungen im LDAP auf die Systemkonfiguration und OX-Datenbank repliziert
- sowie Anpassungen an der Postfix-, Cyrus-, Sieve-, MySQL-Infrastruktur

Open Xchange ist zum großen Teil in Java programmiert. Daher muss SUN Java 5 sowie mod_jk für den Apache installiert werden. Es ist empfohlen, auch die Apache-Module mod_deflate und mod_expires zu installieren, diese verbessern die Kommunikation zwischen Browser und Webserver. Außerdem wird der MySQL-Server 5 benötigt, welcher aber schon installiert wurde, da auch andere LAMP-Anwendungen (siehe 3.5.2) diesen benötigen. Open Xchange wird unterhalb von `/opt/open-xchange` abgelegt. Der Filestore, also der Bereich, in dem online Dokumente abgelegt werden können, ist auf Dateisystemebene unter `/var/oxfilestore` zu finden. Für eine genaue Installationsanleitung siehe auch [20]. Open-Xchange besitzt die Möglichkeit, User gegen einen LDAP zu authentisieren, jedoch nur die User. Dennoch werden alle anderen Daten wie Adressbuch, Aufgaben, Kalendereinträge, Zuordnung zwischen Filestoredatei im Web und auf dem Dateisystem, Rechte und so weiter intern in SQL-Tabellen gespeichert. Da unter UCS alle Daten im LDAP gespeichert werden, damit diese sowohl über die Web-GUI (Univention Directory Manager) zugänglich und administrierbar sind und auch

Clients, die LDAP-Adressbücher verwenden können (z. B. Mozilla Thunderbird), auf die Daten zugreifen können, musste ein Listener-Mechanismus entwickelt werden, welcher die Änderungen zwischen LDAP und MySQL syncronisiert. Das Webinterface, also die HTML-, CSS- und Javascript-Dateien sind unter `/var/www/ox6` abgelegt. Ein Apache Vhost wurde angelegt, damit die Webseiten unter `http://ox.horads.de` bzw. `http://ox.redaktionzukunft.de` erreichbar sind. OX ist in der Lage, mit mehreren IMAP-Servern umzugehen, sobald diese bestimme Voraussetzungen erfüllen (siehe Installationshandbuch), getestet wurden Cyrus IMAP, Courier und Dovecot. Die Integration nutzt den ausgewählten Cyrus-Server. Open-Xchange stellt für seine HE Updates bzw. Service Packs bereit. Zurzeit wird die OXHE Service Pack 4 eingesetzt. Ebenso wird UCS von Univention weiterentwickelt und Updates werden bereitgestellt. Die Updates müssen vor dem Einspielen auf gegenseitige Verträglichkeit getestet werden, was iKu übernimmt. Open Xchange ist noch erweiterbar, zum einen wäre ein eigenes oder ein anderes Authentication Plug-In denkbar, dass SSO an der Weboberfläche möglich wäre (siehe Kapitel 6 und 8.2) zum anderen existiert das OSGi-Framework[1], es können Java Servlets programmiert werden sowie Widgets (z. B. von Netvibes) benutzt werden, auch die Weboberfläche kann an die eigenen Bedürfnisse bzw. Farben angepasst werden und es gibt Erweiterungen von OX, die z. B. eine Integration eines Instant-Messenger-Systems bieten[21].

Aus der Zusammenarbeit von Open Xchange, Univention und iKu Systems und Service ist mittlerweile die Open-Xchange Appliance Edition entstanden, welches ein speziell angepasstes UCS mit OX als fertige Lösung ist, und sich an kleine und mittlere Unternehmen wendet. Einige Funktionen, die UCS bietet, sind in der Appliance nicht enthalten. Die OX Appliance Edition ist eine Single-Server-Lösung, verteilte Strukturen, wie in Abb. 5.3 zu sehen, sind daher nicht möglich. In Kürze soll außerdem OX4UCS erscheinen, also eine Lösung, die der an der HdM ähnelt[2].

Die Open Xchange Integration in UCS ist als Open Source unter der GPLv2 freigegeben. Die iKu Systems & Services übernimmt das Weiterentwickeln und Maintainen der Lösung auch weiterhin. Die HdM ist damit einer der ersten Anwender von Open Xchange Server Edition sowie von OX4UCS[22].

[1] Das OSGi-Framework stellt ein Plug-In-Konzept auf Basis von SOA und Java zur Verfügung siehe `http://de.wikipedia.org/wiki/OSGi`

[2] Open Xchange stellt eine Produktmatrix zur Verfügung, welche die Unterschiede erklärt und welche Variante für wen geeignet ist. siehe `http://www.open-xchange.com/fileadmin/downloads/matrix_oxae_oxforucs_oxse_oxhe.pdf`

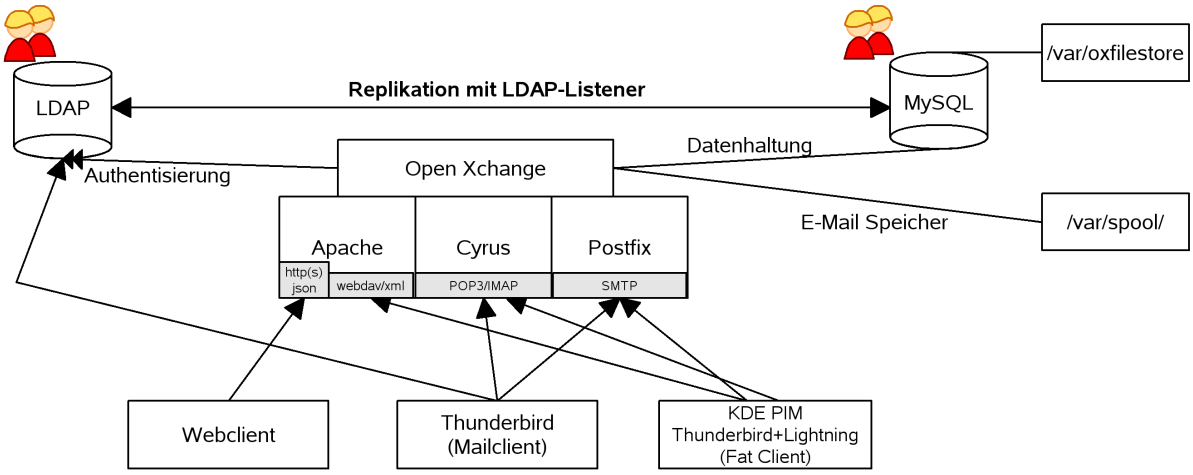


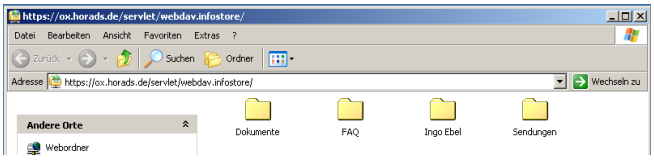
Abbildung 5.4: Schematische Darstellung OX4UCS mit Clients, die im CMC eingesetzt werden

5.4 Betrieb und Nutzung von Open Xchange

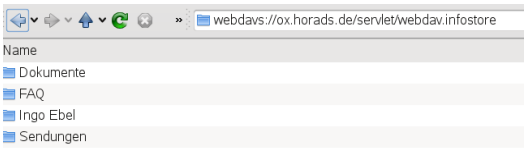
OX wird an erster Stelle zur E-Mailkommunikation eingesetzt. Open Xchange ist Multi-Domain-fähig, daher werden alle E-Mail-Domains, also convergentmedia.de, redaktion-zukunft.de und horads.de, in der Groupware verwendet. Mailinglisten, sprich mehrere Empfänger hinter einer E-Mailadresse, sind möglich und werden verwendet. Weiterhin werden natürlich die typischen Groupwarefunktionen wie Kalender und Kontaktverwaltung genutzt, jeder OX-Teilnehmer für sich sowie einige Gemeinschaftskalender, dazu zählt z. B. der Sendeplanungskalender von HoRadS. HoRadS nutzt die Groupware zur kompletten Sendeplanung, der CvD des CMC nutzt die Kalender zur Tagesplanung/Redaktionsplanung. Stark genutzt wird außerdem die Dokumentenverwaltung, die OX Infostore getauft hat. Damit ist der Datenaustausch zwischen den Redakteuren, Hochschulen und anderen Institutionen möglich. Auch wird ein Beitrags- und Sendearchiv verwaltet. FAQs, Bookmarks und andere Dokumente werden in den Infostores abgelegt, besonders geschickt ist dabei die eingebaute Versions- und Änderungskontrolle.

Infostores

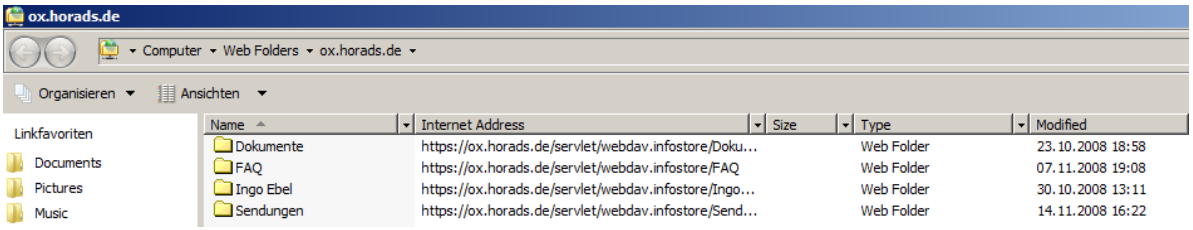
Die Infostores können auf verschiedenen Betriebssystemen einfach eingebunden werden, ein Umweg über die WebGUI ist nicht nötig. Dafür werden die Infostores über WebDav eingebunden. WebDav ist ein offener Standard und eine Erweiterung des HTTP-Protokolls, um Dateien auch auf den Server hochladen zu können, da normalerweise HTTP nur eine Richtung kennt, nämlich vom Server zum Client (Browser). Wie die ein-



(a) Infostore in Windows XP



(b) Infostore auf Linux mit KDE Konqueror



(c) Infostore in Windows Vista

Abbildung 5.5: Infostore über SSL auf verschiedenen Systemen

zelnen Clients einen WebDav Infostore einbinden können, ist dem Open Xchange Benutzerhandbuch[3] zu entnehmen. Damit Windows Vista auf WebDav zugreifen kann, ist ein Software-Update nötig, welches sich unter http://support.microsoft.com/kb/907306 abrufen lässt. Da die Verbindungen über HTTP nur verschlüsselt erfolgen sollten (der Apache erzwingt dies sogar), damit kein Passwort und keine Daten im Klartext durchs Internet transportiert werden, muss statt dem http:// oder webdav:// wie im Handbuch angegeben https:// oder webdavs:// geschrieben werden. Außerdem muss bei Windows XP/Vista noch das Cacert-Root-Zertifikat importiert werden, da die Verbindung sonst nicht zu Stande kommt. Wenn das Zertifikat von einer Stelle ausgestellt ist, die in Windows schon enthalten ist, ist dieser Schritt nicht nötig. Sowohl das Class-1- als auch das Class-3-Zertifikat, welches unter http://www.cacert.org/index.php?id=3 zu finden ist, sollte heruntergeladen werden und im Windows Explorer doppelt angeklickt und installiert werden. Danach können die Infostores, wie in Abb. 5.5 zu sehen ist, benutzt werden. Der einzige Nachteil bei dieser Lösung ist, dass nur die aktuelle Version der Dateien angezeigt wird, wird eine Datei gelöscht, wird die komplette Datei mit allen Versionen vernichtet. Wird ein vorheriger Version benötigt, bleibt nur der Weg über die WebGUI.

[3]Download unter: http://software.open-xchange.com/OX6/doc/OXHE-User-Manual-German.pdf

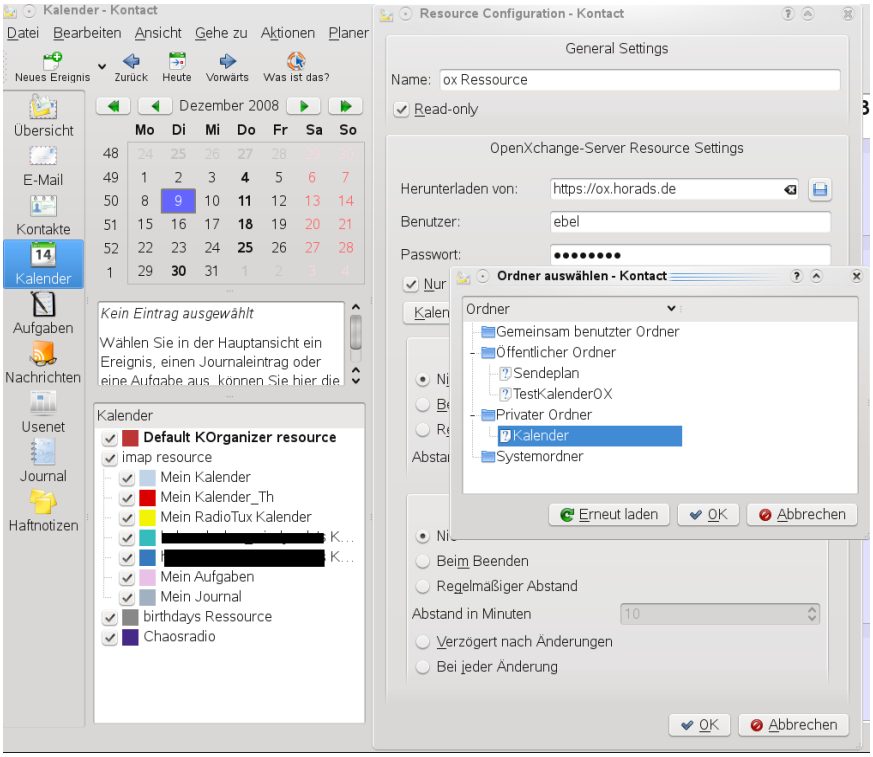
Kalender/Kontakte über WebDav

Nicht nur die Infostores sind über WebDav ansprechbar, sondern auch Kalender und Kontakte. So lassen sich Clients wie Thunderbird mit dem Plugin Lightning[4] oder die KDE-PIM-Suite Kontact[5] anbinden. Kontact bringt die nötigen Einstellungen selbst mit, es muss nur Open Xchange ausgewählt werden, bei Thunderbird lässt sich für den Kalender die URL `https://ox.horads.de/servlet/webdav.ical` wählen. Kontakte lassen sich über die URL `https://ox.horads.de/servlet/webdav.vcard` ansprechen. Großer Wermutstropfen dabei ist, dass zurzeit bei OX HE/SE nur die Möglichkeit besteht, lesend darauf zuzugreifen. Hoffentlich ändert sich das bald. Dass es möglich ist, auch schreibend auf die Kalender und Kontakte zuzugreifen, zeigt der seit kurzem verfügbare OXtender für Mac OS X[6] siehe Abb. 5.6. Dieser kann den Infostore einbinden, Kontakte, Kalender und Aufgaben zwischen dem Mac-OS-X-Adressbuch und iCal synchronisieren. Damit können diese selbst auf iPhones oder Geräte/Smartsphones synchronisiert werden, die mit den Mac synchronisieren können. Noch besser ist aber ein Abgleichen über die Luft, z. B. über SyncML, siehe Abschnitt 8.6.

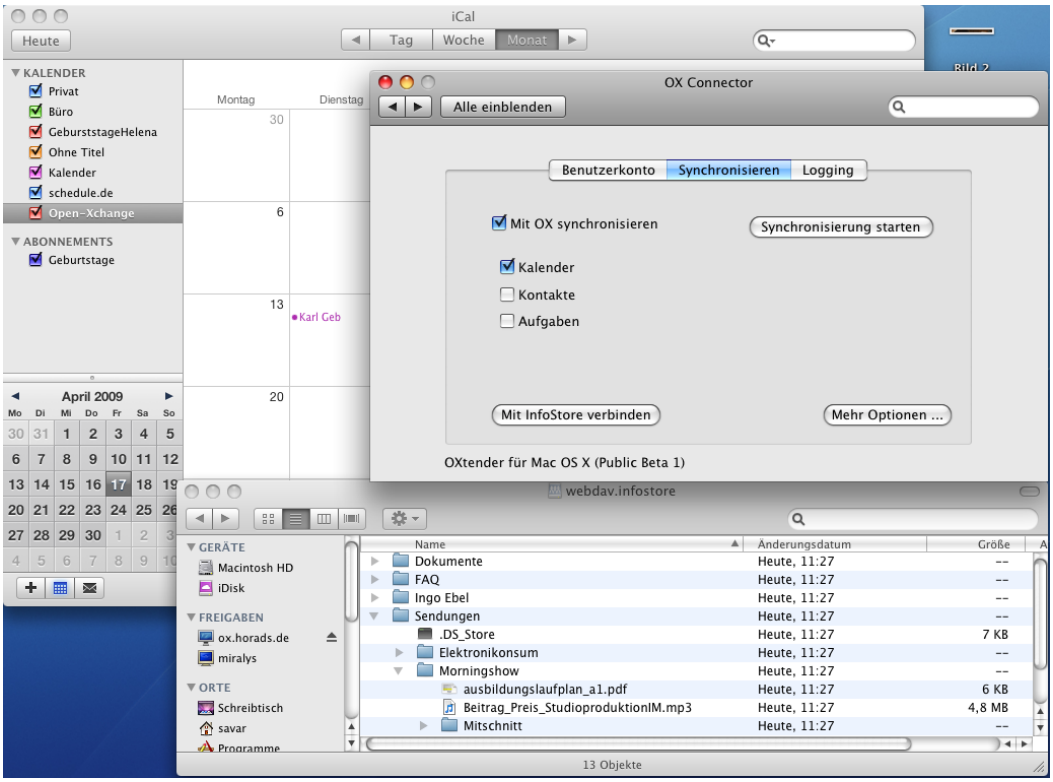
[4] Lightning ist eine Kalender Komponete für Mozillas Thunderbird siehe: `http://www.mozilla.org/projects/calendar/lightning/`

[5] die KDE PIM Komponenten sind in KDE enthalten, hier gibt es spannende Entwicklungen gerade durch den PIM Storage akonadi siehe `http://pim.kde.org/` und `http://radiotux.de/interviews/2008-05-30.RadioTux.Till.Adam.akonadi.linuxtag.mp3`

[6] siehe `http://www.open-xchange.com/oxpedia#MacOXtender`



(a) Kalendereinstellungen auf KDE PIM (Kontact)



(b) Kalender und Infostore und MacOS X

Abbildung 5.6: Kontakt- und Kalenderverwaltung

6 Single Sign On

Single Sign On (SSO) bedeutet, dass sich ein User nur ein Mal mit seinem Usernamen und Passwort authentisieren muss und danach mehrere unterschiedliche Dienste nutzen kann. Single Sign On ist zu einem Buzzword geworden, da heutzutage jedes große Unternehmen versucht, Single Sign On zu benutzen, meist werden dazu sogenannte Portale (vgl. [36]) eingesetzt, die unternehmensweit betriebliche Prozesse vereinen. Auch im Internet gibt es Portale (z. B. web.de, yahoo.com, bahn.de), die eine Reihe von Diensten anbieten.

Es gibt im Wesentlichen drei unterschiedliche Lösungsansätze[39]:

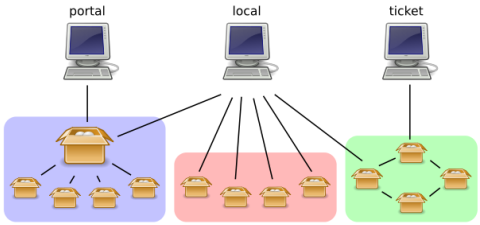


Abbildung 6.1: Lösungsansätze für SSO[39]

- *Portallösung:* der Benutzer loggt sich auf einem Portal ein und bekommt Zugriff auf alle eingebundenen Dienste
- *Lokale Lösung*: Es wird ein Client installiert, der die Login-Masken für verschiedene Dienste ausfüllt. Dieser hat in einer Datenbank zu jedem Dienst den richtigen Benutzernamen und Passwort. Ein User muss sich nur noch an diesem Client authentisieren. Die Daten können dabei in einer verschlüsselten Datei liegen, wie es z. B. beim Browser Mozilla Firefox der Fall ist, auf einer Smartcard (Hardware Security Module) oder es wird eine Appliances eingesetzt, die diese Aufgabe übernimmt.
- *Ticketlösung*: Ein Netz aus vertrauenswürdigen Diensten wird aufgebaut. Meist wird einer dritten Partei vertraut, die die Authentisierungen vornimmt (Trusted Third Party). Ein Beispiel dafür ist Kerberos, siehe auch Abschnitt 8.2.

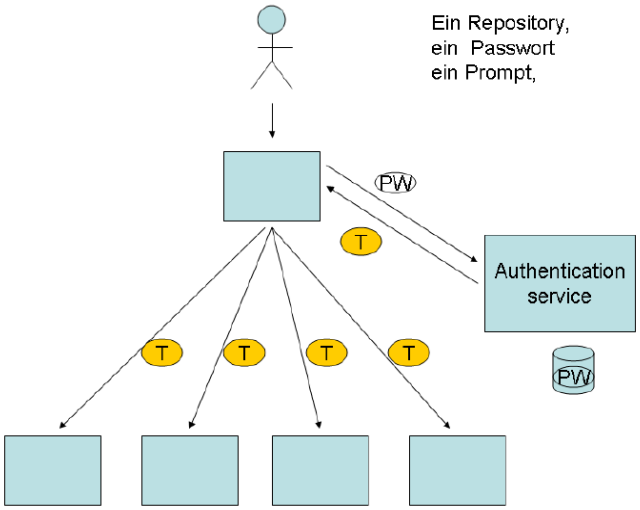


Abbildung 6.2: SSO mit Tickets bzw. Token[17]

Jede dieser Lösungsansätze hat unterschiedliche Vor- und Nachteile. Bei der lokalen Lösung ist der Pflegeaufwand deutlich höher, da die Benutzernamen und Passwörter nicht synchron gehalten werden. Jeder einzelne Dienst hat eine extra Userverwaltung. Eine solche Lösung wird meist zu Legacy-Zwecken verwendet, also wenn viele Altsysteme bestehen, die nicht an ein Ticketsystem angebunden werden können. Zu bevorzugen ist jedoch auf Grund der besseren Wartbarkeit ein System auf Basis von Tickets, bei der es nur ein Repository gibt, welches verwaltet werden muss.

SSO im Internet

Ein interessante Lösung für SSO im Internet könnte OpenID (http://openid.net/) werden. OpenID ist ein offener Standard und jeder kann OpenID-Provider werden. Ein User muss sich nur bei einem OpenID-Provider anmelden und kann in der Folge theoretisch, d. h. wenn die verschiedenen Provider sich untereinander vertrauen, viele Dienste bei anderen Providern nutzen. Dieses Verfahren basiert auch auf Trusted Third Party sowie Delegation (vgl. [18] Kapitel 6.3). Mittlerweile wird OpenID auch von großen Providern wie Yahoo!, IBM, Google und Microsoft unterstützt.

6.1 Vor- und Nachteile von SSO

Vorteile von SSO allgemein sind die Sicherheitszugewinne wie z. B., dass ein Passwort nur einmal eingegeben werden muss und ggf. auch nur einmal übertragen wird. Statt einer Vielzahl an meist unsicheren Passwörtern müssen sich die User nur noch ein Passwort merken, das auch komplexer sein kann. Dies ist wiederum auch ein Vorteil für die User, die nicht mehr von vielen Passwortabfragen in ihrem Arbeitsablauf gestört werden. Nachteile ergeben sich, wenn es einem Angreifer gelingt, die Identität eines Benutzers anzunehmen und damit Zugriff auf alle Dienste erlangt. Dies ist aber insoweit immer möglich, wenn es ihm beispielsweise gelingt, einen Keylogger auf dem Rechner des Benutzers zu installieren und somit alle Passwörter abzufangen. Ein weiterer großer Nachteil ist, dass ein Single Point of Failure (SPOF) geschaffen wird: fällt der SSO Dienst aus, können keine Anmeldungen mehr vorgenommen werden.

6.2 SSO im CMC

Single Sign On wird noch nicht durchgängig benutzt. Zwar gibt es erste Ansätze wie in Abschnitt 6.2.2 erklärt, aber die meisten Dienste haben „nur“ eine LDAP-Anbindung. Damit ist eine zentrale Authentisierungsstelle geschaffen, ein User muss nur an einer Stelle sein Passwort ändern, welches dann sofort für die Windows-Domain-Anmeldung, für die Groupware und alle anderen Dienste funktioniert. Das spart Arbeit für den Admin, der nur noch eine Benutzerdatenbank pflegen muss und ist für den User angenehmer, da er sich nur noch eine UserID und Passwort zu merken braucht. Manchmal wird auch diese Methode schon als Single Sign On bezeichnet, jedoch eher fälschlicherweise. Trotzdem kann man mit diesem Beinahe-SSO, bei dem es nur ein Repository, aber immer noch mehrere Aufforderungen gibt (vgl. Abb. 6.3), das Passwort einzugeben, vorerst leben.

Richtiges Single Sign On einzuführen, also auch keine Legacy-Lösung, bei der die Usernamen/Passwörter von einer Clientsoftware bzw. Appliances immer automatisch ausgefüllt werden, erfordert einen höheren Aufwand. Die Technologien sind jedoch alle verfügbar. Mit OpenLDAP, Samba, Kerberos, Apache lassen sich SSO-Umgebungen erstellen. In Bezug auf ein SSO mit Windows als Client wird es aber erst mit dem Erscheinen von Samba 4 (vgl. 3.3) spannend, da dieser eine fertige Kombination von File- und Druckerdiensten für Windows, LDAP-Server und Kerberos sein wird, also eine vollständige Active-Directory-Umgebung. Im CMC werden leider keine Linux-Clients eingesetzt, hier wäre es wesentlich einfacher, die Anmeldung gleich über Kerberos zu machen und in der Folge mehrere Dienste zu verwenden. Mehr zu Kerberos allgemein

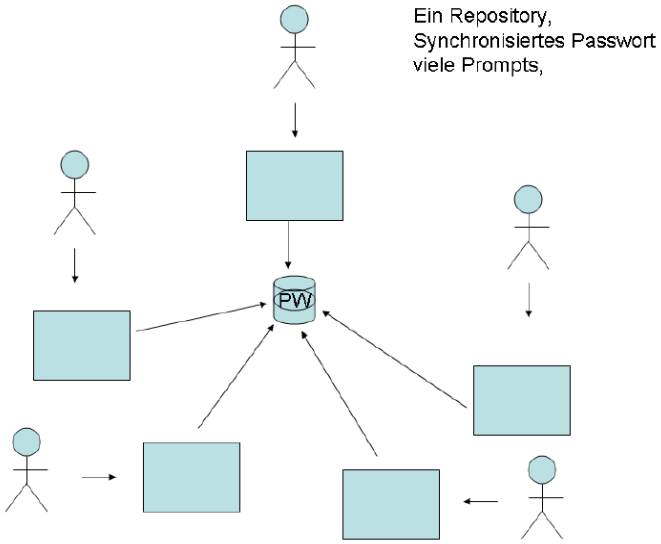


Abbildung 6.3: “SSO” an einem LDAP[17]

und zu weiterer Planung in diese Richtung für eine CMC-Infrastruktur, siehe das letzte Kapitel unter 8.2.

6.2.1 Mac OS X mit LDAP-Authentifikation

Im Medienbereich kommt oft Mac OS X zum Einsatz. Auch im CMC werden iMac und Mac Minis verwendet, aktuell mit OS X 10.5.5. Hier sollen wie bei den Windows-Clients auch keine lokalen User gepflegt werden sondern zentral über den LDAP. Daher ist eine LDAP-Anbindung von Mac OS X nötig[26].

Unter Mac OS X findet sich in den Dienstprogrammen ein Tool namens Verzeichnisdienst. Apple nennt seinen LDAP-Server Open Directory, es kann aber jeder LDAPv3-verstehende Server angebunden werden. Die erweiterten Einstellungen müssen eingeblendet werden. Dann kann unter Dienste der OpenLDAP-Server eingerichtet werden. Dazu muss LDAPv3 ausgewählt und der Stift zum Bearbeiten angeklickt werden, siehe Abb. 6.4. Damit das Mapping von Usern im LDAP zu Mac OS X richtig klappt müssen noch eigene Pfade eingetragen werden. Ist der LDAP-Server eingetragen, lassen sich über Bearbeiten im Tab Suche & Pfade Änderungen vornehmen. Bei „Zugriff auf diesen LDAPv3-Server über“ muss RFC 2307 (Unix) ausgewählt werden. Als Suchbeginn-Suffix muss die Base-Dn des LDAP-Servers eingetragen werden, also z. B. `dc=media,dc=hdm-stuttgart,dc=de`. Aufbauend auf diesen Einstellungen ist das Attribut von NFSHomeDirectory auf `#/Users/$uid$` geändert worden, siehe Abb. 6.5.

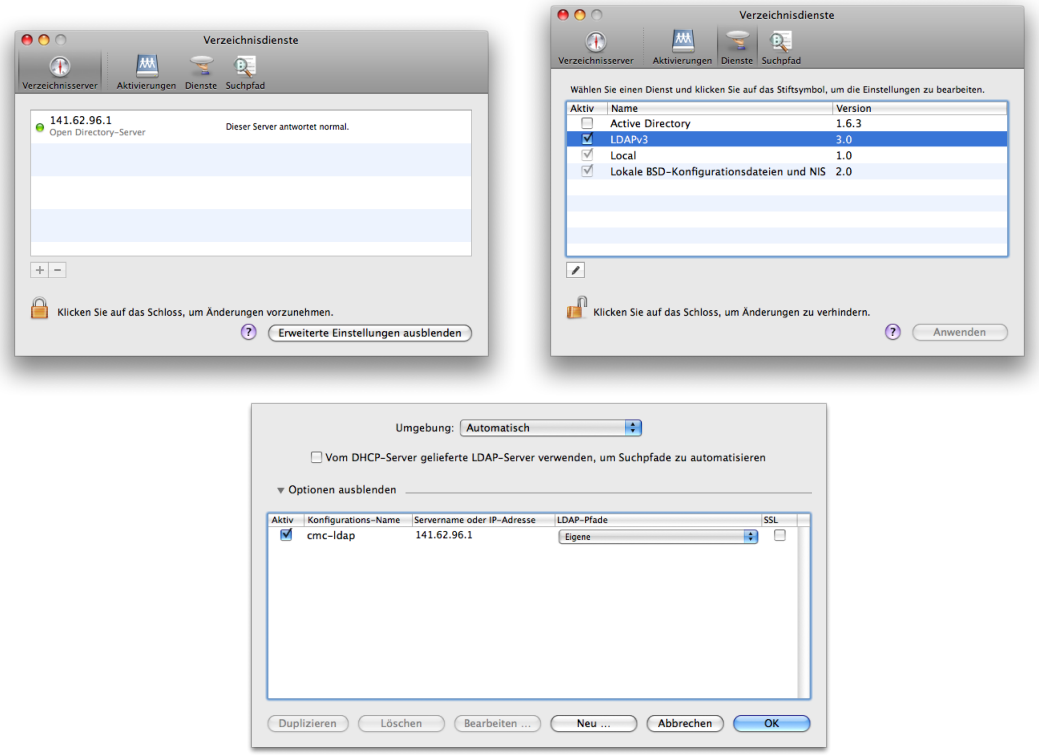


Abbildung 6.4: Mac OS X, Verzeichnisdienste-Programm

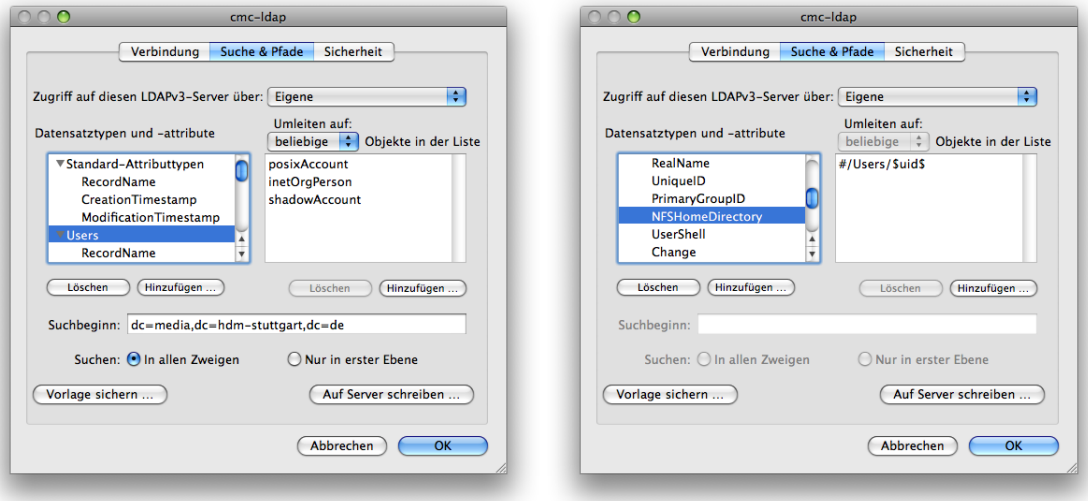


Abbildung 6.5: LDAP-Pfade konfigurieren für Mac OS X

Damit wird für jeden User der sich einloggt ein Verzeichnis auf der Festplatte erstellt, welches sich unter `/Users/Benutzername` befindet. Nachdem alles fertig eingerichtet ist, kann mit dem Kommando `dscl localhost` im Mac-OS-X-Terminal überprüft werden, ob die Verbindung zum LDAP-Server zu Stande gekommen ist, ob Zugriff auf die LDAP-Elemente besteht. Es besteht auch die Möglichkeit, den Usern, die sich einloggen, schon feste Elemente und Verknüpfungen auf den Desktop zu legen. Diese Einstellungen können unter `/System/Library/User Template/German.lproj/Desktop` vorgenommen werden.

Zukünftig sollen die Laufwerke auch über NFS gemapped werden und eine Integration mit Kerberos wäre wünschenswert.

6.2.2 SSO mit Apache und Firefox unter Windows

Damit aus Windows heraus mit einem Browser SSO benutzt werden kann, sind noch einige Schritte nötig. Das Apache-Modul `mod_auth_ntlm_winbind` nutzt das ursprünglich für den Proxy Squid entwickelte Programm ntlm_auth für die Authentifikation. Neben dem schon installierten Samba ist dafür noch das Paket winbind nötig, welches sich einfach mit `apt-get install winbind` installieren lässt. Mit `wbinfo -u` lässt sich testen, ob winbind User auflisten kann. Ist dies nicht der Fall, muss der Server noch einmal in die Domäne aufgenommen werden. Das Apache-Modul selbst lässt sich unter http://samba.org/ftp/unpacked/lorikeet/mod_auth_ntlm_winbind/ herunter-

laden oder kann per SVN[1] ausgecheckt werden. Für Debian und UCS existieren keine fertigen Pakte, bei den openSUSE-Distributionen lässt sich dieses Paket einfacher installieren. Das Modul muss selbst gebaut werden mit:

```
autoconf
./configure
apxs2 -DAPACHE2 -c -i mod_auth_ntlm_winbind.c
```

In dem Unterverzeichnis debian liegt eine Datei `auth_ntlm_winbind.load`, die nach `/etc/apache2/mods-available` kopiert werden muss. Danach kann das Modul mit `a2enmod auth_ntlm_winbind` aktiviert werden und der Apache2 muss neugestartet werden. Nun folgt die Konfiguration des Apache Vhosts, der für die Authentifikation benutzt werden soll. Dazu werden in der Directory Directive, also zwischen <Directory "/pfadname>...</Directory>, die Authentifikations-Parameter angegeben:

```
AuthName "NTLM Authentication"
NTLMAuth on
NTLMAuthHelper "/usr/bin/ntlm_auth --helper-protocol=squid-2.5-ntlmssp"
NTLMBasicAuthoritative on
AuthType NTLM
require valid-user
```

Dies kann allerdings auch über sogenannte .htaccess-Dateien für einzelne Verzeichnisse geschehen. Danach müssen noch einige Rechte richtig gesetzt werden mit `chmod 750 /var/run/samba/winbindd_privileged`. Außerdem sollte der User, unter dem der Apache läuft, also meist www-data, in die Gruppe winbindd_priv aufgenommen werden. Mehr Infos zum Einrichten finden sich auch unter http://adldap.sourceforge.net/wiki/doku.php?id=mod_auth_ntlm_winbind. Als Letztes muss noch der Client konfigurieret werden, hierzu ruft man im Firefox in der Adressleiste `about:config` auf und trägt unter dem Parameter `network.negotiate-auth.trusted-uris` die Domain oder IP des Servers ein. Der Internet Explorer kann ebenfalls über diese Methode authentifizieren. Mit dieser Methode können selbst Programme wie die Monitoring-Suite Nagios (vgl. [2] S. 661 – 668) oder die E-Learning-Plattform Moodle[2] angebunden werden und es ist kein weiterer Login mehr nötig.

[1] svn co svn://svnanon.samba.org/lorikeet/trunk/mod_auth_ntlm_winbindmod_auth_ntlm_winbind

[2] siehe: http://docs.moodle.org/en/NTLM_authentication#Using_the_NTLM_part_of_Samba_.28Linux.29

7 Open Source Software auf den Clients

Auch wenn das Thema dieser Thesis den Schwerpunkt auf die Serverlandschaft legt, soll kurz eine Betrachtung der Open-Source-Software auf den Client eingeschoben werden und warum diese Software überhaupt zu bevorzugen ist.

Open Source bzw. Freie Software[1] erlangt immer größere Bedeutung. So benutzen viele Menschen mittlerweile den Webbrowser Firefox, ohne zu wissen, welche Rechte ihnen dabei eingeräumt werden. Diese Art Software beeinflusst heute maßgeblich den Zugang zu Kommunikation aber auch Bildung und Arbeit. Meist werden die Programme natürlich aus dem Grund heraus benutzt, weil diese in aller Regel kostenlos abgegeben werden und man diese einfach aus dem Internet herunterladen kann. Bei Freier Software steht das „Frei“ aber nicht für den Preis, sondern für Freiheit. Um das Zitat von Richard M. Stallman, dem Gründer der Free Software Foundation, zu benutzen „Free as in Free Speech, not as in Free Beer“[9]

Dadurch ergeben sich eine ganze Reihe von Nutzungsrechten, die auch die 4 Freiheiten genannt werden:

- Die Freiheit, das Programm zu jedem Zweck zu verwenden
- Die Freiheit, zu studieren wie die Software funktioniert und es für eigene Zwecke anzupassen
- Die Freiheit, Kopien des Programmes herzustellen und es zu verbreiten
- Die Freiheit, das Programm zu verbessern und diese Verbesserungen zu veröffentlichen, damit alle davon profitieren

Im Convergent Media Center werden eine ganze Reihe von Programmen eingesetzt, die diese Freiheiten bieten, unter anderem die Office-Suite OpenOffice.org. Diese wurde zum einen gewählt, um die Kosten zu drücken, was wie oben schon erläutert natürlich oft ein

[1] Auch wenn man Grenzen zwischen der Open-Source- und der Freie-Software-Bewegung ziehen kann, werden diese beiden Begriffe synonym verwandt. Open Source stellte mehr das überlegene Entwicklungsmodell und den offengelegten Quelltext heraus, während bei Freier Software die Freiheit herausgestellt wird. [33]

Hauptgrund ist. Im Gegensatz zu Microsoft Office, das auch in einer Studenten-/Lehr-Version immer noch mehrere Hundert Euro kostet, ist OpenOffice.org einfach aus dem Internet zu laden, Updates erscheinen regelmäßig und die Installation ist um ein Vielfaches schneller, außerdem entfällt eine lästige Registrierung und Aktivierung der Software. Ein weiterer Grund war auch, dass Microsoft mit MS Office 2007 ihr Bedienkonzept komplett umgestellt hat auf sogenannte Ribbons, das Konzept mag für Personen, die noch nie mit einer Office-Suite gearbeitet haben durchaus leichter zu verstehen sein, die Studierenden, sind jedoch eher mit einer klassischen Bedienung einer Office-Suite vertraut. Zudem haben Studenten heutzutage oft auch schon Erfahrungen mit OpenOffice gesammelt, und falls nicht, kann ihnen die Software zur Verfügung gestellt werden, damit sie diese auch daheim nutzen können, dies zur Not sogar in vielen verschiedenen Sprachen. Ein weiterer Punkt ist, dass OpenOffice.org plattformübergreifend verfügbar ist, so läuft es unter verschiedenen Windows-Versionen, unter Mac OS X, aber auch unter Linux bzw. anderen Unices, für Windows steht auch eine Portable-Version zur Verfügung; damit kann OpenOffice.org auf einem USB-Stick installiert und von dort benutzt werden, der User hätte also ein eigens angepasstes OpenOffice.org immer dabei. Im CMC selbst gibt es sowohl Windows Vista, Windows XP als auch Mac OS X. Studenten können aber auch ihren eigenen Laptop mitbringen und daran arbeiten. Damit ist der Datenaustausch zwischen allen Plattformen gegeben. Studenten, die auf Ihren Rechnern Microsoft Office einsetzen, können entweder OpenOffice.org dazu installieren oder ein Plug-In verwenden, um Dokumente im OpenDocument-Format zu speichern[2]außerdem sollen künftige Microsoft-Office-Versionen mit dem Dateiformat umgehen können[3]. Der letzte Punkt ist damit auch das OASIS Open Document Format for Office Applications[34] (kurz: OpenDocument), welches einen offenen Standard für Dateiformate von Bürodokumenten wie Texten, Tabellendokumenten, Präsentationen, Zeichnungen, Bildern und Diagrammen darstellt. Viele Programme benutzen mittlerweile das OpenDocument-Format als Standard zum Speichern oder können es zumindest lesen und schreiben, viele öffentliche Stellen setzen es mittlerweile ein oder akzeptieren es[4]. Das Format wurde durch die ISO (International Organization for Standardization) als Standard spezifiziert und 2006 als internationale Norm ISO/IEC 26300 veröffentlicht und setzt auf XML auf, dadurch ist es für die Zukunft gerüstet, da XML keine Binärdaten sind sondern zur Not auch von Menschen gelesen werden können. Durch die Standardisierung ist es jedem Programm-

[2]siehe http://odf-converter.sourceforge.net/ für ein Projekt, welches auch von Microsoft unterstützt wird oder http://www.sun.com/software/star/odf_plugin/index.jsp für ein von Sun Microsystems vorangetriebenes Projekt

[3]siehe http://www.microsoft.com/Presspass/press/2008/may08/05-21ExpandedFormatsPR.mspx

[4]siehe http://de.wikipedia.org/wiki/OpenDocument

Name	Zweck	Link
7Zip	Packen und Entpacken von Archiven	http://www.7-zip.org
audacity	Audioschnitt/Soundbearbeitung	http://audacity.sf.net
Filezilla	FTP Client	http://filezilla-project.org/
Mozilla Firefox	Webbrowser	http://mozilla.com
Mozilla Thunderbird	Mailclient	http://mozilla.com
OpenOffice.org	Bürosuite, Textverarbeitung, Tabellenkalkulation ...	http://de.openoffice.org
VLC	Medienabspieler (MP3, MPEG, DVDs etc.)	http://videolan.org

Tabelle 7.1: Links zu eingesetzter Software

autor möglich, einen Import- oder Export-Filter für eigene Programme zu schreiben[5]. Die XML-Dateien werden zu einer ZIP-Format-Datei zusammengefasst und sind damit erheblich kleiner als die alten Microsoft-Formate.

Im CMC ist der Mozilla Firefox der Standardbrowser, er verfügt im Gegensatz zum Internet Explorer aus dem Hause Microsoft über eine bessere Unterstützung von Webstandards wie CSS, bietet zahlreiche Erweiterungen.

Für den Audioschnitt wird unter anderem das Programm Audacity verwendet. Es bietet alle grundlegenden Funktionen eines Soundbearbeitungsprogrammes wie Audioschnitt und mehrere Filter wie Rauschunterdrückung und Kompressor. Es ist im Gegensatz zu anderen Produkten einfacher zu erlernen und wie bei den anderen Programmen bietet es die Vorteile Freier Software wie Plattformunabhängigkeit. Audacity hat aber auch einige Schwächen und bietet nicht alle Funktionen, die gebraucht werden, daher ist es nicht das einzige Audioschnittprogramm, das auf den Rechnern installiert ist.

Als Standardmedienplayer wird der VideoLanClient (kurz: VLC) eingesetzt, zum Entpacken der verschiedensten Archivformate wie zip, rar und Co. wird 7zip verwendet, für die Übertragung von Daten über das FTP-Protokoll wird Filezilla benutzt. Als Mailclient kommt der Mozilla Thunderbird zum Einsatz. Dies ist eine Auswahl von Programmen, die unter einer Open-Source-Lizenz stehen. In der Tabelle 7.1 sind die Programme mit ihrem Zweck und der Webseite zusammengestellt.

[5] OpenDoument wird innerhalb der OASIS entwickelt, welche Entwicklung der Standard nimmt und wie er aussieht, ist unter http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office zu finden.

8 Zukunft/Mögliche Anschlussprojekte

Im letzten Kapitel soll noch mal ein Überblick gegeben werden, welche Projekte noch aufgegriffen werden können. Zwar ist ein lauffähiges System entstanden, das die Aufgaben, die an es gestellt werden, erfüllt, jedoch sind noch Punkte ungeklärt und benötigen weitere Betrachtung. Auch wird das System bei steigenden oder anderen Aufgabenstellungen angepasst werden müssen. Diese Zukunftsprojekte haben auf keinen Fall den Anspruch auf Vollständigkeit, es wäre auch kaum schaffbar, alle Ideen in diesem Kapitel zu behandeln.

8.1 Sicherheit

Zwar sind grundlegende Sicherheitsaspekte berücksichtigt worden, jedoch ist es empfehlenswert, hier noch zusätzlich Arbeit zu investieren. Jeder offene Port kann grundsätzlich ein Angriffspunkt sein. Der SSH-Server ist dabei sicher noch das geringste Problem, da er nur über Keys authentifiziert und noch wie einige andere Dienste auch mit Fail2Ban[1] geschützt ist. Auch schützt die HdM-Firewall vor gängigen Angriffen, jedoch geschehen heute viele Angriffe auf den Webserver (Apache) selbst, der offen im Netz steht. So sind Angriffe wie XSS (Cross-Site Scripting) möglich, auch durch die Verwendung von AJAX bei OpenXchange sind neue Angriffstypen denkbar. Für diese Art von Angriffen hilft es nur, das System noch stärker abzudichten, um einen Ausfall oder im schlimmsten Fall auch ein Kompromittieren des Systems zu verhindern. Hier zählen z. B. der Einsatz von speziell gehärtetem, abgedichtetem PHP[2], der Einsatz von SE Linux oder AppArmor sowie von Web Application Firewalls[3]; diese könnte man mit einem extra Apache-Modul names mod_security[4]der Firma Breach realisieren.

Neben Firewalls, die bestimmte Dienste schützen, sollte trotz der Firewall, die die HdM vor der Außenwelt abschottet, trotzdem noch eine Firewall auf den Servern installiert werden, denn vor internen Angriffen oder auch nur falsch konfigurierten oder

[1] Bei mehr als 5 falschen Einlogversuchen wird die IP des „Angreifers“ per Firewall/Iptables-Regeln gesperrt. Mehr Infos unter: http://www.fail2ban.org/
[2] siehe: http://www.hardened-php.net/
[3] kurz WAF: http://de.wikipedia.org/wiki/Web_Application_Firewall
[4] http://www.modsecurity.org/

infizierten Rechnern sind die Server noch nicht ausreichend geschützt. Auch könnte über ein Intrusion Detection System (IDS) nachgedacht werden wie z. B. snort, jedoch sollten eher Firewalls und andere Methoden möglichst viel Schutz bieten, denn ein IDS kann erst Alarm schlagen, wenn der Angreifer schon einen Weg ins System gefunden hat.

Auch kritisch zu beleuchten ist, dass bei einigen Diensten noch ein Fallback auf unverschlüsselte Authentifizierung möglich ist. So können sich die User zwar nicht mehr unverschlüsselt über das Webinterface am OX anmelden, jedoch können sie mit einem E-Mail-Client per IMAP/POP/SMTP noch unverschlüsselt kommunizieren, auch bei FTP ist es möglich, sich unverschlüsselt zu verbinden. Zwar sind alle Dienste auch in einer SSL/TLS-Verbindung ausgestattet, aber diese Verbindung wird nicht erzwungen. Dies ist natürlich zurzeit noch der Einfachheit halber so gehalten, viele User verstehen auch die Verschlüsselung nicht und wissen überhaupt nicht, dass ihr Passwort und alle Daten, die sie austauschen, theoretisch von vielen Personen eingesehen werden können. Hier wäre es nötig, die User zu schulen, damit diese den Unterschied verstehen und die Notwendigkeit sehen, warum die unverschlüsselten Dienste nicht mehr angeboten werden.

8.2 Kerberos

Wie schon im Kapitel 6 ausgeführt, ist nur ein simples Single Sign On zurzeit benutzbar. Alles wird gegen LDAP authentifiziert. Es geht aber auch besser, und zwar mit Kerberos. Kerberos ist ein verteilter Authentifizierungsdienst, der für offene und unsichere Netze konzipiert worden ist, er ermöglicht Single Sign On und ist plattform- und systemunabhängig. Der Kerberos Network Authentication Service (V5) ist in RFC 4120[5] beschrieben. Auf dem Server sind LDAP und Kerberos[6] bereits installiert, damit ist es auch möglich, ein richtiges SSO zu fahren. Statt sich also an mehreren Diensten immer einloggen zu müssen, kann das auch über Kerberos geschehen. Kerberos kann die Informationen wie Benutzername und Passwort ebenfalls aus dem LDAP ziehen. Wie in Abbildung 6.2 schon zu sehen, geschieht die Authentisierung und ggf. Autorisierung über einen Authentisierungs-Server, der bei Kerberos Key Distribution Center (KDC) genannt wird; dies ist die gemeinsame Vertrauensbasis aller Clients. Ein Client authentifiziert sich bei diesem KDC und erhält ein Authentisierungs-Token, bei Kerberos Ticket genannt, welches zur Authentisierung innerhalb einer Kerberos-Umgebung verwendet

[5] Request for Comments: ftp://ftp.rfc-editor.org/in-notes/rfc4120.txt
[6] eingesetzt wird die Heimdal-Kerberos-Implementierung, es gibt auch andere Implementierung wie z. B. vom MIT

werden kann. Zu dem genauen Verfahren und kryptographischen Hintergründen siehe [18] Seite 129 - 137.

Mit Kerberos ist es also möglich, dass ein User nach seiner Anmeldung am Windows-Rechner und einer Generierung eines Kerberostickets mehrere Dienste/Services sofort verwenden kann, ohne sich an einer anderen Stellen noch mal authentisieren zu müssen. So können beispielsweise Mozilla Thunderbird und Mozilla Firefox Anmeldungen über Kerberos abwickeln. Die Passwörter müssen nicht mehr lokal im Browser oder Mailclient gespeichert werden, sondern die Authentisierung erfolgt über Kerberos, was zu einer erhöhten Sicherheit führt, da das Kennwort nur bei der Windowsanmeldung eingegeben werden muss und danach weder auf der Festplatte gespeichert liegt noch nocheinmal über der Netzwerk transportiert werden muss. Hierfür wäre es nötig, dem Webserver Apache[7] oder anderen Diensten wie dem unter 3.7 erwähnten proftpd[8] nicht nur LDAP-Unterstützung, sondern auch Kerberos-Unterstützung beizubringen. SASL unterstützt schon das Generic Security Services Application Program Interface (GSSAPI), damit wäre es möglich, Kerberos zu nutzen, die Login-Mechanismen müssten für die E-Mail-Kommunikation noch dem Postfix bzw. Cyrus bekannt gemacht werden.

8.3 Ausbau Netz auf Glasfaser oder 1000MB Ethernet

Das Convergent Media Center ist aus heutiger Sicht nicht mehr optimal angebunden. Da es geographisch weit weg vom Rechenzentrum der HdM ist, liegen keine Glasfaserleitungen bis in diesen Raum, noch ist das Netz auf Gigabit-Ethernet ausgerichtet. Um dies zu erreichen, ist ein Umbau der Netzverkabelung im Haus nötig und ggf. neue Swichtes. Die Rechner im Newsroom sind bereits in der Lage, mit Gigabit-Ethernet umzugehen, ebenso die meisten Laptops werden heute mit einer Gigabit-Ethernet-Netzwerkkarte geliefert, auch die Server haben On-Board-Netzwerkkarten, die mit dieser Geschwindigkeit umgehen können.

Da im CMC mit vielen Daten gearbeitet wird und auch Videos mit mehreren Gigabyte an Daten produziert werden, kommt die Verbindung zum Server sehr schnell an ihre Grenzen. In einer der nächsten Semesterferien sollte hier der Ausbau beginnen, um zukünftige Engpässe zu vermeiden.

[7] Kerberos Modul für Apache-Webserver siehe: http://modauthkerb.sourceforge.net/
[8] Kerberos Unterstützung für proftpd: http://gssmod.sourceforge.net/

8.4 Automatische Software-Verteilung

Windows bietet im Gegensatz zu Linux-Distributionen kein einheitliches Softwarerepository, mit dem sich Software schnell installieren und bei Bedarf updaten lässt, um ggf. Sicherheitslücken zu schließen. Jede Software muss einzeln installiert werden, es kommen verschiedene Installationsroutinen zum Einsatz und so ist es bei einer Standardkonfiguration der Fall, dass jeder Rechner ein Unikat ist. Dieses klassische Modell nennt man „Management by Sneaker“ oder auch Turnschuhadministration, da der Admin von Rechner zu Rechner laufen muss und die Einstellungen selbst vornehmen. Bei dieser einfachen Technik entsteht aber ein großer Aufwand. der mit der Anzahl der zu betreuenden Rechner steigt, daher gibt es verschiedene Lösungen am Markt, die je nach Größe des Netzes unterschiedliche Funktionen haben (vgl. [15]).

Zur Zeit ist im CMC noch keine PC-Management-Lösung installiert, durch die zentrale Anmeldung über eine Windows-Domain können gewisse Aufgaben wie das Installieren von Programmen jedoch erledigt werden. Microsoft bietet seit Windows 2000 über den Windows-Installer, vormals Microsoft-Installer (MSI)[9], die Möglichkeit, eine Installation ohne Benutzerinteraktion durchzuführen. Wenn Software als MSI-Paket vorliegt, kann diese auf einem Netzlaufwerk abgelegt werden und bei der Anmeldung automatisch im Hintergrund („silent“) installiert werden. Diese Möglichkeit wird genutzt, um OpenOffice.org[7] und Firefox[10] zu installieren und ggf. auf einen neuen Versionsstand zu bringen. Die Installationsroutine von OpenOffice.org basiert auf MSI, nachdem das Setup aufgerufen wurde, werden alle Dateien in einen frei wählbaren Pfad entpackt, hier findet sich dann auch das entsprechende MSI-Paket. Die Installationsroutine kann abgebrochen werden. Das MSI-Paket kann mit verschiedenen Properties für Einstellungen aufgerufen werden, z. B. um den Installationspfad zu setzen, die zu installierende Komponenten auszuwählen oder die MS Office-Dateiverknüpfungen zu übernehmen, außerdem bietet OpenOffice.org über sogenannte XCU-Dateien (Registry Update Format als XML-Datei) nach der Installation die Möglichkeit, diese an die Bedürfnisse der Einsatzumgebung anzupassen. So können Einstellungen gesperrt werden, persönliche Einstellungen vorgenommen werden, Sicherheitsoptionen gesetzt werden und vieles mehr.[11]

```
msiexec /qn /norestart /i t:\oo.org\openofficeorg30.msi
    INSTALLLOCATION="C:\OOo" ADDLOCAL=ALL
```

[9] siehe: http://de.wikipedia.org/wiki/Windows_Installer

[10] Mozilla bietet Firefox nicht als MSI-Paket an. Bei Frontmotion gibt es jedoch ein entsprechendes Paket: http://www.frontmotion.com/Firefox/

[11] mehr Infos zu den verschiedenen Einstellungen unter: http://de.openoffice.org/doc/setupguide/2.0/netzwerkinstallation_windows.pdf oder im Admin Guide auf openoffice.org

Dies alles ersetzt jedoch keine richtige Softwareverteilung, bei der der Softwarestand für jeden einzelnen Computer erfasst sind, die Updates erkennen und einspielen kann, die auf ein Repository zugreifen kann, auf dem schon Software vorpaketiert liegt, die verschiedene Windows-Versionen unterschiedlich behandeln kann, Windows-Service-Packs und Security-Patches einspielen kann und so weiter. So hat Microsoft von Windows XP zu Windows Vista gravierende Änderungen vorgenommen, wie und wo Software installiert wird und wo Benutzerprofile gespeichert werden. Oft mischt sich auch die neue Benutzerkontensteuerung ein, bei der der User bestätigen muss, dass die Software auch gerade das darf, was sie möchte, d. h. wirkliche „silent“-Installationen werden schwieriger, auch fehlen den Usern, die sich einloggen, in der Regel die Rechte, überhaupt Software installieren zu können. Ebenso muss eine Softwareverteilung auch Profile für unterschiedliche Rechner kennen und nur nach diesen Regeln Software und Updates ausliefern.

All dies würde nach einer Anfangsinvestition und Einarbeitungszeit dem Administrator Arbeit sparen, ein Inventar bieten und die Sicherheit erhöhen, da Patches/Updates schneller auf die Rechner angewendet werden. Für das CMC wäre die Lösung OPSI (open - PC ServerIntegration) der Mainzer Firma uib[12] zu empfehlen. Diese Lösung arbeitet seit Kurzem auch mit Windows Vista zusammen und bietet eine Integration in das UCS-Management-System an (opsi4ucs). Die Software steht seit 2004 auch als Open-Source-Variante zur Verfügung. Der Support und die Windows-Vista-Anbindung kosten jedoch Geld. Eine Umsetzung könnte im ersten Halbjahr 2009 durchgeführt werden.

8.5 OpenVPN

FTP ist zwar für den Datenaustausch weitestgehend ausreichend, jedoch ist das Protokoll zum einen sehr kompliziert, zum anderen bleibt die Möglichkeit, dass die User den einfachen Weg nehmen und keine Verschlüsselung nutzen, dabei wird das Passwort im Klartext übers Internet übertragen und könnte missbraucht werden. Eine bessere und sichere Lösung wäre, eine OpenVPN-Verbindung aufzubauen. Da an der HdM für die WLAN-Authentisierung ebenfalls OpenVPN eingesetzt wird, kennen sich viele der User schon mit der Einrichtung aus. Es müsste also nur ein OpenVPN-Server geschaffen werden, die Konfigurationsdateien erstellt und an die User verteilt werden. Ideal wäre es hierbei, wenn ebenfalls das LDAP-Passwort zur Authentisierung[13] verwendet werden kann und dass nicht wie beim HdM-WLAN ein kompletter Zertifikatserstellungsprozess

[12] mehr Infos: http://www.uib.de bzw. http://www.opsi.org
[13] http://code.google.com/p/openvpn-auth-ldap/

programmiert werden muss.

Mit einer OpenVPN-Verbindung könnten die User Ihre Laufwerke dann normal mappen und müssten kein extra FTP-Programm verwenden, außerdem könnte der komplette IP-Verkehr zwischen dem PC des Users und dem Netzwerk des CMCs verschlüsselt werden, auch Druckdienste könnte man über diese Weise anbieten. So könnte man Außenreportern die Möglichkeit bieten, sofort auf die Infrastruktur zuzugreifen, ebenso könnten verschiedene Redaktionen vernetzt werden, z. B. an einer Partnerhochschule.

8.6 SyncML Funambol

PIM-Daten wie E-Mails, Kalender und Kontakte auf dem einen Server zu haben ist schön und gut, aber bei größeren Firmen als Außendienstler oder auch beim Radio als Außenreporter will man nicht immer einen Laptop mit sich herumschleppen, um auf diese Daten zuzugreifen, daher ist es nötig, diese mit verschiedenen Geräten zu synchronisieren. Viele der mobilen Geräte wie Handys können Daten mittels SyncML abgleichen, dabei ist egal, ob dies über Bluetooth (OBEX) oder über beispielsweise HTTP geschieht. SyncML[40] hat sich hier sozusagen als Standard durchgesetzt. Dieser basiert auf XML und wird unter dem Dach der Open Mobile Alliance entwickelt, in der Unternehmen wie Nokia, Palm, IBM, Motorola, Ericsson, Symbian und Lotus zusammengeschlossen sind. So können also alle Smartphones mit Symbian wie die vielen Nokia Telefone der Symbian-S60-Reihe mit SyncML umgehen. Microsoft geht mit seinem Windows CE/Windows Mobile einen anderen Weg und benutzt ActiveSync, welches besonders gut mit ebenfalls aus dem Hause Microsoft kommenden Exchange-Server und dessen Client Outlook funktioniert, aber auch hier existieren Plug-Ins.

Der Markt für mobile Geräte aus dem Bereich Smartphones wächst rasant, innerhalb eines Jahres um knapp 28 %[4]. Viele der Studenten und Professoren haben heute ein Smartphone oder ein Handy, auf dem E-Mail, Kalender und Kontaktdaten sich speichern lassen. Dies ist ein zurzeit höchst vitaler und interessanter Markt, in dem viele Innovationen stattfinden und der durch den Markteintritt von Apple 2007 und dem kürzlich vorgestellten ersten Smartphone auf Basis von Googles Andoid, dem T-Mobile G1 with Google[14], sowie dem komplett freien (hard- und softwaretechnisch) OpenMoko Freerunner[15] große Zukunftsperspektiven versprochen werden.

[14] siehe: http://www.heise.de/mobil/T-Mobile-G1-Der-Vorbote-einer-grossen-Android-Offensive--/newsticker/meldung/116428

[15] mehr zum Thema OpenMoko und Marktanalysen siehe: http://www.mynethome.de/BachelorThesis/BachelorThesis_OpenMoko.pdf und zum Thema Mobile-Plattformen allgemein der Audiopodcast unter: http://archiv.radiotux.de/sendungen/horads/2008-10-23.RadioTuxatHoRadS.mp3

Worldwide smart phone market
Market shares Q3 2008, Q3 2007

OS vendor	Q3 2008 shipments	% share	Q3 2007 shipments	% share	Growth Q3'08/Q3'07
Total	39,850,100	100.0%	31,156,240	100.0%	27.9%
Symbian	18,583,060	46.6%	21,219,390	68.1%	-12.4%
Apple	6,899,010	17.3%	1,107,460	3.6%	523.0%
RIM	6,051,730	15.2%	3,298,090	10.6%	83.5%
Microsoft	5,425,470	13.6%	3,797,360	12.2%	42.9%
Linux	2,028,490	5.1%	1,361,810	4.4%	49.0%
Others	862,340	2.2%	372,130	1.2%	131.7%

Source: Canalys estimates, © canalys.com ltd. 2008

Abbildung 8.1: Marktanteile von Smartphones

Eine stationäre Ausrichtung auf einen Client, wie bei vielen Unternehmen üblich Outlook, ist jedoch nicht mehr zeitgemäß. Zwar bringen viele Smartphones und PDAs die Möglichkeit mit, sich mit Outlook zu synchronisieren, aber dies geht eben nur, wenn das Gerät in der Nähe des Computers mit dem Client ist. Der Abgleich der Daten sollte aber immer funktionieren, das heißt „over-the-air“ mittels Internetverbindung, daher ist ein Synchronisations-Server nötig. Funambol bietet einen auf Open Source basierenden SyncML-Server[16] an, welcher sich einfach auf Linux-Servern installieren lässt. Funambol bietet außerdem für eine Reihe von Plattformen wie Apple iPhones und iPods, Google Android, RIM Blackberrys, Windows Mobile, Outlook und Java-ME-Telefone Konnektoren an. Telefone, die SyncML implementiert haben, können direkt mit dem Server kommunizieren. Im Oktober 2008 gaben die Unternehmen Funambol Inc. und Open-Xchange eine Zusammenarbeit bekannt[17]. Der Funambol-Server wird dann die Daten zwischen OX und den der mobilen Endgeräten abgleichen können, damit jederzeit auf E-Mail, Kontakte und Kalender von unterwegs zugegriffen werden kann. Funambol bietet ebenso die Möglichkeit, die Daten auf das Endgerät zu pushen, dabei ist dann keine User-Interaktion mehr erforderlich, neue E-Mails und Kontakte werden automatisch auf das Smartphone gebracht.

Sobald hier eine fertige, stabile Lösung existiert, kann dieses Thema angegangen werden.

[16] https://www.forge.funambol.org/download/
[17] http://www.open-xchange.com/de/node/601

Literaturverzeichnis

[1] Hans-Joachim Baader. Projekt Virtueller hochverfügbarer Linux-Server, Teil 5, 2007. http://www.pro-linux.de/work/virtual-ha/virtual-ha5.html abgerufen am 12.11.2008.

[2] Wolfgang Barth. *Nagios*. open source press, zweite edition, 2008.

[3] Dr. Christian Böttger. Groupware für linux, mar 2007. http://www.boettger-consulting.de/download/CLT/Groupware-Chemnitz2007-CB-web.pdf abgerufen am 5.11.2008.

[4] canalys. Gobal smart phone shipments rise 28 percent, 2008. http://www.canalys.com/pr/2008/r2008112.htm abgerufen am 19.11.2008.

[5] Hochschule der Medien. CMC, 2008. http://www.convergentmedia.de/cmc abgerufen am 01.10.2008.

[6] Ingo Ebel. Interview mit Volker Lendecke, mar 2006. http://radiotux.de/interviews/volker_lendecke_samba.mp3 abgerufen am 01.10.2008.

[7] Florian Effenberger. OpenOffice.org im Netzwerk, may 2008. http://de.openoffice.org/files/documents/66/4267/OpenOffice.org_im_Netzwerk.pdf abgerufen am 3.11.2008.

[8] Prof. Stephan Ferdinand and Michaela Stumberger. Das Convergent Media Center an der Hochschule der Medien in Stuttgart. *Medienwirtschaft*, 5(3):53–56, 2008.

[9] Free Software Foundation. The free software definition. http://www.gnu.org/philosophy/free-sw.html abgerufen am 18.10.2008.

[10] Univention GmbH. Technologie. http://univention.de/technologie.html abgerufen am 18.11.2008.

[11] Golem.de. Open-Xchange veröffentlicht freie Community Edition, 2008. http://www.golem.de/0802/57711.html abgerufen am 20.11.2008.

[12] Florian Haas, Philipp Reisner, and Lars Ellenberg. The DRBD User's Guide. http://www.drbd.org/users-guide/ abgerufen am 2.12.2008.

[13] Peer Heinlein. *Das Postfixbuch*. open source press, dritte edition, 2008.

[14] Ralf Hildebrand and Patrick Koetter. *Postfix - Einrichtung, Betrieb und Wartung*. d.punkt verlag, 2006.

[15] Nils Kaczenski. Turnschuh ade. *iX*, 15(10):88–94, oct 2008.

[16] Dieter Klünter and Jochen Laser. *LDAP verstehen - OpenLDAP einsetzen*. dpunkt.verlag, 2003.

[17] Walter Kriha. Web application security infrastructure. http://www.kriha.de/krihaorg/docs/lectures/security/infrastructure/infrastructure.pdf abgerufen am 12.11.2008.

[18] Walter Kriha and Roland Schmitz. *Internet-Security aus Software-Sicht*. Springer, 2008.

[19] Mailradar.com. Mail server statistics, nov 2008. http://www.mailradar.com/mailstat/ abgerufen am 26.11.2008.

[20] OpenXchange. Open-Xchange Hosted Edition Installation and Administration. http://software.open-xchange.com/OX6/doc/OXHE-Installation-and-Administration.pdf abgerufen am 7.12.2008.

[21] OpenXchange. Open-Xchange Technology. http://www.open-xchange.com/fileadmin/downloads/Open-Xchange_technology.pdf abgerufen am 5.12.2008.

[22] OpenXchange. Hochschule der Medien Stuttgart migriert auf Open-Xchange Server Edition, nov 2008. http://www.open-xchange.com/de/node/657 abgerufen am 5.12.2008.

[23] Optaros. Open source katalog 2009, 2008. http://www.optaros.de/nachrichten/white-papers-reports#open-source-katalog-2009 abgerufen am 27.11.2008.

[24] Linux High Availability Project. Getting Started with Linux-HA (Heartbeat). http://linux-ha.org/GettingStarted abgerufen am 5.12.2008.

[25] John H. Terpstra and Jelmer R. Vernooij. *Samba 3*. ADDISON-WESLEY, 2005.

[26] The Pennsylvania State University. Configuring Mac OS X LDAP authorization for leopard. http://clc.its.psu.edu/Labs/Mac/Resources/authdoc/ldapauthorization-10.5.aspx abgerufen 10.11.2008.

[27] Andre von Raison. Zarafa wird open source. *iX*, (10), oct 2008. auch auf heise online unter: http://www.heise.de/newsticker/Lizenzaenderung-bei-Groupware-Zarafa--/meldung/116137 abgerufen 19.11.2008.

[28] Rod Whitworth. Proftpd mini-howto - symlinks and chroot(), apr 2003. http://www.castaglia.org/proftpd/doc/contrib/ProFTPD-mini-HOWTO-Chroot.html abgerufen am 16.11.2008.

[29] Wikipedia. Cyrus (Server). http://de.wikipedia.org/wiki/Cyrus_(Server) abgerufen am 26.11.2008.

[30] Wikipedia. Dynamic Host Configuration Protocol. http://de.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol abgerufen am 6.12.2008.

[31] Wikipedia. Lamp. http://de.wikipedia.org/wiki/LAMP abgerufen am 4.12.2008.

[32] Wikipedia. Linux-Distributionen. http://de.wikipedia.org/wiki/Linux-Distribution abgerufen am 24.11.2008.

[33] Wikipedia. Open Source. http://de.wikipedia.org/wiki/Open-Source abgerufen am 25.11.2008.

[34] Wikipedia. Opendocument. http://de.wikipedia.org/wiki/OpenDocument abgerufen am 10.10.2008.

[35] Wikipedia. Openldap. http://de.wikipedia.org/wiki/OpenLDAP abgerufen am 29.11.2008.

[36] Wikipedia. Portal (informatik). http://de.wikipedia.org/wiki/Portal_(Informatik) abgerufen 11.12.2008.

[37] Wikipedia. Postfix. http://de.wikipedia.org/wiki/Postfix_(Mail_Transfer_Agent) abgerufen am 7.11.2008.

[38] Wikipedia. Samba (software). http://de.wikipedia.org/wiki/Samba_(Software) abgerufen am 29.11.2008.

[39] Wikipedia. Single sign on. http://de.wikipedia.org/wiki/Single_Sign-on angerufen 8.12.2008.

[40] Wikipedia. Syncml. http://de.wikipedia.org/wiki/SyncML abgerufen am 20.11.2008.

Glossar

AD ..... Active Directory oder auch ADS für Active Directory Service ist der Verzeichnisdienst mit Erweiterungen von Microsoft

CRC ..... cyclic redundancy check, ist geeignet um Fehler bei der Übertragung oder Duplizierung von Daten erkennen zu können.
Wenn Sicherheit gefordert ist, müssen kryptografische Hash-Funktionen wie z. B. SHA verwendet werden

Debian ..... auch Debian GNU/Linux genannt, ist ein freies Betriebssystem, welches nicht nur von einem Hersteller abhängt, wie bei SLES und RHEL der Fall, sondern von der Community gepflegt wird

DRBD ..... Distributed Replicated Block Device, ein RAID 1 über ein Netzwerk

FLOSS ..... Abkürzung für Free/Libre/Open Source Software, auch oft nur OSS für Open Source Software.

FQDN ..... Fully Qualified Domain Name, vollständiger Name einer Domain also eine absolute Adresse. Beispiele: www.hdm-stuttgart.de oder media.hdm-stuttgart.de

FTP ..... File Transfer Protocol, dt.: Dateiübertragungsverfahren, ist ein im RFC 959 spezifiziertes Netzwerkprotokoll zur Übertragung von Dateien über TCP/IP-Netzwerke.

GPL ..... GNU General Public License, ist die meistverwendete Lizenz für freie Software und benutzt das Copyleft-Prinzip

GUI ..... Graphical User Interface, dt.: Grafische Benutzeroberfläche, vereinfacht die Steuerung von Computersystemen und kann meist mit der Computer-Maus bedient werden

IMAP ..... Internet Message Access Protocol, Protokoll zum Zugriff und zur Verwaltung von E-Mails auf einem Mailserver, früher wurde oft POP3 verwendet

LAMP ..... ein Akronym für das Betriebssystem Linux, den Webserver Apache, das Datenbanksystem MySQL und meist die Scriptsprache PHP

LAN ..... Local Area Network, ist ein lokales Netz, welches mehrere Rechner zusammenschaltet und sich meist über viele Räume erstrecken kann

LDAP ..... Lightweight Directory Access Protocol, Standardprotokoll für die Abfrage und die Modifikation von Informationen eines Verzeichnisdienstes.

LMTP ..... Local Mail Transfer Protocol ist dem SMTP sehr ähnlich, es wird als Transport zwischen verschiedenen lokalen Serverkomponenten wie etwa MTA und MDA benutzt.

LVM ..... Logical Volume Manager, ist Abstraktionsebene zwischen Festplatten und Dateisystemen. Festplatten werden zu einem Pool zusammengefasst, aus diesem werden logische Partitionen erstellt. Darauf aufsetzend kann ein Dateisystem erstellt werden.

MDA ..... Mail Delivery Agent, Teil des Mailservers der E-Mails annimmt und diese einsortiert und zur Abholung über IMAP/POP3 bereithält

MTA ..... Mail Transfer Agent, Teil des Mailservers der sich mit der Annahme und Weiterleitung von E-Mails auseinandersetzt meist über das SMTP-Protokoll

NAS ..... Network Attached Storage

OX ..... Open Xchange, ist eine Open Source Groupware-Lösung, sowie eine Firma aus Deutschland mit dem gleichen Namen, die diese Groupware herstellt.

PAM ..... Pluggable Authentication Modules, stellt eine Programmierschnittstelle (API) für Authentisierungsdienste zur Verfügung, damit muss nicht jede Applikation div. Authentisierungen unterstützen sondern nur die PAM-API

PDA ..... Personal Digital Assistant, tragbarer, kompakter Computer mit Software zur Aufgaben- und Adressverwaltung, Terminplanung, etc.

PDC ..... Primary Domain Controller, ist ein Server zur zentralen Authentifizierung und Autorisierung von Computern und Benutzern in einem Rechnernetz mit Windows Clients.

PIM ..... Personal Information Management, bezeichnet die Verwaltung von persönlichen Daten wie Kalender, Aufgaben, Adressbuch, E-Mail, neuerdings auch RSS-Feeds etc.

POP3 ..... Post Office Protocol, Protokoll mit dem E-Mail von einem Mailserver abgeholt werden kann, heute wird jedoch öfter IMAP verwendet.

RAID ..... redundant array of independent disks, dt.: Redundante Anordnung unabhängiger Festplatten, dient der Datensicherheit, je nach RAID-Level können Festplatten ausfallen ohne dass Daten verloren gehen.

RFC ..... Requests for Comments, dt. Forderung nach Kommentaren, sind eine Reihe von technischen und organisatorischen Dokumenten des RFC-Editors zum Internet

RHEL ..... Red Hat Enterprise Linux ist eine Distribution der US-amerikanischen Firma Red Hat, die sich speziell an Geschäftskunden richtet

RRD ..... Round-Robin-Database, damit werden zeitbezogene Messdaten gespeichert, zusammengefasst und visualisiert

SAN ..... Storage-Area-Network

SASL ..... Simple Authentication and Security Layer, ist ein Framework, das von verschiedenen Protokollen zur Authentifizierung verwendet wird. Es ist in RFC 4422 beschrieben.

SLES ..... SUSE Linux Enterprise Server ist eine Linux-Distribution von Novell, die speziell auf Unternehmenskunden ausgelegt ist.

Smartphone .... Geräte, die die Funktionen von Mobiltelefonen und PDAs vereinen.

SMB ..... Server-Message-Block-Protokoll, ursprünglich von IBM entwickelt ist ein Kommunikationsprotokoll für Datei-, Druck- und andere Serverdienste in Netzwerken und wird in allen Windows Betriebssystemen verwandt, heute von Microsoft eher als CIFS betitelt

SNMP ..... Simple Network Management Protocol ist ein Netzwerkprotokoll, um Netzwerkelemente (z. B. Router, Server, Switches, Drucker, Computer usw.) von einer zentralen Station aus überwachen und steuern zu können.

SPOF ..... Single Points Of Failure (dt.: einzelne Fehlerstelle), der Ausfall einer Komponente legt das komplette System lahm, solche Fehlerstellen müssen bei hochverfügbaren Systemen vermieden werden

SQL ..... Structured Query Language, Datenbanksprache zur Definition, Abfrage und Manipulation von Daten in relationalen Datenbanken

SSL ..... Secure Sockets Layer, ist der Vorgänger von TLS

SSO ..... Single Sign-on, dt.: Einmalanmeldung, bezeichnet einen Mechanismus bei dem nach der einmaligen Authentisierung mehrere Dienste verwendet werden können

TLS ..... Transport Layer Security, ist ein hybrides Verschlüsselungsprotokoll zur Datenübertragung und die standardisierten Weiterentwicklungen von SSL.

UCS ..... Univention Corporate Server, Debian-basierte Distribution und Hauptprodukt der Firma Univention GmbH aus Bremen

URL ..... Universal Resource Locator, Adressangabe im Internet, z.B. die Adresse einer Website.

WINS ..... Wie DNS dient der Windows Internet Naming Service der zentralen Namensauflösung in lokalen Netzwerken.

WLAN ..... Wireless Local Area Network, bezeichnet ein drahtloses, lokales Funknetz nach IEEE 802.11 Standard

Lizenz

Die in diesem Werk wiedergegebenen Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. werden ohne Gewährleistung der freien Verwendbarkeit benutzt und können auch ohne besondere Kennzeichnung eingetragene Marken oder Warenzeichen sein und als solche den gesetzlichen Bestimmungen unterliegen.

Dieses Dokument unterliegt der Creative-Commons-Lizenz CC-BY-SA DE. Informationen, welche Rechte damit eingeräumt werden, können unter http://creativecommons.org/licenses/by-sa/3.0/de/ nachgelesen werden.