

**FOM Fachhochschule für Oekonomie & Management
Essen / Neuss**

**Diplomarbeit
zur Erlangung des akademischen Grades des
Diplom-Informatikers**

Open Source Groupware am Beispiel Kolab

Betreuer: Prof. Dr.-Ing. Torsten Finke

Autor: Magnus Stoermer

Kontakt: magnus.stoermer@gmx.de

Veröffentlichung unter der Creative Commons Licence
<http://creativecommons.org/licenses/by/2.0/de/>

Inhaltsverzeichnis

Abbildungsverzeichnis	V
Tabellenverzeichnis	VI
Abkürzungsverzeichnis	VII
1 Einführung	1
1.1 Motivation	1
1.2 Zielgruppe und Umfeld	1
1.3 Struktur dieser Arbeit	1
1.4 Konventionen	2
1.5 Einführung von Begriffen	3
2 Groupware	4
2.1 Definition Groupware und CSCW	4
2.1.1 Klassifikation von CSCW-Systemen	5
2.1.1.1 Klassifikation nach Art und Grad der Unterstützung	5
2.1.1.2 Klassifikation nach räumlicher und zeitlicher Trennung	7
2.1.1.3 Klassifikation unter Berücksichtigung der Vorhersehbarkeit	8
2.2 Betrieblicher Nutzen von Groupware	8
2.3 Funktionen von Groupware und bekannte Vertreter	10
2.4 Ansätze von Open Source Groupware	11
3 Informationen zu Kolab	14
3.1 Entstehung	14
3.2 Der Kolab-Server	15
3.3 Protokolle und Standards	16

3.3.1	SSL/TLS	18
3.3.2	IMAP	18
3.3.3	POP3	19
3.3.4	SMTP	19
3.3.5	LMTP	20
3.3.6	HTTP	20
3.3.7	FTP	20
3.3.8	LDAP	20
3.4	Kolab-Server-Komponenten	21
3.4.1	Cyrus-SASL	21
3.4.2	Cyrus-IMAPd	21
3.4.3	Postfix	22
3.4.4	Apache	23
3.4.5	ProFTPD	24
3.4.6	OpenLDAP	24
3.4.7	Perl	27
3.4.8	PHP	27
3.5	Funktionsbetrachtung	27
3.5.1	Unterstützte Funktionen	27
3.5.2	Sicherheit	28
3.5.3	Plattformunabhängigkeit	29
4	Praktische Betrachtung des Kolab-Servers	32
4.1	Kolab-Server Installation	32
4.1.1	OpenPKG	32
4.1.2	Wahl der Installationsalternativen	33
4.1.2.1	Installation mittels Source-RPM-Paketen	33
4.1.2.2	Installation plattformspezifischer OpenPKG-Pakete	34
4.1.2.3	Installation unter Mandrake Linux	34
4.1.3	Installation einer Referenzplattform	34
4.1.3.1	Paketauswahl	35
4.1.3.2	Update des Betriebssystems	35
4.1.3.3	Deaktivierung von Diensten	35
4.1.3.4	Installation von Kolab	36
4.1.4	Kolab Bootstrap-Prozess	36
4.2	Probleme bei der Installation	38
4.2.1	Export von Umgebungsvariablen unter Red Hat Linux	38
4.2.2	Installation mittels ZfOS-Binaries	39

4.2.3	Auftretende Fehler beim Bootstrap-Prozess	39
4.2.4	Portbelegung	39
4.2.5	LDAP Replikationsdienst manuell stoppen	40
4.2.6	E-Mail-Konten werden nicht angelegt	40
4.2.7	überprüfung der Ereignisprotokolle	42
4.3	Skalierbarkeit und Hochverfügbarkeit	42
4.4	Installation eines Kolab High Availability Clusters	45
4.4.1	Hardwareplattform	45
4.4.2	Installation des Betriebssystems	46
4.4.3	Installation der Clustersoftware	48
4.4.4	Konfiguration von heartbeat	50
4.4.5	Installation von Kolab	51
4.4.6	Test des Clusters	56
4.5	Backup und Restore	59
4.5.1	Sicherung der LDAP-Datenbank	59
4.5.1.1	Offline Backup	60
4.5.1.2	Export der Daten	60
4.5.1.3	Online Backup	60
4.5.2	Sicherung der Postkörbe	61
4.6	Weitere Betriebsaspekte	62
4.6.1	Erweiterbarkeit	62
4.6.2	Datenpflege	62
4.6.3	Benutzerfreundlichkeit	64
4.6.4	Administrativer Aufwand	64
5	Praktische Betrachtung der Kolab-Clients	65
5.1	Kolab KDE-Client	65
5.1.1	Konzept und Plattform	65
5.1.2	Installation	67
5.1.3	Sicherheit	67
5.1.4	Benutzerfreundlichkeit	67
5.2	Aethera	68
5.2.1	Konzept und Plattform	69
5.2.2	Installation	69
5.2.3	Sicherheit	69
5.2.4	Benutzerfreundlichkeit	69
5.3	Outlook mit Connector	70
5.3.1	Konzept und Plattform	71

5.3.2	Installation	71
5.3.3	Sicherheit	71
5.3.4	Benutzerfreundlichkeit	71
5.4	Horde Webclient	72
5.4.1	Konzept und Plattform	73
5.4.2	Installation	73
5.4.3	Sicherheit	73
5.4.4	Benutzerfreundlichkeit	74
6	Wirtschaftliche Aspekte	75
6.1	Kostenbetrachtung	75
6.2	TCO-Betrachtung	76
6.3	Anreize für öffentliche Organe und KMU	77
7	Ausblick und Fazit	79
7.1	Ausblick	79
7.2	Fazit	80
	Glossar	83
	Literaturverzeichnis	86
	Buchquellen	86
	Internetquellen	87

Abbildungsverzeichnis

2.1	3K-Modell	6
2.2	Raum-Zeit-Matrix	7
2.3	Neun-Felder-Matrix	9
3.1	Interaktion der Kolab-Komponenten	16
3.2	E-Mail Datenfluss im Kolab-Konzept	23
3.3	Kolab Administrationskonzept	25
4.1	Kolab Bootstrap-Prozess	37
4.2	Active/Passive Cluster	44
5.1	KDE Kolab-Client	66
5.2	Aethera	68
5.3	Outlook	70
5.4	Horde	72

Tabellenverzeichnis

4.1	Hardwarespezifikation des Kolab HA-Clusters	45
4.2	Clusterknoten	46
5.1	Funktionen der Kolab-Clients	65

Abkürzungsverzeichnis

2000	Windows 2000
ACL	Access Control List
AIX	Advanced IBM Unix
AMaViS	A Mail Virus Scanner
Bash	Bourne Again Shell
BBS	Bulletin Board System
BMWA	Bundesministerium für Wirtschaft und Arbeit
BSD	Berkeley Software Distribution
BSI	Bundesamt für Sicherheit in der Informationstechnik
bzw.	beziehungsweise
CSCW	Computer-Supported Cooperative Work
CVS	Concurrent Versions System
d.h.	das heisst
DAP	Directory Access Protocol
DNS	Domain Name System
DB	Database
et al.	et alii
evtl.	eventuell
f.	folgende
FAQ	Frequently Asked Questions
FC	Fibre Channel
ff.	fortfolgende
FTP	File Transfer Protocol
FTPD	File Transfer Protocol Daemon
Gbit	Gigabit
gcc	GNU C Compiler
GPG	GNU Privacy Guard
HA	High Availability

HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol SSL/TLS
IBM	Industrial Business Machines
i.d.R.	in der Regel
IETF	Internet Engineering Task Force
IIS	Internet Information Server
IMAP	Internet Message Access Protocol
IMAP4rev1	Internet Message Access Protocol Version 4 Revision 1
IMAPd	Internet Message Access Protocol daemon
IMAPS	Internet Message Access Protocol SSL/TLS
IP	Internet Protocol
IT	Information Technology
KDE	K Desktop Environment
KMU	Kleine und mittlere Unternehmen
LAMP	Linux Apache MySQL PHP
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LDAPv3	Lightweight Directory Access Protocol Version 3
LDIF	LDAP Data Interchange Format
LMTP	Local Mail Transport Protocol
Mac	Macintosh
MSSQL	Microsoft SQL
MTA	Mail Transport Agent/Message Transfer Agent
MUA	Mail User Agent
MX	Mail Exchanger
o.g.	oben genannt
OS	Operating System
PDA	Personal Digital Assistant
Perl	Practical Extraction and Reporting Language
PGP	Pretty Good Privacy
PHP	Hypertext Preprocessor
PKI	Public Key Infrastructure
POP	Post Office Protocol
POP3	Post Office Protocol Version 3
POP3S	Post Office Protocol SSL/TLS
RFC	Request For Comments
RPM	Red Hat Package Manager

SASL	Simple Authentication and Security Layer
SCSI	Small Computer System Interface
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol SSL/TLS
sog.	so genannte
SQL	Structured Query Language
SSL	Secure Sockets Layer
tar	Tape Archiver
TCO	Total Cost of Ownership
TLS	Transport Layer Security
tty	Teletypewriter
u.a.	unter anderem
u.U.	unter Umständen
URL	Uniform Ressource Locator
USV	Unterbrechungsfreie Stromversorgung
vgl.	Vergleiche
VoIP	Voice over IP
WAMP	Windows Apache MySQL PHP
WebDAV	Web-based Distributed Authoring and Versioning
WinNT	Windows NT
XP	Windows XP
z.B.	zum Beispiel
ZfOS	Zen for Open Source

1 Einführung

1.1 Motivation

Ein grosser Teil der Funktionalität proprietärer Softwareprodukte wird heute bereits durch Open Source Software abgedeckt, die als alternative Produkte Einzug in die Unternehmen halten. Während viele Unternehmen bereits auf Servern Open Source Software erfolgreich einsetzen, hat sich dieser Trend bei den Desktop-Systemen aus unterschiedlichen Gründen bisher nicht fortgesetzt. Ein Grund dafür ist das Fehlen stabiler und ausgereifter Groupware-Lösungen, die im betrieblichen Einsatz zur computergestützten Gruppenarbeit genutzt werden können. Die Motivation zu dieser Arbeit ergibt sich aus der Situation, dass zum Zeitpunkt der Erstellung dieser Arbeit am Markt für Open Source Software im Gegensatz zu proprietären Produkten kein etabliertes Produkt für den Bereich Groupware zur Verfügung steht. Diese Arbeit soll prüfen, ob die Open Source Groupware-Lösung *Kolab* eine Alternative zu proprietären Produkten darstellt.

1.2 Zielgruppe und Umfeld

Zielgruppe dieser Arbeit sind fachlich versierte Entscheider und Administratoren, die Informationen zu dem Projekt Kolab erhalten möchten. Darüber hinaus soll die Arbeit als Leitfaden für die Integration einer Test- bzw. Hochverfügbarkeitsumgebung dienen und einen objektiven Erfahrungsbericht darstellen. Das vorliegende Dokument basiert auf den zum Zeitpunkt der Erstellung aktuellen Informationen zu den Themen Groupware, Open Source Groupware und Kolab.

1.3 Struktur dieser Arbeit

In den einzelnen Kapiteln werden die folgenden Themen behandelt:

- Kapitel 1 dient einer kurzen Einführung in die Thematik, beschreibt Auditorium sowie technisches Umfeld dieser Arbeit und legt die in dieser Arbeit genutzten Konventionen fest.
- Kapitel 2 beinhaltet die Definition von Begriffen aus den Bereichen Groupware und Computer Supported Cooperative Work, erläutert die Bedeutung des Einsatzes von Groupware im betrieblichen Umfeld und stellt bekannte Groupware-Produkte, Groupware-Funktionen sowie alternative Open Source Groupware-Lösungen vor.
- Das dritte Kapitel bietet einen Überblick über die Entstehung des Kolab-Projekts, erläutert die zum Einsatz kommenden Software-Komponenten und Konzepte und behandelt die in dem Projekt geforderten Funktionalitäten.
- In dem vierten Kapitel werden praktische Aspekte des Kolab-Servers behandelt, Installationsalternativen aufgezeigt, Hinweise für die Installation einer Referenzplattform erläutert sowie auf mögliche Probleme bei der Installation erörtert. Weiterhin wird die Installation einer hochverfügbaren Kolab-Lösung geschildert und wichtige Betriebsaspekte dargestellt.
- Kapitel 5 betrachtet die verschiedenen zur Verfügung stehenden Kolab-Clients, erläutert deren Konzepte sowie Installationsabläufe und gibt einen Überblick über betriebsrelevante Aspekte
- In dem letzten Kapitel werden wirtschaftliche Überlegungen dargestellt, die die Schwierigkeiten einer komplexen Kostenbetrachtung im Zusammenhang mit Kolab erläutern. Des Weiteren werden sowohl Anreize als auch mögliche Probleme der Kolab Groupware-Lösung für öffentliche Organe sowie kleine und mittlere Unternehmen kritisch beleuchtet.
- Den Abschluss dieser Arbeit bildet eine Zusammenfassung, in der die in der Arbeit gewonnenen Erkenntnisse bewertet und ein Ausblick auf zukünftige Entwicklungen gegeben werden.

1.4 Konventionen

Die in der Arbeit verwendeten typographischen Konventionen sind wie folgt festgelegt:

Kursive Schrift

Kursivschrift wird für variable Dateinamen, Pfadnamen oder URLs genutzt, aber auch um neu eingeführte Begriffe bei ihrer ersten Nennung hervorzuheben.

`Festbreitenschrift`

Festbreitenschrift wird für die Darstellung von Ein- und Ausgaben auf einer Systemkonsole und Programmcode sowie Datei- oder Pfadnamen genutzt.

„Anführungszeichen“

Anführungszeichen kennzeichnen ein wörtliches Zitat.

1.5 Einführung von Begriffen

Wichtige, fachspezifische Begriffe werden in dem angehängten Glossar erklärt. Einige der in dieser Arbeit verwendeten Termini wurden vom Autor definiert und werden ebenfalls in dem angehängten Glossar näher erläutert.

2 Groupware

2.1 Definition Groupware und CSCW

„Groupware is technology designed to facilitate the work of groups. This technology may be used to communicate, cooperate, coordinate, solve problems, compete, or negotiate. While traditional technologies like the telephone qualify as groupware, the term is ordinarily used to refer to a specific class of technologies relying on modern computer networks, such as email, newsgroups, videophones, or chat.“¹

Computergestützte Gruppenarbeit – insbesondere in Bereichen mit hohem Spezialisierungsgrad – ist für viele Arbeitsbereiche ein wichtiger Faktor für erfolgreiche und ökonomisch sinnvolle Zusammenarbeit. Hierbei entfällt ein entscheidender Teil der Zusammenarbeit auf die Mittel, die informationstechnisch unterstützte Gruppenarbeit ermöglichen. Bei der Wahl eines oder mehrerer Mittel, die diese Aufgaben erfüllen, gibt es eine Vielzahl von möglichen Alternativen, die sich unter dem im weiten Sinne und aus theoretischer Sicht betrachteten Oberbegriff *CSCW*-Systeme (Computer-Supported Cooperative Work) einordnen lassen. Dieser Begriff wird in dieser Arbeit als Synonym für alle Unterstützungssysteme der Gruppenarbeit verstanden. Zum Anderen wird der Begriff *Groupware* – wie auch im späteren Verlauf dieser Arbeit – im engeren Sinne als Synonym für eine Klasse von Software verwendet, die es einer über ein Computernetzwerk interagierenden Arbeitsgruppe ermöglicht via E-Mail, Instant Messaging oder Chat zu kommunizieren, Terminpläne abzustimmen, Projekte zu planen und durchzuführen, Dateien gemeinsam zu bearbeiten sowie Bulletin Boards zu nutzen.

Groupware ist mit dem Begriff des Computer-Supported Cooperative Work als wissenschaftliche Disziplin eng verbunden und kann als Produkt der theoretischen Erkenntnisse aus den Studien über CSCW betrachtet werden. Dabei deckt das Studienobjekt des CSCW viele Teilbereiche anderer wissenschaftlicher Disziplinen ab:

¹ vgl. Brinck, T.: Usability First Groupware Introduction; in: <http://www.usabilityfirst.com/groupware/intro.txt> – Zugriff am 4.5.2004.

„CSCW (Computer-Supported Cooperative Work) refers to the field of study which examines the design, adoption, and use of groupware. Despite the name, this field of study is not restricted to issues of ‘cooperation‘ or ‘work‘ but also examines competition, socialization, and play. The field typically attracts those interested in software design and social and organizational behavior, including business people, computer scientists, organizational psychologists, communications researchers, and anthropologists, among other specialties.“²

2.1.1 Klassifikation von CSCW-Systemen

CSCW-Systeme können nach verschiedenen Aspekten unterschieden werden. Aus theoretischer Sicht sind vor allem drei Ansätze zu nennen.³

- Unterscheidung nach Art und Grad der Unterstützung von Gruppenarbeit sowie deren Einordnung in Systemklassen.
- Unterscheidung nach räumlicher und zeitlicher Trennung der Kommunikationspartner.
- Unterscheidung nach räumlichen und zeitlichen Aspekten unter Berücksichtigung der Vorhersehbarkeit von Ereignissen.

2.1.1.1 Klassifikation nach Art und Grad der Unterstützung

Zu der Klassifikation dieser Systeme nach Art und Grad der Unterstützung ist grundlegend das Modell zur Klassifikation von CSCW-Systemen nach Burger⁴ zu nennen. Dabei werden die folgenden Kriterien zur Unterteilung verwendet:

- Kommunikationsunterstützung
- Kooperationsunterstützung
- Koordinationsunterstützung

² vgl. Brinck: Usability First Groupware Introduction.

³ vgl. Teufel, S. et al.: Computerunterstützung für die Gruppenarbeit; Bonn 1995, S. 24.

⁴ vgl. Burger, C.: Groupware - Kooperationsunterstützung für verteilte Anwendungen; Heidelberg 1997, S. 20.

Diese Unterstützungsarten werden in dem *3K-Modell* nach Teufel⁵ aufgegriffen, in Zusammenhang mit informationstechnischen Systemen gebracht, und am Beispiel mehrerer Unterklassen wie z.B. E-Mail oder *BBS* (Bulletin Board System) graphisch dargestellt.

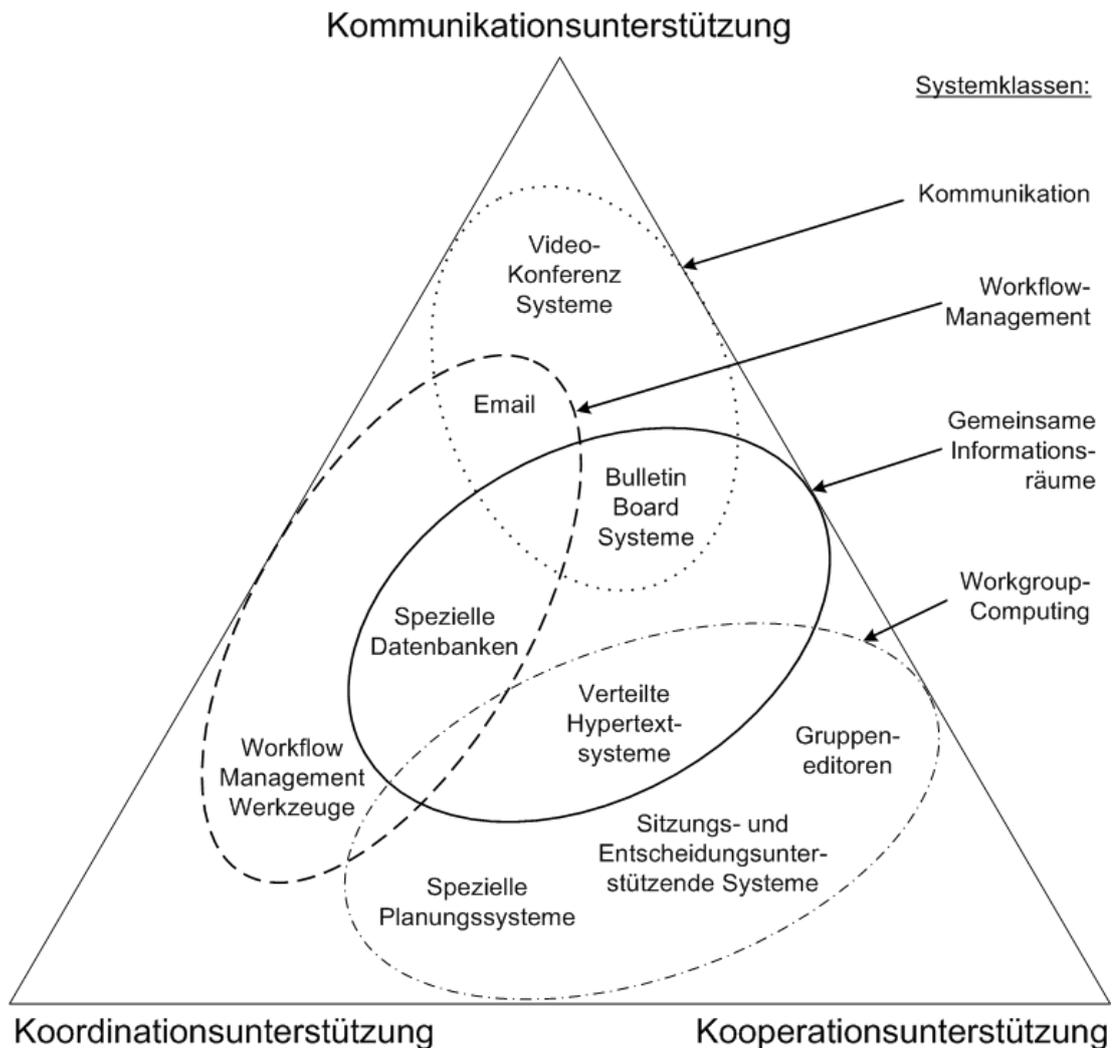


Abbildung 2.1: Das 3K-Modell nach Teufel⁶

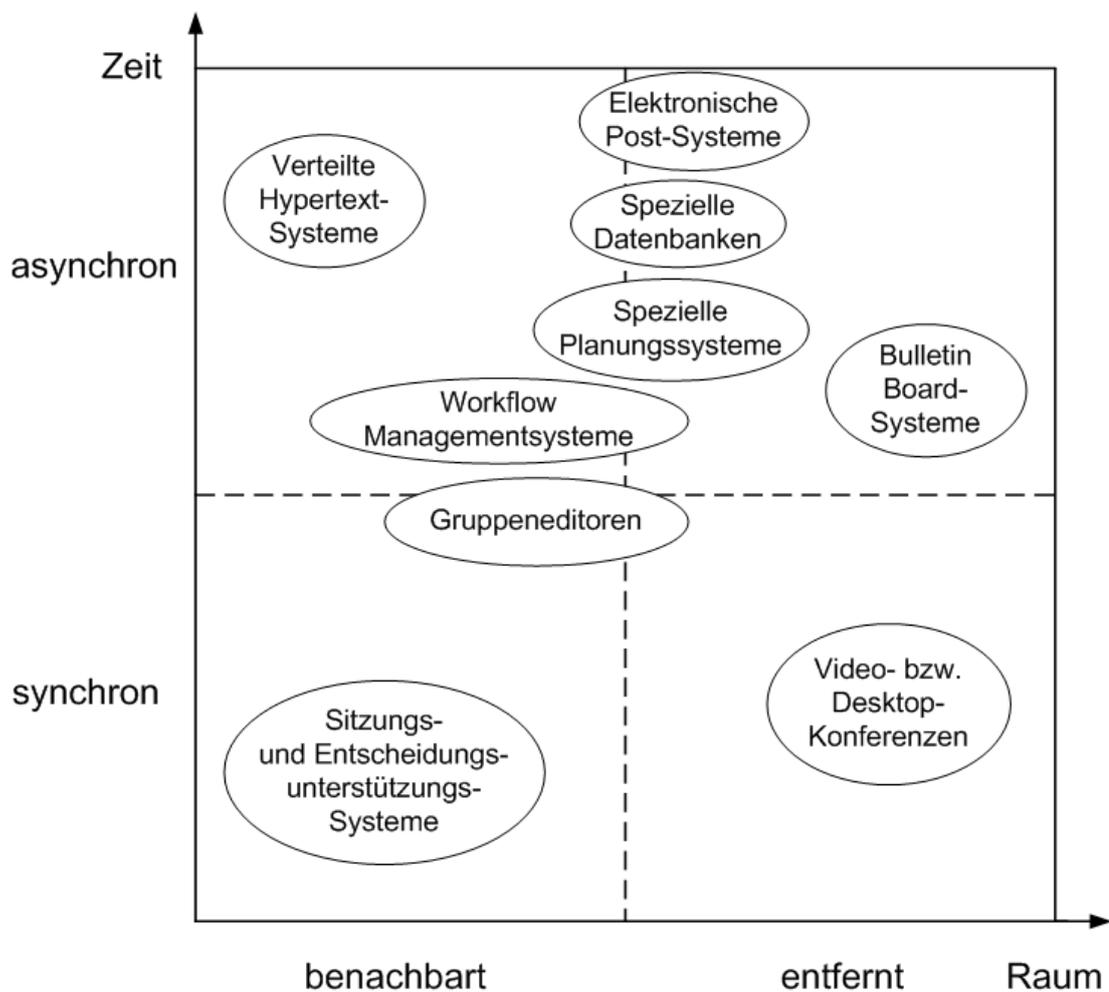
Die in der Abbildung bezeichneten CSCW-Systeme sind gemäß ihrer Eigenschaften im Bezug zu den oben genannten Unterstützungsfunktionen ihrer Eignung nach plziert. Weiterhin werden die Systeme in Systemklassen wie Kommunikation, Workflow Management, gemeinsame Informationsräume oder Workgroup Computing unterteilt.

⁵ vgl. Teufel et al.: Computerunterstützung für die Gruppenarbeit, S. 27.

⁶ vgl. Teufel et al.: Computerunterstützung für die Gruppenarbeit, S. 27

2.1.1.2 Klassifikation nach räumlicher und zeitlicher Trennung

Für die Klassifikation von CSCW-Systemen nach räumlicher und zeitlicher Trennung der Kommunikationspartner und dem damit einhergehenden synchronen oder asynchronen Nachrichtenaustausch ist als Grundlage die *Raum-Zeit-Matrix* nach Teufel⁷ zu nennen (siehe Abbildung 2.2).

Abbildung 2.2: Die Raum-Zeit-Matrix nach Teufel⁸

In diesem Modell sind verschiedene Funktionen von CSCW-Systemen aufgeführt, die nach den Kriterien Raum, Zeit und Synchronität unterschieden werden. Eine räumlich benachbarte Kommunikation beschreibt eine Kommunikationsweise, bei der die Kommunikationspartner z.B. ein direktes Gespräch an einem Ort miteinander führen. Die räumlich entfernte Kommunikation geht hingegen von einer räumlichen Distanz zwis-

⁷ vgl. Teufel et al.: Computerunterstützung für die Gruppenarbeit, S. 25.

⁸ vgl. Teufel et al.: Computerunterstützung für die Gruppenarbeit, S. 25

chen den Kommunikationspartnern aus. Der in dem Modell beschriebene synchrone Nachrichtenaustausch geht von der Erwartungshaltung eines Kommunikationspartners auf die direkte Antwort des anderen Kommunikationspartners aus. Ein Beispiel hierfür ist ein Telefonat oder eine Videokonferenz, beide Kommunikationspartner nehmen zeitgleich an dem Nachrichtenaustausch teil. Bei asynchroner Kommunikation wird eine Nachricht an einen Kommunikationspartner versendet, der nach unbestimmter Zeit auf diese Nachricht antworten kann, wie z.B. bei der Kommunikation via E-Mail. Die Kommunikationspartner nehmen nicht zeitgleich an dem Nachrichtenaustausch teil.

2.1.1.3 Klassifikation unter Berücksichtigung der Vorhersehbarkeit

Im dritten Ansatz der Klassifizierung von CSCW-Systemen sind Teilaspekte der genannten Modelle in der *Neun-Felder-Matrix* nach Grudin⁹ beinhaltet, die neben den Faktoren Raum und Zeit nun auch den Faktor Vorhersehbarkeit berücksichtigt. Anhand der verschiedenen Umstände, unter denen Gruppenarbeit ermöglicht werden soll, sind in dieser Matrix Beispiele genannt, welches CSCW-System im weiteren Sinne die z.T. komplexen Anforderungen erfüllt. Abbildung 2.3 stellt die unterschiedlichen Situationen graphisch dar.

2.2 Betrieblicher Nutzen von Groupware

Der Einsatz von Groupware Systemen in Unternehmen ist praktisch unabdingbar geworden. Aufgrund von Teamarbeit in spezialisierten Gruppen, ökonomisch notwendig gewordenen Reaktionszeiten und dezentralisierten Unternehmensstandorten müssen flexible und leistungsfähige Produkte zum Informationsaustausch zur Verfügung stehen. Informationen werden neben den klassischen Produktionsfaktoren inzwischen als weiterer Produktionsfaktor¹¹ angesehen und müssen daher effizient verwaltet und verarbeitet werden können. Dabei ist die Anwenderfreundlichkeit ein wichtiger Aspekt.

„Die Globalisierung verschärft den Konkurrenzkampf um Märkte und Marktanteile. Es besteht kein Zweifel, daß die Informations- und Kommunikationstechnologie für viele

⁹ vgl. Grudin, J.: CSCW History and Focus; in: <http://www.ics.uci.edu/~grudin/Papers/IEEE94/IEEEComplastsub.html> – Zugriff am 13.5.2004.

¹⁰ vgl. Grudin: CSCW History and Focus

¹¹ vgl. Stickel, E.: Informationsmanagement; München 2001, S. 3.

		Time		
		Same	Different but predictable	Different and unpredictable
Place	Same	Meeting facilitation	Work shifts	Team rooms
	Different but predictable	Teleconferencing Videoconferencing Desktop conferencing	Electronic mail	Collaborative writing
	Different and unpredictable	Interactive multicast seminars	Computer boards	Workflow

Abbildung 2.3: Die Neun-Felder-Matrix nach Grudin¹⁰

Unternehmen zum wichtigsten strategischen und auch operativen Instrument geworden ist, um diesen Konkurrenzkampf zu bestehen. Für Unternehmen ist es daher überlebenswichtig,

- die Kommunikation zwischen Mitarbeitern innerhalb und zwischen einzelnen Organisationseinheiten zu verbessern,
- die Gruppen- und Teamarbeit generell effektiver und effizienter zu gestalten,
- Produktzyklen zu verkürzen,
- nötige Organisationsänderungen rasch vollziehen zu können,
- Entscheidungszeiten und -wege zu verkürzen und
- die Qualität strategischer Entscheidungen zu verbessern.“¹²

Neben den klassischen Anwendungsbereichen wie E-Mail, Projekt Workflows, Adressverzeichnissen und Kalender ermöglichen moderne Groupware-Systeme auch den Einsatz

¹² vgl. Teufel et al.: Computerunterstützung für die Gruppenarbeit, S. 3, 4.

von Eigenentwicklungen wie z.B. Ressourcenplanung für Pool-Fahrzeuge oder Besprechungsräume, Arbeitszeiterfassung, Literaturverwaltung, Abrechnungswesen, Bestellwesen etc., wodurch zum Teil zeitaufwändige Verwaltungsvorgänge entfallen oder vereinfacht werden.

2.3 Funktionen von Groupware und bekannte Vertreter

Groupware erfüllt in den meisten Fällen eine Schnittmenge der folgenden Funktionen:

- E-Mail
- persönliche und globale Kalender
- persönliche und globale Adressbücher
- grundlegende Funktionen zur Projektadministration (Termine, Projektmitglieder, Aufgabenzuweisung, Projektverfolgung)
- *Bulletin Board*

Weitere optionale Funktionen können z.B. sein:

- erweiterte Funktionen zur Projektadministration (Prioritäten, Workflow, Zeitplanung etc.)
- *Chat*
- Versionsverwaltung für Dokumente
- *Trouble Ticket System*
- Telefonie
- *Video Conferencing*
- *PDA Synchronisation (Personal Digital Assistant)*

Als auf dem Markt verbreitete Vertreter von kommerziellen Groupware-Lösungen sind die weit verbreiteten Client/Server-Produkte Microsoft Outlook/Exchange und IBM Lotus Notes/Domino zu nennen. Gemäß einer Studie der Radicati Group haben die Microsoft-Produkte Outlook und Exchange im Unternehmensbereich insgesamt einen Marktanteil von 31%¹³, die Produkte Lotus Notes und Domino des Herstellers IBM er-

¹³ vgl. The Radicati Group, Inc.: European MS Exchange Outlook Penetration and Forecast, 2004-2008; 2004 in: <http://www.radicati.com/reports/single.shtml> – Zugriff am 7.8.2004.

reichen einen Marktanteil von 24%.¹⁴ Laut dieser Studie verwenden 74% der weltweiten Unternehmen den E-Mail Client Outlook. Angesichts der hohen Verbreitung von Outlook war es naheliegend, dass die Kompatibilität von Kolab im Hinblick auf Outlook als Kolab-Client eine wichtige Forderung bei der Ausschreibung des Projekts war.

2.4 Ansätze von Open Source Groupware

Auf dem Markt existiert bereits eine Vielzahl von Open Source Groupware-Projekten, die ähnliche Ziele mittels unterschiedlicher Konzepte verfolgen. Als Unterscheidungskriterien wurden Konzept und Funktionen des Produkts, Voraussetzungen für die Installation sowie verfügbare Clients gewählt. Ein Großteil der Open Source Groupware-Lösungen basiert auf so genannten *LAMP*- (Linux, Apache, MySQL, PHP) oder *WAMP*- (Windows, Apache, MySQL, PHP) Systemen. Für die Nutzung einer solchen Lösung wird ein Betriebssystem in Verbindung mit einem Webserver, einer Datenbank sowie PHP benötigt. Eine beispielhafte Auflistung soll die verschiedenen Konzepte und Funktionen verdeutlichen:

phpGroupware¹⁵

Konzept: Web-basierte Groupware-Suite

Funktionen: Kalender, Aufgaben, Adressbuch, E-Mail, News,

Dateiverwaltung, weitere optionale Module¹⁶

Voraussetzungen: Apache, MySQL, PHP und IMAP-Mailserver¹⁷

Client: Webbrowser

eGroupWare¹⁸

Konzept: Web-basierte Groupware-Suite

Funktionen: Kalender, Kontakte, Projekte, Dateiverwaltung,

¹⁴ vgl. The Radicati Group, Inc.: IBM Lotus Messaging Software, Market Analysis, 2004-2008; 2004 in: <http://www.radicati.com/reports/single.shtml> – Zugriff am 7.8.2004.

¹⁵ vgl. phpGroupWare: phpGroupWare; 2004 in: <http://www.phpgroupware.org/> – Zugriff am 31.7.2004.

¹⁶ vgl. phpGroupWare: phpGroupWare.

¹⁷ vgl. phpGroupWare: phpGroupWare; 2004 in: <http://docs.phpgroupware.org/html/install/prerequisites.html> – Zugriff am 31.7.2004.

¹⁸ vgl. eGroupWare: eGroupWare - Enterprise Collaboration; 2004 in: <http://www.egroupware.org> – Zugriff am 31.7.2004.

Content-Management, E-Mail, weitere optionale Module^{19,20}

Voraussetzungen: Unix-Derivat, Macintosh, Windows; diverse Webserver (IIS, Roxen, Apache); diverse Datenbankserver (MySQL, MSSQL, PostgreSQL); diverse MTA (Postfix, Sendmail, Exim); diverse IMAP-Server (Cyrus, Courier, Dovecot); PHP²¹

Client: Webbrowser

Citadel²²

Konzept: Client/Server Messaging BBS mit Groupware Funktionalitäten

Funktionen: E-Mail, Webmail, Mailing Lists, globales Adressbuch, Spamfilter²³

Voraussetzungen: Unix-Derivat; gcc; BerkeleyDB; libical^{24, 25}

Client: verschiedene kommandozeilenbasierte Anwendungen und KDE Kolab-Client²⁶

phpCollab²⁷

Konzept: Web-basierte Projektplanung²⁸

Funktionen: Aufgaben, Kalender, Notizen, Bug Tracking,

Dokumentenverwaltung, Benachrichtigungsalarm, Bulletin Board,

¹⁹ vgl. Reibold, H.: eGroupWare 1.0 kompakt; in: <http://www.bomots.de/egroupware/index.htm> – Zugriff am 31.7.2004.

²⁰ vgl. Reibold, H.: eGroupWare 1.0 kompakt; in: <http://www.bomots.de/egroupware/kap11.htm> – Zugriff am 31.7.2004.

²¹ vgl. eGroupWare: Requirements to install eGW; 2004 in: <http://www.egroupware.org/requirements> – Zugriff am 31.7.2004.

²² vgl. Citadel: Citadel/UX: Flexible, powerful, community-oriented groupware; 2004 in: <http://www.citadel.org/> – Zugriff am 31.7.2004.

²³ vgl. Citadel: Citadel/UX a messaging and collaboration platform for BBS and groupware applications; 2004 in: http://uncensored.citadel.org/viewcvs/viewcvs.cgi/*checkout*/citadel/docs/citadel.html?rev=HEAD&content-type=text/html#Introduction – Zugriff am 31.7.2004.

²⁴ vgl. Cancro, A. und Poulin, M.: Citadel/UX FAQ; in: <http://www.citadel.org/citadel-faq.php#sneelesnorf> – Zugriff am 31.7.2004.

²⁵ vgl. Citadel: Citadel/UX a messaging and collaboration platform for BBS and groupware applications; 2004 in: http://uncensored.citadel.org/viewcvs/viewcvs.cgi/*checkout*/citadel/docs/citadel.html?rev=HEAD&content-type=text/html#Installation – Zugriff am 31.7.2004.

²⁶ vgl. Kolab Project: The Kolab Project::Home; 2004 in: <http://kolab.org/> – Zugriff am 21.7.2004.

²⁷ vgl. phpCollab: phpCollab Home / News; 2004 in: <http://www.php-collab.com/> – Zugriff am 1.8.2004.

²⁸ vgl. phpCollab: phpCollab Home / News.

Kundenverwaltung, Projektplanung²⁹

Voraussetzungen: Windows, Linux; Apache, IIS;

MySQL, MSSQL, PostgreSQL; PHP³⁰

Client: Webbrowser

Eine sehr umfangreiche übersicht über kostenlose und kommerzielle Open Source Groupware-Projekte bietet die Homepage von Grant Bowman.³¹

²⁹ vgl. phpCollab: phpCollab Features; 2004 in: <http://www.php-collab.com/documentation/features.htm> – Zugriff am 1.8.2004.

³⁰ vgl. phpCollab: phpCollab Installation Guide; 2004 in: <http://www.php-collab.com/documentation/install.htm> – Zugriff am 1.8.2004.

³¹ vgl. Bowman, G.: Collaborative Groupware Software; in: <http://www.sypal.org/~grantbow/groupware.html> – Zugriff am 31.7.2004.

3 Informationen zu Kolab

3.1 Entstehung

Die Entstehung der Open Source Groupware-Lösung Kolab, die unter dem Projektnamen *Kroupware* entwickelt wurde, geht auf eine Ausschreibung für die Entwicklung einer Groupware-Lösung basierend auf Open Source Software durch das Bundesamt für Sicherheit in der Informationstechnik (BSI)³² zurück. Ziel der Ausschreibung war die Entwicklung einer Open Source Groupware-Lösung basierend auf freier Software, die sich sowohl in den Punkten Funktionalität als auch Interoperabilität an dem Microsoft Exchange-Server in Verbindung mit Microsoft Outlook 2000-Clients orientieren sollte.³³ Im Oktober 2002 wurde die Ausschreibung von drei Unternehmen gewonnen, die das Projekt nach zehn Monaten im Juli 2003 erfolgreich zum Abschluss brachten.³⁴ Die Intevation GmbH³⁵ übernahm in diesem Projekt die Projektleitung, das Unternehmen Erfrakon³⁶ zeichnete für die Entwicklung des Kolab-Servers sowie des technischen Konzepts verantwortlich und Klarälvdalens Datakonsult³⁷ steuerte Entwicklungsarbeit im Bereich des *KDE* basierten Kolab-Client³⁸ bei. Der Begriff *Kroupware* steht als Synonym für die in dem ausgeschriebenen Projekt entwickelten Ergebnisse, nach Erfüllung des Vertrags wird das Projekt nun unter dem Namen Kolab weitergeführt. Die entwickelten Softwarekomponenten tragen die Namen *Kolab-Server* sowie *KDE Kolab-Client*.

³² vgl. Bundesamt für Sicherheit in der Informationstechnik: Startseite; 2004 in: <http://www.bsi.de/> – Zugriff am 9.5.2004.

³³ vgl. Kuri, J.: Open-Source-Groupware Kolab ist fertig; in: <http://www.heise.de/newsticker/meldung/38907> – Zugriff am 9.5.2004.

³⁴ vgl. Intevation GmbH: Kroupware/Kolab - Freie Software Groupware; 2004 in: <http://www.intevation.de/projects/kroupware.de.html> – Zugriff am 9.5.2004.

³⁵ vgl. Intevation GmbH: Intevation; 2004 in: <http://www.intevation.de/> – Zugriff am 9.5.2004.

³⁶ vgl. Erfrakon: Erfrakon: Erlewein, Frank, Konold und Partner; 2004 in: <http://erfrakon.de/> – Zugriff am 9.5.2004.

³⁷ vgl. Klarälvdalens Datakonsult AB: Startseite; 2004 in: <http://www.klaralvdalens-datakonsult.se/> – Zugriff am 9.5.2004.

³⁸ vgl. Intevation GmbH: Kroupware/Kolab - Freie Software Groupware.

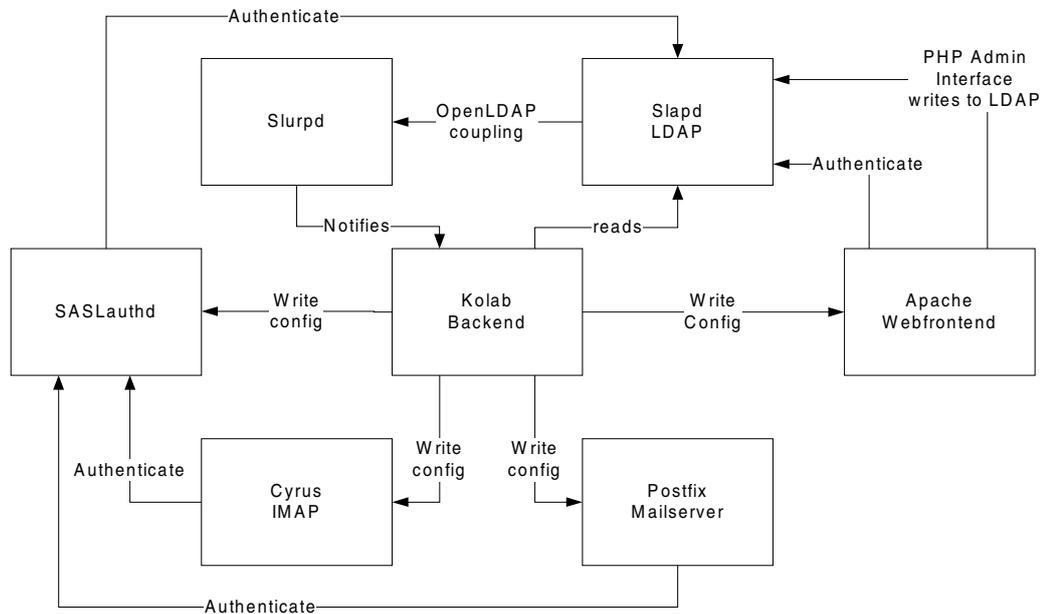
Der Kolab-Server sollte Groupware-Funktionen wie E-Mail, Adressbücher, Gruppenkalender, Notizen und Aufgaben auf Basis von Open Source Software und somit offenen Standards und Programmcode bieten. Wichtige Ziele der Entwicklung waren die Gewährleistung von Sicherheit, Stabilität sowie Skalierbarkeit im späteren Endprodukt. Durch Verwendung von bewährten und praxiserprobten Teilkomponenten sollten diese Ziele realisiert werden. Die verwendeten Softwaremodule basieren wiederum auf den Entwicklungen anderer Open Source Projekte, welche im weiteren Verlauf dieser Arbeit näher erläutert werden (siehe Kapitel 3.4). Ein besonderer Schwerpunkt des Projekts lag in der Bereitstellung eines sicheren Gesamtkonzepts, bei dem Verschlüsselungsmechanismen sowohl auf Anwendungs- als auch auf Transport-Ebene zum Einsatz kommen. Um aus der funktionalen Sicht eines Outlook 2000 Clients einen Open Source-Ersatz für den Microsoft Exchange-Server bieten zu können, wurden bei der Entwicklung allerdings auch Dienste, die auf unsicheren Protokollen wie *FTP* oder *POP3* (siehe Kapitel 3.3) basieren, implementiert.

Der Funktionsumfang des in dem Projekt entwickelten KDE Kolab-Client sollte sich an dem des Microsoft Outlook 2000 Client orientieren, also die Funktionalitäten *IMAP*- oder *POP3*-E-Mail, Kalender, Aufgaben, Adressbücher und eine *Free/Busy*-Liste bieten. Der KDE Kolab-Client wurde auf Basis der Applikationssuite *Kontakt* der KDE-Version 3.1 entwickelt, da diese bereits einige der geforderten Funktionen unterstützte und die Entwicklung eines neuen Clients als zu zeitaufwändig angesehen wurde.³⁹

3.2 Der Kolab-Server

Der Kolab-Server wird durch die Kombination einzelner Open Source Softwareprojekte gebildet. Diese Komponenten kommunizieren untereinander aufgrund definierter Schnittstellen und Standards, die in den folgenden Abschnitten erläutert werden sollen (siehe Kapitel 3.3), wobei die in dem Kroupware-Projekt entwickelte Software zur Konfiguration, Steuerung und Administration der Komponenten dient. Diese Komponenten und deren Aufgaben sollen in diesem Kapitel detailliert betrachtet werden. Die Interaktion der Kolab-Server Komponenten untereinander sowie im Benutzerkontext wird durch Abbildung 3.1 verdeutlicht.

³⁹ vgl. KDE e.V.: FAQ; 2004 in: <http://kontakt.kde.org/faq/#KontaktKolabKroupwareIgetconfusedWhatsthedeal> – Zugriff am 9.5.2004.

Abbildung 3.1: Interaktion der Kolab Komponenten⁴⁰

Das Kolab-Backend dient als zentrale Steuerungsinstanz des Kolab-Servers, es verwaltet die Konfigurationsdateien der einzelnen Kolab-Komponenten. Die Komponenten *Cyrus IMAP* und *Postfix* authentifizieren Benutzer über die von *SASLauthd* gebotenen Methoden gegen den *LDAP*-Dienst *slapd*. Der *LDAP*-Dienst sorgt in diesem Zusammenspiel ausserdem für die direkte Authentifizierung von Benutzern des *Apache* Web-servers. über das *Apache* Webfrontend werden Daten wie z.B. Benutzerdaten oder Adressdaten in die *LDAP*-Datenbank geschrieben. Der *LDAP* Slave-Server *slurpd* dient der Replikation und redundanten Vorhaltung der *LDAP*-Verzeichnisdaten. Die in der Abbildung 3.1 aufgezeigten Komponenten und deren Aufgaben werden in den folgenden Abschnitten noch einmal ausführlich erläutert.

3.3 Protokolle und Standards

Das Kolab Client-Server Konzept baut auf verschiedenen offenen und etablierten Standards auf, die an dieser Stelle aufgezeigt werden. Zunächst gibt die folgende Auflistung einen Überblick über die verwendeten Protokolle:⁴¹

⁴⁰ vgl. Erfrakon: Kolab Server Technical Description; 2003 in: <http://kroupware.org/technical-1.0.1-html/c421.html> – Zugriff am 13.7.2004, S. 2.

⁴¹ vgl. Erfrakon: Protocols; 2004 in: <http://www.kroupware.org/architecture-1.1/c87.html#AEN90> – Zugriff am 1.6.2004.

- SSL/TLS (Secure Socket Layer/Transport Layer Security)⁴²
- Internet Message Access Protocol Version 4rev1 (IMAP4rev1)⁴³, IMAP over SSL/TLS (IMAPS)⁴⁴
- Post Office Protocol Version 3 (POP3)⁴⁵, POP3 over SSL/TLS (POP3S)⁴⁶
- Simple Mail Transfer Protocol (SMTP)⁴⁷, SMTP over SSL/TLS (SMTPS)⁴⁸
- Local Mail Transfer Protocol (LMTP)⁴⁹
- Hyper Text Transfer Protocol (HTTP)⁵⁰, HTTP over SSL/TLS (HTTPS)⁵¹
- File Transfer Protocol (FTP)⁵²
- Lightweight Directory Access Protocol Version 3 (LDAPv3)⁵³
- HotSync® Protocol (PDA Synchronisation)⁵⁴
- Web Distributed Authoring and Versioning (WebDAV) Access Control Protocol⁵⁵

⁴² vgl. Dierks, T. und Allen, C.: The TLS Protocol Version 1.0; in: <ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt> – Zugriff am 8.8.2004.

⁴³ vgl. Crispin, M.: Internet Message Access Protocol - Version 4rev1; in: <ftp://ftp.rfc-editor.org/in-notes/rfc3501.txt> – Zugriff am 21.5.2004.

⁴⁴ vgl. Newman, C.: Using TLS with IMAP, POP3 and ACAP; in: <ftp://ftp.rfc-editor.org/in-notes/rfc2595.txt> – Zugriff am 21.5.2004.

⁴⁵ vgl. Myers, J. und Rose, M.: Post Office Protocol - Version 3; in: <ftp://ftp.rfc-editor.org/in-notes/rfc1939.txt> – Zugriff am 21.5.2004.

⁴⁶ vgl. Newman: Using TLS with IMAP, POP3 and ACAP.

⁴⁷ vgl. Klensin, J.: Simple Mail Transfer Protocol; in: <ftp://ftp.rfc-editor.org/in-notes/rfc2821.txt> – Zugriff am 21.5.2004.

⁴⁸ vgl. Dierks und Allen: The TLS Protocol Version 1.0.

⁴⁹ vgl. Myers, J.: Local Mail Transfer Protocol; in: <ftp://ftp.rfc-editor.org/in-notes/rfc2033.txt> – Zugriff am 1.8.2004.

⁵⁰ vgl. Fielding, R. et al.: Hypertext Transfer Protocol - HTTP/1.1; in: <ftp://ftp.rfc-editor.org/in-notes/rfc2616.txt> – Zugriff am 21.5.2004.

⁵¹ vgl. Rescorla, E.: HTTP Over TLS; in: <ftp://ftp.rfc-editor.org/in-notes/rfc2818.txt> – Zugriff am 21.5.2004.

⁵² vgl. Postel, J. und Reynolds, J.: File Transfer Protocol; in: <ftp://ftp.rfc-editor.org/in-notes/rfc959.txt> – Zugriff am 21.5.2004.

⁵³ vgl. Wahl, M., Howes, T. und Kille, S.: Lightweight Directory Access Protocol (v3); in: <ftp://ftp.rfc-editor.org/in-notes/rfc2251.txt> – Zugriff am 21.5.2004.

⁵⁴ Es existieren freie Implementierungen, das ursprüngliche HotSync-Protokoll hingegen ist nicht frei verfügbar.

⁵⁵ vgl. Clemm, G. et al.: Web Distributed Authoring and Versioning (WebDAV) Access Control Protocol; in: <ftp://ftp.rfc-editor.org/in-notes/rfc3744.txt> – Zugriff am 14.7.2004.

Die im Kolab Kontext verwendeten, offenen Protokolle und Standards sowie deren Funktionalität im Kolab-Server Konzept werden in dem folgenden Abschnitt näher erläutert.

3.3.1 SSL/TLS

SSL/TLS (Secure Socket Layer/Transport Layer Security) ist ein Protokoll, das der Verschlüsselung von Daten bei der Datenübertragung dient. SSL in der Version 3.0 und TLS in der Version 1.0 unterscheiden sich in ihren Implementierungen nur geringfügig, jedoch wurde das de facto Standard-Verschlüsselungsprotokoll SSL erst mit der Standardisierung durch die IETF (Internet Engineering Task Force) zu einem offiziellen Protokoll mit der neuen Bezeichnung TLS.^{56,57} SSL/TLS ist im Kolab-Konzept als Verschlüsselungsmechanismus für fast alle genutzten Protokolle vorgesehen und erlaubt eine sichere Kommunikation auf Transportebene.

3.3.2 IMAP

IMAP (Internet Message Access Protocol) ist ein standardisiertes, sitzungsorientiertes Protokoll, welches in der Version 4 Revision 1 (IMAP4rev1)⁵⁸ im Kolab-Server Konzept implementiert ist. Dieses Protokoll ermöglicht grundsätzlich den Zugriff auf einen oder mehrere Postkörbe von beliebig verteilten, internetfähigen Arbeitsstationen.⁵⁹ Der entscheidende Unterschied zu anderen Protokollen wie z.B. POP liegt darin, dass E-Mails oder Bulletin-Board-Nachrichten auf dem Server vorgehalten werden und somit für verschiedene Benutzer an verschiedenen Orten zu unterschiedlichen Zeiten verfügbar sind und bearbeitet werden können. Dieser Modus wird als *online mode*⁶⁰ bezeichnet. Die Nachrichten werden also nicht wie bei dem Post Office Protocol vorgelesen auf eine Arbeitsstation heruntergeladen, sondern werden auf dem Server vorgehalten und können dort von berechtigten Nutzern u.a. gelesen, weitergeleitet oder editiert werden. Das Protokoll IMAP4rev1 ermöglicht auch die Synchronisation von Daten im

⁵⁶ vgl. Dierks und Allen: The TLS Protocol Version 1.0.

⁵⁷ vgl. The Mozilla Organization: SSL/TLS; 2002 in: <http://www.mozilla.org/projects/security/pki/nss/ssl/> – Zugriff am 9.8.2004.

⁵⁸ vgl. Crispin: Internet Message Access Protocol - Version 4rev1.

⁵⁹ vgl. Wikipedia Project: Internet Message Access Protocol; 2004 in: <http://de.wikipedia.org/wiki/IMAP> – Zugriff am 14.7.2004.

⁶⁰ vgl. University of Washington: Message Access Paradigms and Protocols; 1995 in: <ftp://ftp.cac.washington.edu/imap/imap.vs.pop> – Zugriff am 14.7.2004.

sog. *disconnected mode*⁶¹, der es einem Benutzer erlaubt, ohne permanente Verbindung zum Server E-Mails oder Kalendereinträge zu bearbeiten und zu einem späteren Zeitpunkt online synchronisieren zu können.

3.3.3 POP3

Das Post Office Protocol in der Version 3 (POP3) dient im Kolab-Konzept der Abholung von E-Mails durch nicht IMAP-fähige E-Mail Clients, wahlweise kann der Transport unverschlüsselt oder über SSL/TLS verschlüsselt durchgeführt werden, je nachdem ob dieser transportbasierte Verschlüsselungsmechanismus von dem Client unterstützt wird oder nicht (wie z.B. bei den sog. *Legacy-Clients*).⁶² Im Gegensatz zu IMAP handelt es sich bei POP3 um ein verbindungsloses Protokoll, d.h. es besteht keine permanente Verbindung zu dem Mail-Server. Dieser Zustand wird auch als *offline mode*⁶³ bezeichnet. Zum Abruf von E-Mail wird eine Verbindung aufgebaut und nach Beendigung der Abholung wieder abgebaut, die Verarbeitung von E-Mails findet lokal auf der Arbeitsstation eines Benutzers statt. POP3 bietet allerdings im Gegensatz zu IMAP Version 4 Revision 1 keine Unterstützung für Clients im *disconnected mode*, d.h. der Funktionsumfang beschränkt sich auf Abholung und Löschung von E-Mails auf dem entsprechenden Server.⁶⁴

3.3.4 SMTP

SMTP (Simple Mail Transfer Protocol) ist ein Protokoll für den Transport von E-Mail zwischen *MTA* (Mail Transport Agent) sowie *MUA* (Mail User Agent). Da SMTP zu den unsicheren Protokollen gehört, ist im Kolab-Konzept der Versand von E-Mails über eine SSL/TLS verschlüsselte Verbindung vorgesehen, also über eine SSL/TLS verschlüsselte SMTP Verbindung (SMTPS). Der Betriebsmodus der unverschlüsselten SMTP-Kommunikation für Legacy-Clients ist möglich.

⁶¹ vgl. University of Washington: Message Access Paradigms and Protocols.

⁶² vgl. Erfrakon: Kolab Web Administration Technical Description; 2003 in: <http://kroupware.org/administration-1.0-html/x181.html> – Zugriff am 14.7.2004.

⁶³ vgl. University of Washington: Message Access Paradigms and Protocols.

⁶⁴ vgl. Wikipedia Project: POP3; 2004 in: <http://de.wikipedia.org/wiki/POP3> – Zugriff am 14.7.2004.

3.3.5 LMTP

Das Local Mail Transfer Protocol (LMTP) ist eine Abwandlung des SMTP und dient der lokalen Zustellung von E-Mail-Nachrichten. LMTP ist eine Alternative zu dem herkömmlichen SMTP und erlaubt den Transport von E-Mail ohne dass die empfangende Applikation über eine E-Mail-Warteschlange verfügen muss, wie z.B. *Mail Delivery Agents* (MDA).⁶⁵

3.3.6 HTTP

„Das Hypertext Transfer Protocol (HTTP) ist ein zustandsloses Datenaustausch-Protokoll zur Übertragung von Daten“⁶⁶ und wird im Kolab Konzept über eine SSL/TLS verschlüsselte Verbindung (HTTPS) vor allem für die Darstellung der webbasierten Administrationsoberfläche mittels eines Browsers genutzt. über die *WebDAV*-Funktionalität – eine Erweiterung des Hypertext Transfer Protocols – ist es KDE Kolab-Clients möglich, Informationen für eine Free/Busy-Liste auf den Kolab-Server zu laden. Das Herunterladen dieser Informationen wird über eine HTTPS-Verbindung durchgeführt, für Legacy-Clients steht diese Funktionalität auch über eine unverschlüsselte HTTP-Verbindung zur Verfügung (siehe Kapitel 3.4.4).

3.3.7 FTP

Das FTP (File Transfer Protocol) wird zur interaktiven Übertragung von Dateien verwendet⁶⁷ und ist in dem RFC (Request for Comment) 959 (siehe Kapitel 3.3) definiert. Im Kolab-Kontext dient das File Transfer Protocol und der damit verbundene FTP-Dienst lediglich der Bereitstellung von Free/Busy Informationen für Legacy-Clients (siehe Kapitel 3.4.5).

3.3.8 LDAP

Das Lightweight Directory Access Protocol (LDAP) ist ein Protokoll, das den Zugriff auf Daten eines Verzeichnisdienstes ermöglicht. LDAP ist eine vereinfachte Imple-

⁶⁵ vgl. Wikipedia Project: Local Mail Transfer Protocol; 2004 in: <http://en.wikipedia.org/wiki/LMTP> – Zugriff am 1.8.2004.

⁶⁶ vgl. Wikipedia Project: Hypertext Transfer Protocol; 2004 in: <http://de.wikipedia.org/wiki/HTTP> – Zugriff am 14.7.2004.

⁶⁷ vgl. Hunt, C.: TCP/IP; Köln 1998.

mentierung des Directory Access Protocol (DAP) X.500 und in seiner Funktionsweise vergleichbar mit dem Domain Name System (DNS).⁶⁸ Es erlaubt jedoch eine Vielzahl weiterer Nutzungsmöglichkeiten, wie z.B. Authentifizierungsdienste. Eine populäre Implementierung des LDAP findet sich in dem Verzeichnisdienst Active Directory von Microsoft.⁶⁹

3.4 Kolab-Server-Komponenten

3.4.1 Cyrus-SASL

Die von der Carnegie Mellon University entwickelte Software *Cyrus-SASL* (Simple Authentication and Security Layer) stellt ein Verfahren zur Authentifizierung und Autorisierung für verbindungsorientierte Protokolle dar.^{70,71} Die durch den Dienst *saslauthd* bereitgestellten Mechanismen sind in dem RFC 2222⁷² beschrieben und werden im Kolab Konzept von Postfix und Cyrus-IMAPd in Verbindung mit OpenLDAP als zentrale Authentifizierungsinstanz für Dienste genutzt (siehe Abbildung 3.1). Die in der LDAP-Datenbank vorgehaltenen Daten dienen hierbei als Grundlage für den Authentifizierungsvorgang.⁷³

3.4.2 Cyrus-IMAPd

Cyrus-IMAPd ist ein IMAP4rev1- und POP3-fähiger IMAP Server, der Nachrichten im *maildir*-Format verarbeitet und die Mailbox-Datenbank in einem speziell für Cyrus-IMAPd berechtigten Bereich des Filesystems auf dem Kolab-Server vorhält. Der IMAP Server entnimmt die Mail-Benutzer der LDAP-Datenbank, allerdings gilt dies nicht für IMAP-Benutzergruppen, diese werden nicht in der LDAP-Datenbank vorgehalten. Cyrus-IMAPd entnimmt in diesem Fall die Gruppenzugehörigkeiten der Datei `/etc/imapd.group`.⁷⁴ über SMTP eingehende Nachrichten erhält Cyrus-IMAPd von Postfix über die gemeinsam unterstützte LMTP-Schnittstelle.

⁶⁸ vgl. Carter, G.: LDAP System Administration; Sebastopol 2003, S. 4.

⁶⁹ vgl. Kuppinger, M.: Windows 2000 Server Das Handbuch; Unterschleißheim 2000.

⁷⁰ vgl. Klünter, D. und Laser, J.: LDAP verstehen, OpenLDAP einsetzen; Heidelberg 2003, S. 119.

⁷¹ vgl. Myers, J.: Simple Authentication and Security Layer (SASL); in: <ftp://ftp.rfc-editor.org/in-notes/rfc2222.txt> – Zugriff am 04.07.2004.

⁷² vgl. Myers: Simple Authentication and Security Layer (SASL).

⁷³ vgl. Kolab Project: The Kolab Project::Home.

⁷⁴ vgl. Erfrakon: Kolab Server Technical Description; 2003 in: <http://kroupware.org/technical-1.0.1-html/c368.html> – Zugriff am 13.7.2004.

Die für den Kolab-Server entscheidenden Funktionen des Cyrus-IMAPd sind:⁷⁵

- hohe Skalierbarkeit
- Unterstützung von *ACL* (Access Control List)
- Unterstützung gemeinsam genutzter IMAP-Postkörbe
- Trennung von Systembenutzern und Mail-Konten
- Nutzung des Dateisystems als indizierte hierarchische Datenbank
- Unterstützung von IMAP und POP3 über SSL/TLS
- Benutzerauthentifizierung über SASL gegen LDAP
- Unterstützung der Skriptsprache *Sieve* (siehe Kapitel 4.6.1)
- Unterstützung des LMTP-Mechanismus

3.4.3 Postfix

Postfix ist in dem Kolab-Konzept für den Transport von eingehenden E-Mails vorgesehen. Der MTA arbeitet als SMTP-Relay und unterstützt SMTP über SSL/TLS, unverschlüsseltes SMTP für Legacy-Clients und LDAP-Authentifizierung über SASL. Bei dem Versand von Nachrichten authentifizieren sich Benutzer gegen die LDAP-Datenbank. Postfix übergibt nach erfolgreicher Anmeldung eingehende Nachrichten an den LMTP-Daemon, der als Schnittstelle zwischen Postfix und Cyrus-IMAPd dient.

Die im Zusammenhang mit Kolab entscheidenden Funktionen von Postfix sind:⁷⁶

- einfache Konfiguration
- Sendmail Kompatibilität
- hohe Sicherheit
- hohe Skalierbarkeit

⁷⁵ vgl. Erfrakon: Kolab Server Technical Description; 2003 in: <http://kroupware.org/technical-1.0.1-html/c27.html> – Zugriff am 13.7.2004.

⁷⁶ vgl. Erfrakon: Kolab Server Technical Description.

- SMTP-Unterstützung
 - Unterstützung von SMTP über SSL/TLS
 - SMTP-Authentifizierung gegen LDAP über SASL
- Unterstützung des LMTP Mechanismus

Cyrus-IMAPd und Postfix sind ein wichtiger Bestandteil des Kolab-Servers als Schnittstelle für eingehende und ausgehende E-Mail. Postfix und Cyrus-IMAPd unterstützen eine Vielzahl offener Protokolle und Standards, die für die Zielsetzung des Kolab-Server als sicherer und flexibler Groupware-Server maßgeblich sind. Die verschiedenen Modi beim Senden und Empfangen von E-Mail sowie die Integration von Postfix, Cyrus-IMAPd, LMTP in Verbindung mit Kolab-Clients stellt Abbildung 3.2 dar.

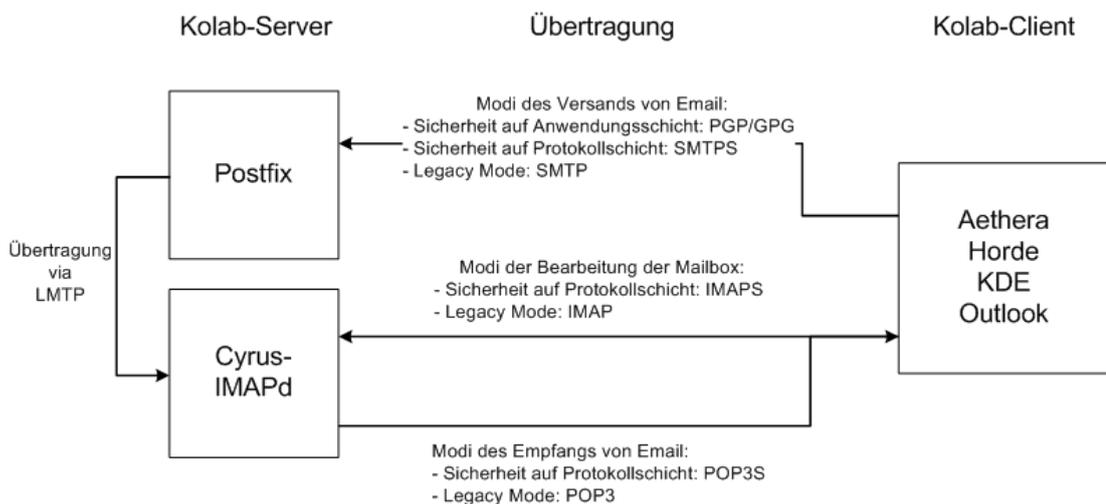


Abbildung 3.2: E-Mail-Datenfluss im Kolab Konzept⁷⁷⁷⁸

3.4.4 Apache

Die folgenden Funktionalitäten waren für den Einsatz des Apache Webservers im Hinblick auf Kolab ausschlaggebend:⁷⁹

- Authentifizierung gegen LDAP

⁷⁷ vgl. Erfrakon: Free Software Groupware Project - Architecture Paper; 2003 in: <http://kroupware.org/architecture-1.1/x124.html> – Zugriff am 13.7.2004

⁷⁸ vgl. Erfrakon: Free Software Groupware Project - Architecture Paper; 2003 in: <http://kroupware.org/architecture-1.1/x133.html> – Zugriff am 13.7.2004

⁷⁹ vgl. Erfrakon: Kolab Server Technical Description.

- HTTP über SSL/TLS-verschlüsselte Verbindungen
- WebDAV-Unterstützung
- PHP-Unterstützung

Die erweiterten Funktionalitäten des Apache Webservers wie LDAP-Authentifizierung, SSL/TLS-Verschlüsselung oder WebDAV-Unterstützung wird durch das Einbinden der Apache-Module `mod_ldap`, `mod_ssl` und `mod_dav` erreicht. Bei der Anmeldung eines Benutzers am Webinterface werden Benutzername sowie Passwort abgefragt und mit den Einträgen in der LDAP-Datenbank verglichen. Die Datenübertragung erfolgt dabei über eine verschlüsselte HTTP-Verbindung. Das Webserver-Zertifikat, das zur Initialisierung der verschlüsselten Verbindung dient, wird bei der Installation des Kolab-Server automatisch erzeugt und ist für den Zeitraum von einem Jahr gültig. Das WebDAV-Modul dient dem Upload von Free/Busy-Informationen für KDE Kolab-Clients, der Download wird über eine HTTPS-Verbindung vorgenommen.

3.4.5 ProFTPD

ProFTPD besitzt ähnlich wie der Apache Webserver ein LDAP-Modul, das die Authentifizierung von Benutzern gegen die LDAP-Datenbank ermöglicht. In Verbindung mit Kolab dient der ProFTPD-Server allein der Unterstützung von anonymen Free/Busy-Uploads für Legacy-Clients⁸⁰ wie z.B. Microsoft Outlook 2000.

3.4.6 OpenLDAP

Der im Kolab Konzept genutzte LDAP-Dienst basiert auf den Entwicklungen des Open Source Projekts OpenLDAP.⁸¹ Die LDAP-Datenbank dient als zentrale Instanz des gesamten Konstrukts, in ihr werden Konfigurationsparameter der Dienste, Authentifizierungsinformationen, Benutzerdaten, gemeinsam genutzte IMAP-Verzeichnisse und Adressdaten gespeichert und organisiert. Zudem stehen für diese Verzeichnisdatenbank viele nützliche Werkzeuge zur Verfügung (siehe Kapitel 3.4.6), durch die Datensicherung, Datenrücksicherung, Replizierung und automatisierte Datenmanipulation ermöglicht werden. In diesem Konzept wird aus Sicherheitsgründen die Manipulation von Daten nur anhand verschiedener Benutzer- bzw. Gruppenberechtigungen

⁸⁰ vgl. Erfrakon: Free Software Groupware Project - Architecture Paper; 2003 in: <http://kroupware.org/architecture-1.1/x154.html> – Zugriff am 14.7.2004.

⁸¹ vgl. OpenLDAP Foundation: openLDAP; 2004 in: <http://www.openldap.org/> – Zugriff am 11.5.2004.

ermöglicht, die Art und Umfang des Zugriffs auf die durch den LDAP-Dienst vorgehaltenen Daten reglementieren. Dies wird durch eine in der LDAP-Konfigurationsdatei `slapd.conf` standardisierte und konfigurierbare ACL (Access Control List) definiert, die vorgibt, welcher Benutzer bzw. welches Gruppenmitglied bestimmte Zugriffsrechte auf Teile der Daten hat.

Als Vorgabe wird bei der Konfiguration des Kolab-Servers standardisiert der Benutzer *manager* eingerichtet, der administrativen Zugriff auf alle in der LDAP-Datenbank gespeicherten Daten hat. Darüber hinaus werden die Gruppen *Administrator* und *Maintainer* eingerichtet, deren Mitglieder bestimmte Berechtigungen zur Administration verschiedener Bereiche der LDAP-Daten haben. Angehörige der Gruppe *Maintainer* dürfen lediglich Userdaten und Adressbücher manipulieren, während Mitglieder der Gruppe *Administrator* – zu denen auch der Benutzer *manager* gehört – sowohl Userdaten, Adressbücher als auch die Serverkonfiguration verändern dürfen. Abbildung 3.3 verdeutlicht die Rechtestruktur der verschiedenen Gruppen und deren Mitglieder.

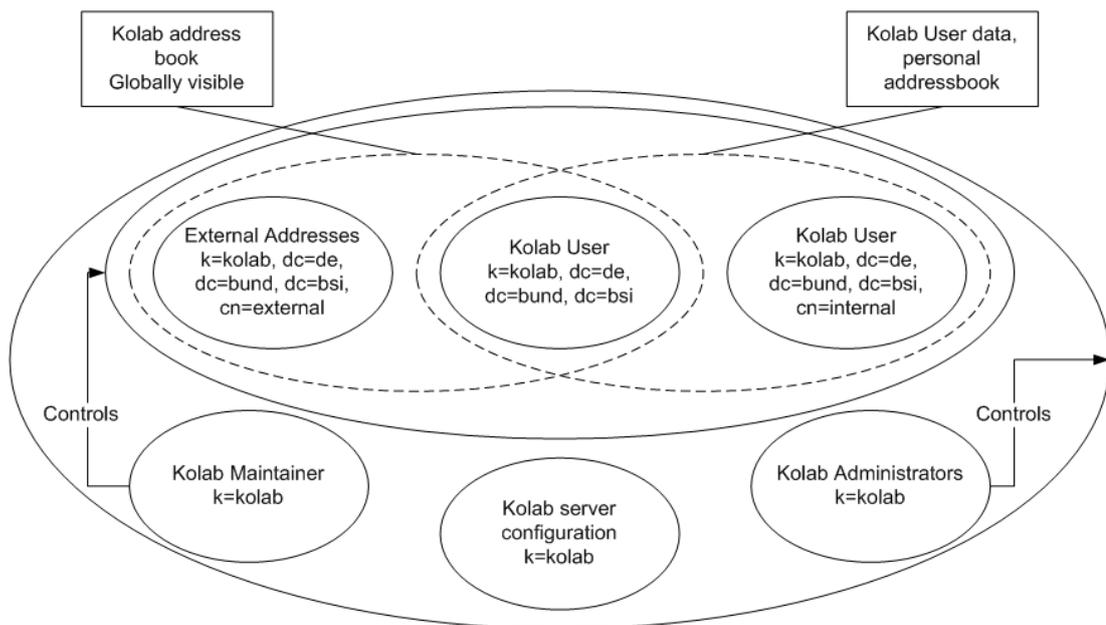


Abbildung 3.3: Kolab Administrationskonzept⁸²

Die Administration eines Kolab-Servers erfolgt über ein PHP-basiertes Webinterface (siehe Kapitel 3.4.8), an dem sich Benutzer oder Administratoren authentifizieren und anschließend die in der LDAP-Datenbank gespeicherten Daten abhängig von deren Zugriffsrechten manipulieren können. Die Authentifizierung erfolgt über die in der LDAP-Datenbank gespeicherten Benutzerdaten wie Benutzername und Benutzerpass-

⁸² vgl. Kroupware Project: Design Criteria; 2003 in: <http://kroupware.org/administration-1.0-html/c24.html> – Zugriff am 11.6.2004, S. 3.

wort. Anhand der Gruppenzugehörigkeit werden dem angemeldeten Benutzer bestimmte Rechte eingeräumt, die es ihm erlauben

- im Falle eines höher privilegierten Benutzers (Mitglieder der Gruppen Administrator oder Maintainer) Änderungen an der Serverkonfiguration bzw. den Benutzerdaten vorzunehmen oder
- im Falle eines normal privilegierten Benutzers Zugriff auf eigene, benutzerbezogene Daten zu erhalten und dort Änderungen vorzunehmen, wie z.B. die Änderung des Passworts oder Einstellungen zu Abwesenheitsbenachrichtigungen.

Um die Ausfallsicherheit des LDAP-Dienstes zu erhöhen, enthält das OpenLDAP-Installationspaket einen Replikationsdienst *slurpd*, der Änderungen an der LDAP-Datenbank auf einen *Slave-Server* repliziert (siehe Kapitel 3.2). In der interaktiv erzeugten Grundkonfiguration (siehe Kapitel 4.1.4) der betrachteten Version des Kolab-Servers wird in der Konfigurationsdatei `slapd.conf` des LDAP-Dienstes kein Replikationsserver eingetragen und auch die Konfiguration eines Slave-Servers ist im administrativen Bereich des Webinterface nicht vorgesehen. Die Eintragung eines Replikationsservers ist durch manuelle Modifikation in der Konfigurationsdatei des LDAP-Dienstes vorzunehmen, welche in der OpenLDAP Dokumentation⁸³ näher beschrieben ist.

Der LDAP-Dienst nutzt in der Kolab-Standardkonfiguration *back-ldbm* (Lightweight DBM) als Datenbank-Schnittstelle (sog. Datenbank-Backend) in Verbindung mit BerkeleyDB als Datenbank. Dieses Backend ist in der Standardkonfiguration durch Indizierung der zugrunde liegenden Datenbank auf Lesezugriffe optimiert und nutzt mehrere Indizes wie *id2entry* oder *dn2id* zur Optimierung der Performanz von Abfragen.⁸⁴ Für *back-ldbm* stehen nützliche Administrationswerkzeuge zur Erstellung von Datenbankauszügen (sog. *dumps*) oder automatisierten Operationen zur Verfügung. Eine Sicherung der Datenbank zur Laufzeit ist mit diesem Backend allerdings nicht möglich.⁸⁵ Wird eine Änderung an einem der Kolab-Komponenten vorgenommen, sorgt ein *Perl*-basiertes (siehe Kapitel 3.4.7) Skript (das sog. Kolab-Backend) für die Änderung der Objekte und Attributwerte in der LDAP-Datenbank und ändert die entsprechenden Parameter in den Konfigurationsdateien der betroffenen Dienste. Diese Dienste werden –

⁸³ vgl. OpenLDAP Foundation: openLDAP 2.2 Administrators Guide: Replication with slurpd; 2004 in: <http://www.openldap.org/doc/admin22/replication.html> – Zugriff am 11.5.2004.

⁸⁴ vgl. Chu, H.: RE: Backend databases – what are the differences? in: <http://www.openldap.org/lists/openldap-software/200209/msg00167.html> – Zugriff am 11.5.2004.

⁸⁵ vgl. Chu: RE: Backend databases – what are the differences?.

wenn nötig – nach Änderung der Parameter neu gestartet, ohne dass ein Neustart des gesamten Kolab-Servers notwendig ist.

3.4.7 Perl

Perl ist eine Skriptsprache, die im Kolab-Konzept dazu dient, mittels angepasster Module eine Modifikation der Konfigurationsdateien der einzelnen Dienste oder Daten der LDAP-Datenbank vorzunehmen. Das Kolab-Backend basiert auf einem Perl-Skript, welches in einer Endlosschleife die LDAP-Datenbank auf Änderungen überwacht⁸⁶ und bei Bedarf die Konfigurationsdateien der Kolab Dienste modifiziert (siehe Kapitel 3.2).

3.4.8 PHP

PHP (Hypertext Preprocessor) ist eine Skriptsprache für Webserver und bietet die Möglichkeit, dynamische Webseiten zu erstellen.⁸⁷ Das Webinterface des Kolab-Servers ist in PHP4 geschrieben und nutzt das Apache-Modul `mod_php` zur Darstellung der Formulare, die die graphische Administration des Servers ermöglichen.⁸⁸

3.5 Funktionsbetrachtung

In den folgenden Abschnitten sollen die gebotenen Funktionen des Kolab-Servers in Verbindung mit Kolab-Clients anhand verschiedener Kriterien dargestellt werden.

3.5.1 Unterstützte Funktionen

Der Kolab-Server bietet auf Basis der genannten Protokolle und Dienste die folgenden Funktionen:

- E-Mail Zugriff über POP3 bzw. POP3S sowie
- IMAP bzw. IMAPS

⁸⁶ vgl. Erfrakon: Kolab Server Technical Description.

⁸⁷ vgl. Kronsbein, M. und Weinert, T.: PHP4; Düsseldorf 2001, S. 1.

⁸⁸ vgl. Erfrakon: Kolab Web Administration Technical Description; 2003 in: <http://kroupware.org/administration-1.0-html/c44.html> – Zugriff am 15.7.2004.

- Mail Filtering mittels Sieve (siehe Kapitel 3.5.2)
- Adressbücher mit Hilfe von LDAP
- Free/Busy View für Outlook 2000 Clients über FTP und HTTP
- Administration über ein Webinterface
- Verschlüsselung auf Applikations- und Transportebene

3.5.2 Sicherheit

Ein Schwerpunkt bei der Entwicklung von Kolab war die Implementierung von Sicherheitsmechanismen auf Applikations- und Transportebene. Auf Seite des KDE Kolab-Clients kann optional die ebenfalls im Rahmen eines von dem BSI ausgeschriebenen Projekts *ägypten*^{89, 90} entwickelte *PKI* (Public Key Infrastructure) zur Verschlüsselung von E-Mail eingesetzt werden. Die Kommunikation des Clients mit dem Server erfolgt über SSL/TLS-verschlüsselte Protokolle wie SMTPS oder IMAPS. Für Webclients wie *Horde* (siehe Kapitel 5.4) ist eine über SSL/TLS-verschlüsselte HTTP-Datenübertragung vorgesehen. Die Nutzung der Free/Busy-Liste in Verbindung mit Outlook 2000 Clients stellt ein Sicherheitsrisiko dar, da hier Authentifizierungsdaten im Klartext übertragen werden. Wird kein Legacy-Client eingesetzt, kann die Free/Busy-Liste mittels des WebDAV-Moduls über SSL/TLS verschlüsselt bereitgestellt werden. Ein weiterer Sicherheitsaspekt des Kolab-Konzepts ist die Implementierung von verschiedenen Benutzerrollen in Verbindung mit administrativen Beschränkungen. Durch die Verwendung einer ACL sind die Berechtigungen der Benutzer bei Zugriff auf Verzeichnisse oder Postkörbe definierbar.

Auf der Seite des Kolab-Servers sind aufgrund der flexiblen Kolab-Komponenten verschiedene Mechanismen hinsichtlich der Ausfallsicherheit realisierbar. Diese Thematik wird jedoch gesondert in Kapitel 4.3 behandelt und soll an dieser Stelle nicht weiter vertieft werden. In der in dieser Arbeit betrachteten Kolab-Version 1.0.8 werden sowohl Benutzer- als auch Administrator Passwörter in Klartext in der LDAP-Datenbank vorgehalten. Diese werden zwar auf Transportebene verschlüsselt, dennoch besteht bei

⁸⁹ vgl. Bundesamt für Sicherheit in der Informationstechnik: Sphinx Open Source; 2004 in: <http://www.bsi.de/aufgaben/projekte/sphinx/aegypten/opensource.htm> – Zugriff am 10.6.2004.

⁹⁰ vgl. Klarälvdalens Datakonsult AB: KMail and mutt as Sphinx clients for German authorities; 2002 in: <http://www.klaralvdalens-datakonsult.se/?page=projects&sub=aegypten> – Zugriff am 15.7.2004.

entsprechenden Zugriffsrechten auf den LDAP-Dienst die Möglichkeit, alle Benutzerpasswörter auszulesen, obwohl diese mit den von LDAP unterstützten Mechanismen *CRYPT*, *SHA*, *SSHA*, *MD5* oder *SMD5* verschlüsselt werden könnten.⁹¹ In zukünftigen Versionen von Kolab soll dieser Mangel allerdings behoben sein.⁹² Als optionale Sicherheitsmechanismen des Kolab-Servers sind *AMaViS* (A Mail Virus Scanner) und *Sieve* zu nennen (siehe Kapitel 4.6.1). Es handelt sich bei *AMaViS* um eine Open Source-Schnittstelle für Virenschanner, die den E-Mail Verkehr auf Viren untersucht und somit die Verbreitung von Schädlingen – besonders im Hinblick auf Microsoft-basierte Clients – eindämmen kann. *Sieve* ist eine Skriptsprache, mit deren Hilfe Spamnachrichten ausgefiltert werden können; dies führt nur sekundär zu erhöhter Sicherheit, kann aber durchaus dazu beitragen, virenverseuchte Spam-Mails nicht zuzustellen und somit eine Sicherheitsgefährdung zu minimieren. Für den Einsatz von *Sieve* im Kolab Kontext steht eine Online-Dokumentation⁹³ zur Verfügung. Der rechtmäßige Einsatz dieser Erweiterungen ist jedoch generell fragwürdig, da das Löschen, Unterdrücken oder Verändern von Daten gegen geltendes Recht des Strafgesetzes und des Telekommunikationsgesetzes verstößt.⁹⁴

3.5.3 Plattformunabhängigkeit

Die Plattformunabhängigkeit des Kolab-Servers wird vor allem dadurch gewährleistet, dass er durch die Installation auf Basis von OpenPKG-Softwarepaketen (siehe Kapitel 4.1.1) auf vielen Unix-Derivaten wie z.B. FreeBSD, Debian Linux, Red Hat Linux, SuSE Linux oder Sun Solaris lauffähig ist.

Je nachdem welcher Client für den Zugriff auf den Kolab-Server eingesetzt wird, ist die Anzahl der unterstützten Plattformen groß. Der Outlook 2000 Client ist für die Betriebssysteme Windows NT 4 Workstation, 95, 98, 2000, ME und Mac OS 8 erhältlich, der Aethera-Client mit Kolab Unterstützung steht für die Betriebssysteme Mac OS, Linux sowie Windows zur Verfügung. Der KDE Kolab-Client hingegen ist unter allen Betriebssystemen nutzbar, für die auch der Desktop Manager KDE zur Verfügung ste-

⁹¹ vgl. OpenLDAP Foundation: man slappasswd; 2000 in: http://gd.tuwien.ac.at/linuxcommand.org/man_pages/slappasswd8.html – Zugriff am 10.6.2004.

⁹² vgl. Konold, M.: No Password Encryption? in: <http://www.kolab.org/pipermail/kolab-users/2004-May/000415.html> – Zugriff am 10.6.2004.

⁹³ vgl. Kroupware Project: Kroupware Project Frequently-Asked Questions; 2003 in: <http://www.erfrakon.de/projects/kolab/documentation/faq/faq.html#Kolab%20Server1> – Zugriff am 10.6.2004.

⁹⁴ vgl. Andresen, F.: Leeren verboten! in: Linux Magazin 9 2004, S. 78–79.

ht.⁹⁵ Dies sind nahezu alle bekannten Linux Distributionen, BSD-Derivate als auch IBM AIX, Mac OS X und Sun Solaris.

Wird ein Web-Client genutzt, ist prinzipiell jedes Betriebssystem mit einem aktuellen Browser für den Zugriff auf den Kolab-Server geeignet.

⁹⁵ vgl. KDE e.V.: Distributions shipping KDE; 2004 in: <http://www.kde.org/download/distributions.php> – Zugriff am 12.5.2004.

<

4 Praktische Betrachtung des Kolab-Servers

4.1 Kolab-Server Installation

Die im Rahmen dieser Arbeit durchgeführten Installationen des Kolab-Server wurden auf den Plattformen Red Hat Linux 9, Fedora Linux Core 1, Mandrake Linux 10, Debian Linux 3.0 und SuSE Linux 9.1 getestet. Die Mandrake Linux Distribution in der Version 10 hat Kolab-Server in der Version 1.0 als RPM-Installationspaket in den Distributionsumfang aufgenommen.

4.1.1 OpenPKG

Alle Kolab-Installationsverfahren mit Ausnahme der Mandrake Linux 10 Distribution basieren auf den Softwarepaketen des OpenPKG-Projekts.⁹⁶ OpenPKG ist ein auf dem Red Hat Package Manager⁹⁷ (RPM) Version 4 basierender Paketmanager, der über einen *Bootstrap*-Mechanismus installiert wird. Dieser Mechanismus erzeugt ein eigenes Dateisystem innerhalb des Dateisystem-Baums des Betriebssystems, in dem die für Kolab notwendigen Pakete installiert werden. Binary-Pakete werden zur Zeit für die Plattformen SuSE 9.0, SuSE 8.2, Red Hat 9, Red Hat Enterprise Linux 3, Gentoo 1.4.3, FreeBSD 5.2, FreeBSD 4.9, Fedora Core 1, Debian 3.1, Debian 3.0 und Debian 2.2 angeboten. Neben dem Aspekt der Plattformunabhängigkeit (siehe Kapitel 3.5.3) bietet die auf OpenPKG basierende Kolab-Server-Installation den Vorteil, dass sicherheitsrelevante Update-Pakete innerhalb kurzer Zeit durch das OpenPKG-Projekt zur Verfügung⁹⁸ gestellt werden können. Dieser Vorteil ist darin begründet, dass im

⁹⁶ vgl. The OpenPKG Project: openPKG Cross Platform Unix Software Packaging; 2004 in: <http://www.openpkg.org/> – Zugriff am 11.5.2004.

⁹⁷ vgl. RPM Community: RPM HOWTO; 1999 in: <http://www.rpm.org/RPM-HOWTO/#INTRO> – Zugriff am 10.7.2004.

⁹⁸ vgl. The OpenPKG Project: Security; 2003 in: <http://www.openpkg.org/security.html> – Zugriff am 10.7.2004.

Gegensatz zu den Software-Updates der Distributoren nur Updates für die OpenPKG-Umgebung entwickelt werden müssen und nicht für alle Betriebssystemversionen bzw. Prozessorarchitekturen.

4.1.2 Wahl der Installationsalternativen

Die Installation eines Kolab-Servers kann auf verschiedene Arten durchgeführt werden, da mehrere alternative Installationspakete zur Verfügung stehen. Die Installationsdokumentation⁹⁹ der Kroupware Homepage beschreibt die notwendigen Schritte, um den Kolab-Server mit Source-Paketen im RPM-Format zu installieren, deren Installation aufgrund des Aufwands für die Kompilierung allerdings recht zeitaufwändig ist. Wird eine einfachere Vorgehensweise bei der Installation bevorzugt, so können die für den Kolab-Server benötigten Komponenten in Form von plattformspezifisch angepassten RPM-Paketen inklusive des Paketmanagers OpenPKG von dem ZfOS-Archiv¹⁰⁰ heruntergeladen und mit Hilfe der bereitgestellten Installationsdokumentation¹⁰¹ installiert werden.

4.1.2.1 Installation mittels Source-RPM-Paketen

Die ursprünglichen, im Rahmen des Kroupware Projekts entwickelten Installationspakete des Kolab Servers 1.0 sind im RPM-Format erhältlich und beinhalten den für die Kompilierung der Software notwendigen Sourcecode der jeweiligen Kolab-Server Komponenten, wie z.B. Apache, ProFTPD oder Postfix, aber auch die für die Kompilierung notwendigen Werkzeuge wie C-Compiler, Bibliotheken und Linker sowie einige zusätzliche Werkzeuge. Die Grundlage für den Beginn einer Installation schafft das OpenPKG Bootstrap-Skript, welches eine eigenständige Dateisystem-Struktur unter einem gewünschten Mountpoint anlegt, in dem später die Kolab-Software unabhängig von dem zugrunde liegenden Betriebssystem installiert werden soll. Diese Installationsvariante bietet im Vorfeld die Möglichkeit, weitere Anpassungen hinsichtlich gewünschter Funktionalitäten während der Kompilation vorzunehmen, indem die Software mit den gewünschten Unterstützungsparametern (sog. *flags*) kompiliert wird.

⁹⁹ vgl. Konold, M.: Quick Install Manual Kolab 1.0.4; in: <http://www.erfrakon.de/projects/kolab/download/kolab-server-1.0/src/QIM> – Zugriff am 15.5.2004.

¹⁰⁰ vgl. Zen for Open Source: Zen for Open Source; 2004 in: <ftp://ftp.zfos.org/brew/kolab/BIN/kolab-20040217-2.0.0/ix86-fedora1/> – Zugriff am 15.5.2004.

¹⁰¹ vgl. Zen for Open Source: Zen for Open Source; 2004 in: <ftp://ftp.zfos.org/brew/kolab/BIN/kolab-20040217-2.0.0/ix86-fedora1/README> – Zugriff am 15.5.2004.

4.1.2.2 Installation plattformspezifischer OpenPKG-Pakete

Die Installation von Kolab mittels der für das jeweilige Betriebssystem (siehe Kapitel 3.5.3) vorkompilierten Pakete und dazugehörigem Installationskript erlaubt eine schnelle und einfache Handhabung im Vergleich zu der Installation auf Basis von Source RPM-Paketen. Eine Liste der erhältlichen Pakete findet sich im FTP-Archiv des ZfOS.¹⁰² Die Pakete werden mit Hilfe des Installationskriptes `obmtool` und der zugehörigen Konfigurationsdatei `obmtool.conf` weitestgehend automatisiert installiert, nachdem zuvor die notwendige OpenPKG-Umgebung durch ein Bootstrap-Skript erzeugt wurde. Die entsprechende Installationsdokumentation¹⁰³ liefert einige weitere Informationen zur Vorgehensweise. Sollen wie im vorherigen Abschnitt beschrieben bei der Installation Funktionsanpassungen vorgenommen werden, so sind diese in die Datei `obmtool.conf` einzutragen.

4.1.2.3 Installation unter Mandrake Linux

Mandrake Linux ist bislang der einzige Linux Distributor, der den Kolab-Server 1.0 in den Lieferumfang von Mandrake Linux 10 aufgenommen hat (siehe Kapitel 4.1). Hierbei werden die Komponenten des Kolab-Servers nicht in einer gesonderten OpenPKG-Umgebung installiert, sondern an der durch den Distributor vorgesehenen Stelle im Dateisystem. Mandrake bietet neben dem Kolab-Server auch KDE Kolab-Client Installationspakete an; diese können in Mandrake Entwicklerversionen (sog. *Cooker*-Pakete) von den entsprechenden FTP Spiegel-Servern¹⁰⁴ heruntergeladen werden.

4.1.3 Installation einer Referenzplattform

Dieser Abschnitt zeigt die optimalen Voraussetzungen sowie die Möglichkeiten für die Installation eines Kolab-Servers auf der Basis eines auf Red Hat basierenden Betriebssystems wie z.B. Mandrake Linux, Fedora Linux oder Red Hat Enterprise Linux auf.

¹⁰²vgl. Zen for Open Source: Zen for Open Source; 2004 in: <http://www.zfos.org/> – Zugriff am 15.5.2004.

¹⁰³vgl. Zen for Open Source: Brewing Facts Kolab; 2004 in: <ftp://ftp.zfos.org/brew/kolab/BIN/kolab-20040217-2.0.0/ix86-fedora1/README> – Zugriff am 25.7.2004.

¹⁰⁴vgl. MandrakeSoft: Want to download Mandrakelinux? 2004 in: <http://www.mandrakelinux.com/en/ftp.php3> – Zugriff am 25.7.2004.

4.1.3.1 Paketauswahl

Die für eine Betriebssysteminstallation gewählten Softwaregruppen sind für die Installation von Kolab nicht relevant, denn eine Minimalinstallation enthält bereits die erforderlichen betriebssystemseitigen Voraussetzungen (siehe Kapitel 4.2.2) für die Installation eines Kolab-Servers, da alle für die Installation von Kolab benötigten Softwarekomponenten bereits im Umfang der OpenPKG-Pakete enthalten sind.

4.1.3.2 Update des Betriebssystems

Um bekannte Softwarefehler oder Sicherheitslücken weitestgehend ausschliessen zu können, ist ein Software-Update des Betriebssystems zu empfehlen. Downloadmöglichkeiten für Update-Pakete können auf den Internetseiten des jeweiligen Distributors in Erfahrung gebracht werden. Nach dem Herunterladen der Update-Pakete wird die Aktualisierung des Betriebssystems durchgeführt:

```
[root@fc1 updates]# rpm -Fvh *.rpm
```

```
[...]
```

4.1.3.3 Deaktivierung von Diensten

Nach Installation der Update-Pakete sollten die nicht benötigten Dienste deaktiviert werden, um mögliche Konflikte aufgrund kollidierender Dienste bzw. belegter Ports nach Installation des Kolab-Servers zu vermeiden und unnötig belegte Systemressourcen freizugeben. Bei den auf Red Hat basierenden Systemen wird das Start- bzw. Stopverhalten in den verschiedenen Runleveln üblicherweise mit dem Befehl `chkconfig` gesteuert:

```
[root@fc1 root]# chkconfig --level 2345 iptables off
```

```
[root@fc1 root]# chkconfig --level 2345 sendmail off
```

```
[root@fc1 root]# chkconfig --level 2345 httpd off
```

```
[...]
```

Die Abschaltung der Dienste sollte den gegebenen Umständen entsprechend gewählt werden, beispielsweise ist es wenig ratsam den Firewalldienst `iptables` in einer kritischen Umgebung ohne zusätzliche Firewall abzuschalten. Je nachdem wie der

Firewall-Dienst konfiguriert ist, können die von Kolab genutzten Ports geblockt werden, was zu einer eingeschränkten Funktion führt. Eine Aufstellung der von Kolab genutzten Ports findet sich in dem Kapitel 4.2.4. Nach der Deaktivierung der nicht benötigten Dienste und dem Update der Betriebssystemsoftware sollte in jedem Fall ein Reboot durchgeführt werden.

4.1.3.4 Installation von Kolab

Die für die Installation von Kolab notwendigen Software-Pakete können von dem ZfOS-Archiv heruntergeladen und durch die Eingabe des Befehls

```
[root@fcl kolab]# sh obmtool kolab
```

installiert werden. Hierzu dient das Skript `obmtool` und die dazugehörige Konfigurationsdatei `obmtool.conf`, mit deren Hilfe die Installation gesteuert wird. Zu Beginn der Installation wird die für die Installation notwendige OpenPKG-Umgebung üblicherweise unterhalb des Verzeichnisses `/kolab` im Dateisystem des Betriebssystems angelegt, dieser Vorgang wird auch als *bootstrapping* bezeichnet (siehe Kapitel 4.1.1). Im Anschluss daran werden die für die Installation von Kolab notwendigen OpenPKG-Pakete in dieser Umgebung installiert. Eine ausführliche Auflistung des Installationsverlaufs befindet sich in Kapitel 4.4.5.

4.1.4 Kolab Bootstrap-Prozess

Der Kolab Bootstrap-Prozess dient der Konfiguration der einzelnen Dienste und ist von dem OpenPKG Bootstrap-Prozess zu unterscheiden. Für die Konfiguration des Kolab-Servers wird das Kolab-Bootstrap-Skript mit dem Befehl `/kolab/etc/kolab/kolab_bootstrap -b` ausgeführt. Nachdem der Benutzer in einem interaktiven Kontext alle notwendigen Daten wie Hostname, Maildomain und das Passwort des Benutzers `manager` eingegeben hat, wird die Kolab Konfigurationsdatei `/kolab/etc/kolab/kolab.conf` erzeugt. Im nächsten Schritt des Bootstrap-Prozesses wird ein auf Perl basierender *Template Generator* aufgerufen, der mit Hilfe von Konfigurationsvorlagen für die Kolab-Dienste und den vom Administrator eingegebenen Daten die Konfigurationsdateien der Kolab-Komponenten erzeugt.

Nachdem die Konfigurationsdatei `/kolab/etc/openldap/slapd.conf` des

LDAP-Servers erzeugt wurde, wird nun eine LDIF-Datei (LDAP Data Interchange Format) anhand der entsprechenden Benutzereingaben generiert. Eine LDIF-Datei wird für den Import bzw. Export von Daten der LDAP-Datenbank genutzt, in ihr kann die Datenbank in Form einer strukturierten Textdatei abgebildet werden. Um das überschreiben einer u.U. schon vorhandenen LDAP-Datenbank zu vermeiden, wird die eventuell bestehende Datenbank in eine Backup-LDIF-Datei exportiert. Anschliessend wird die im Bootstrap-Prozess generierte LDIF-Datei mit den vom Administrator eingegebenen Daten importiert und die LDAP-Datenbank neu aufgebaut. Abbildung 4.1 verdeutlicht schrittweise den o.g. Verlauf des Kolab Bootstrap-Prozesses.

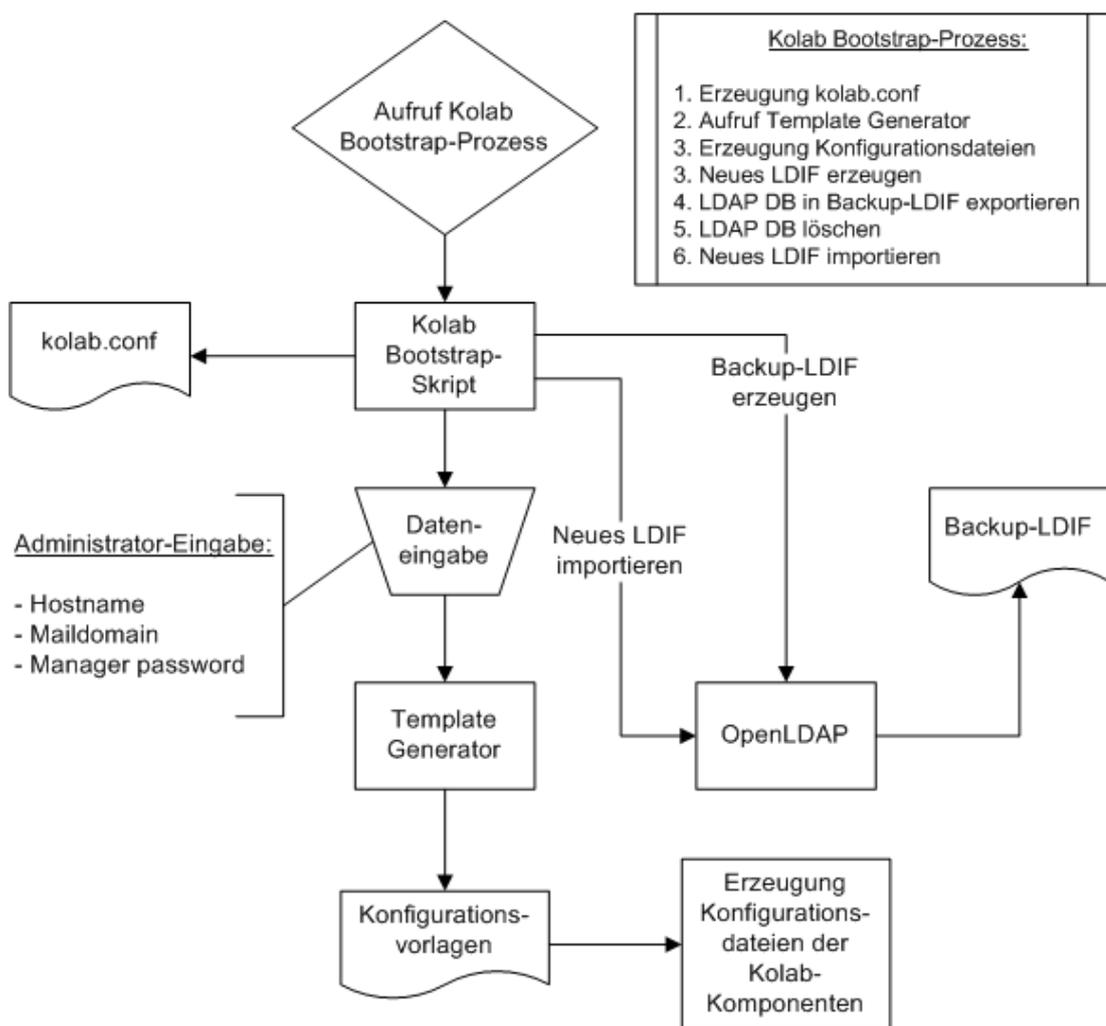


Abbildung 4.1: Der Kolab Bootstrap-Prozess¹⁰⁵

¹⁰⁵vgl. Code Fusion CC and Radley Network Technologies CC: Kolab Bootstrap Process; 2004 in: <http://ftp.intevation.de/kolab/contrib/kolab-bootstrap.pdf> – Zugriff am 20.5.2004, S. 2.

Nachdem die LDAP-Datenbank erzeugt wurde, wird nun das Skript `/kolab/etc/kolab/kolab_sslcert.sh` aufgerufen, um die notwendigen SSL-Zertifikate zu erzeugen. Im letzten Schritt kann der Kolab-Server mittels des Befehls `/kolab/etc/rc all start` gestartet werden. Die Konsolenausgabe während des Bootstrap-Prozesses wird in Kapitel 4.4.5 noch einmal detailliert dargestellt.

Da das Passwort für den Benutzer `manager` in Klartext in der LDAP-Konfigurationsdatei `/kolab/etc/openldap/slapd.conf` eingetragen wird, empfiehlt es sich, dieses nachträglich noch zu verschlüsseln und in die Konfigurationsdatei einzutragen:

```
[root@fc1 fedora1]# /kolab/sbin/slappasswd
New password:
Re-enter new password:
{SSHA}j1xszJv2fIdq8oJXCcCHICzNyj8qyAU3

[root@fc1 fedora1]# vi /kolab/etc/openldap/slapd.conf
#rootpw          "admin"
rootpw           {SSHA}j1xszJv2fIdq8oJXCcCHICzNyj8qyAU3
```

Nach einem Neustart des Kolab-Servers ist das Webinterface der beschriebenen Referenzplattform unter `https://hostname.domainname/admin` verfügbar.

4.2 Probleme bei der Installation

Die bei der Installation des Kolab-Server aufgetretenen Probleme und Maßnahmen zur präventiven Vermeidung dieser sollen in diesem Abschnitt näher beschrieben werden.

4.2.1 Export von Umgebungsvariablen unter Red Hat Linux

Um präventiv Installationsprobleme und Fehler bei der Installation der Kolab Sourcepakete auf Red Hat basierten Betriebssystemen zu vermeiden, wird in dem Kolab Quick Installation Manual¹⁰⁶ ausdrücklich darauf hingewiesen, dass vor Beginn der Installation die folgenden Umgebungsvariablen gesetzt werden müssen:

```
[root@fc1 root]# LC_ALL=C
[root@fc1 root]# LC_MESSAGES=C
[root@fc1 root]# LANG=C
[root@fc1 root]# SUPPORTED=C
[root@fc1 root]# export LC_ALL LC_MESSAGES LANG SUPPORTED
```

¹⁰⁶Vgl. Konold: Quick Install Manual Kolab 1.0.4.

4.2.2 Installation mittels ZfOS-Binaries

Werden für die Installation von Kolab die Installationspakete des ZfOS-Archivs verwendet, muss unter Red Hat basierten Systemen das Werkzeug *uudecode* zur Verfügung stehen. Bei den auf Red Hat basierenden Distributionen ist dieses in dem Paket *sharutils* enthalten.

4.2.3 Auftretende Fehler beim Bootstrap-Prozess

Während des Bootstrap Prozesses bzw. beim anschließenden Starten des Kolab-Servers treten häufig Fehlermeldungen der folgenden Art auf:

```
failed to write entry: modifications require authentication at
/kolab/etc/kolab/kolab_bootstrap line 226, <DATA> line 283.
```

[...]

```
Can't call method "attributes" on an undefined value at /kolab/etc/kolab/kolab line
353, <DATA> line 283.
```

[...]

Diese Problematik wurde bereits mehrfach in der Kolab-Users Diskussionsliste¹⁰⁷ erörtert. Der Fehler wird durch eine manuelle Änderung in der Datei `/kolab/etc/kolab/slapd.conf.template` behoben. In diesem Fall muss die Funktion `bind_pw_hash` durch `bind_pw` ersetzt werden.¹⁰⁸

4.2.4 Portbelegung

Um Fehler bei der Installation des Kolab-Servers zu vermeiden empfiehlt es sich, nicht benötigte Dienste zu deaktivieren (siehe Kapitel 4.1.3.3). Beispielsweise äußert sich ein Fehler bei einem bereits über das Betriebssystem gestarteten SMTP-Daemon in der folgenden Art in dem Ereignisprotokoll von Postfix:

```
Jun 13 14:29:11 fcl <info> postfix/postfix-script[13316]: starting the Postfix
mail system
Jun 13 14:29:11 fcl <critical> postfix/master[13317]: fatal: bind INADDR_ANY
port 25: Address already in use
```

¹⁰⁷vgl. Kolab.org: The Kolab-users Archives; 2004 in: <http://kolab.org/pipermail/kolab-users/> – Zugriff am 25.7.2004.

¹⁰⁸vgl. Albest: Error in slapd.conf.template; in: <http://eforum.de/viewtopic.php?t=114> – Zugriff am 21.6.2004.

Eine Übersicht über die gestarteten Dienste und belegten Ports bietet beispielsweise unter Linux der Befehl `netstat -atlu`:¹⁰⁹

```
[root@fcl root]# netstat -atlu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 *:32768                 :::*                    LISTEN
tcp      0      0 *:imaps                  :::*                    LISTEN
tcp      0      0 *:pop3s                  :::*                    LISTEN
tcp      0      0 *:ldap                    :::*                    LISTEN
tcp      0      0 localhost:9999           :::*                    LISTEN
tcp      0      0 *:imap                    :::*                    LISTEN
tcp      0      0 *:sunrpc                  :::*                    LISTEN
tcp      0      0 *:http                    :::*                    LISTEN
tcp      0      0 *:smtps                   :::*                    LISTEN
tcp      0      0 *:ftp                      :::*                    LISTEN
tcp      0      0 *:ssh                      :::*                    LISTEN
tcp      0      0 *:smtp                     :::*                    LISTEN
tcp      0      0 *:https                    :::*                    LISTEN
tcp      0      0 localhost:ldap           localhost:32773        ESTABLISHED
tcp      0      0 localhost:32773          localhost:ldap         ESTABLISHED
tcp      0      0 localhost:32777          localhost:ldap         ESTABLISHED
tcp      0      0 localhost:ldap           localhost:32777        ESTABLISHED
udp      0      0 *:32768                 :::*                    LISTEN
udp      0      0 *:32769                 :::*                    LISTEN
udp      0      0 *:32770                 :::*                    LISTEN
udp      0      0 *:948                     :::*                    LISTEN
udp      0      0 225.0.0.7:ha-cluster    :::*                    LISTEN
udp      0      0 *:ha-cluster              :::*                    LISTEN
[...]
```

4.2.5 LDAP Replikationsdienst manuell stoppen

Unter bestimmten Voraussetzungen kann es dazu kommen, dass nach dem Stoppen des Kolab-Servers der LDAP Replication-Daemon `slurpd` weiterhin aktiv ist. Dies führt bei einem anschließenden Start des Kolab-Servers zu Problemen. Dies kann durch manuelles Stoppen des `slurpd`-Prozesses verhindert werden.

4.2.6 E-Mail-Konten werden nicht angelegt

Ein häufiger Fehler bei Kolab-Installationen ist, dass bei der Einrichtung von Benutzern über das Webinterface keine E-Mail-Konten in Cyrus-IMAPd angelegt werden. Da die IMAP-Funktionalität zu den grundlegenden Eigenschaften des Kolab-Servers gehört, ist diese Problematik inakzeptabel. Nach Installation und Starten des Kolab-Servers wird im Systemprotokoll die folgende Meldung ausgegeben:

¹⁰⁹vgl. Konold: Quick Install Manual Kolab 1.0.4.

```
Jun 21 19:57:14 fcl kolabd[2645]: Kolab is starting up
Jun 21 19:57:16 fcl perl: No worthy mechs found
Jun 21 19:57:19 fcl kolabd[2645]: Y Error: Unable to authenticate with Cyrus
admin interface, Error = ``
```

Auch der Zugriff auf Cyrus-IMAPd mit Hilfe des Administrationswerkzeugs `cyradm` ist nicht möglich:

```
[root@fcl root]# /kolab/bin/cyradm -u manager localhost
IMAP Password:
Login failed: authentication failure at
/kolab/lib/perl/vendor_perl/5.8.3/i686-linux/Cyrus/IMAP/Admin.pm line 118
cyradm: cannot authenticate to server with as manager
```

Wird eine andere Syntax zur Anmeldung genutzt, gelingt zwar ein Login, jedoch ist es nicht möglich, manuell einen Postkorb zu erstellen:

```
[root@fcl root]# /kolab/bin/cyradm -u manager@matrix.com localhost
IMAP Password:
fcl.matrix.com> listmailbox
fcl.matrix.com> createmailbox neo
createmailbox: Permission denied
```

Im Rahmen dieser Arbeit gelang es mit keiner aktuellen Red Hat-Version wie Red Hat Linux 9, Fedora Linux Core 1 sowie Red Hat Enterprise Linux 3 nach der Installationsdokumentation einen funktionsfähigen Kolab-Server mittels Source- oder Binary-Paketen in den offiziellen, stabilen Versionen aufzubauen. Diese Problematik trat auch unter anderen Betriebssystemen wie FreeBSD 4.9¹¹⁰, Mandrake Linux 10¹¹¹ und SuSE Linux 8.1¹¹² auf. Auch wurde von diesem Fehler mehrfach und ausführlich auf der Kolab-Users Diskussionsliste berichtet.¹¹³ Aufgrund der im Rahmen dieser Arbeit durchgeführten Untersuchungen konnte dieses Problem durch die Modifikation der Datei `/etc/hosts` behoben werden.¹¹⁴ Red Hat-basierte Systeme haben standardmässig nach der Installation folgende Einträge in der Datei `/etc/hosts`:

¹¹⁰vgl. Prochnow, S.: Problem mit Kolab + FreeBSD 4.9 + no worthy mechs found; in: <http://www.kolab.org/pipermail/kolab-users/2004-June/000515.html> – Zugriff am 21.6.2004.

¹¹¹vgl. Croombs, D.: Kolab on mandrake 10.0; in: <http://www.kolab.org/pipermail/kolab-users/2004-June/000534.html> – Zugriff am 21.6.2004.

¹¹²vgl. Walzebuck, F.: [Kroupware] kolab on SuSE 8.1, Problems (Bugreport); in: <https://mail.kde.org/pipermail/kroupware/2003-March/001282.html> – Zugriff am 21.6.2004.

¹¹³vgl. Stoermer, M.: perl, sasl or cyrus problem? in: <http://www.kolab.org/pipermail/kolab-users/2004-June/000525.html> – Zugriff am 21.6.2004.

¹¹⁴vgl. Stoermer, M.: SOLVED: Y Error: Unable to authenticate with Cyrus admin interface, Error = “; in: <http://kolab.org/pipermail/kolab-users/2004-June/000546.html> – Zugriff am 27.6.2004.

```
[root@fcl root]# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1          localhost.localdomain localhost
192.168.0.4       fcl.matrix.com fcl
```

Um Kolab ohne Fehler starten zu können muss die Datei in Zeile 3 wie folgt angepasst werden:

```
[root@fcl root]# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1          localhost
192.168.0.4       fcl.matrix.com fcl
```

Durch die Modifikation hervorgerufene Beeinträchtigungen anderer Programme sind bisher nicht bekannt.

4.2.7 Überprüfung der Ereignisprotokolle

Nach erfolgter Installation von Kolab ist es sinnvoll, die Ereignisprotokolle der einzelnen Kolab-Komponenten auf Fehler- oder Warnmeldungen hin zu überprüfen. Die verschiedenen Protokoll-Dateien sind in der Standardkonfiguration unter `/kolab/var/<Dienst>/log/<Logfile>` bzw. `/kolab/var/<Dienst>/<Logfile>` zu finden. Wie aus dem vorherigen Beispiel ersichtlich ist, erscheinen Fehler- und Warnmeldungen auch im Systemprotokoll des Servers. In diesem Fall ist das Systemlog des jeweiligen Betriebssystems zu prüfen.

4.3 Skalierbarkeit und Hochverfügbarkeit

Eine wichtige Anforderung an eine sichere und zuverlässige Open Source Groupware-Lösung ist die Skalierbarkeit, also das Verhalten des Servers bei ansteigender Kapazitätsauslastung sowie Ausfallsicherheit des Systems. Durch den modularen Aufbau des Kolab-Servers aus flexiblen und zuverlässigen Komponenten sowie bestimmten Modifikationen wird eine hohe Skalierbarkeit des Servers erreicht. Hochverfügbarkeit wird durch die Verwendung bestimmter Hard- und Software erreicht. Die von dem Kolab-Projekt empfohlenen Schritte in diesem Zusammenhang sind beispielsweise:¹¹⁵

¹¹⁵vgl. Kroupware Project: Kroupware Project Frequently-Asked Questions; 2004 in: <http://www.kroupware.org/faq/faq.html#Kolab%20Server0> – Zugriff am 26.5.2004.

- Verteilung der Kolab-Komponenten über mehrere Server, z.B. durch Trennung des MTA und des IMAPd.
- Realisierung einer Cluster-Funktionalität zur Erreichung von Hochleistung und Hochverfügbarkeit, z.B. durch Verwendung mehrerer MTA.
- Verlagerung der Prozessorlast auf die Seite des Clients.
- Optimierung der Schreib-/Lesegeschwindigkeit durch Vermeidung unnötiger Kopiervorgänge sowie Nutzung leistungsfähiger Hardware
- Nutzung verteilter Clustersysteme zur Erreichung von Hochverfügbarkeit

Zum Zeitpunkt der Erstellung dieser Arbeit sind keine Dokumentationen zu dem Thema Skalierbarkeit bzw. Hochverfügbarkeit für den Kolab-Server verfügbar. Auf der Homepage des Kolab-Projekts wird ausdrücklich dazu aufgerufen, das Projekt unter anderem mit Dokumentationen über Hochverfügbarkeit zu unterstützen.¹¹⁶ Von der Firma Erfrakon wurde auf der CEBIT 2003 ein Hochverfügbarkeitscluster¹¹⁷ präsentiert; Informationen über die technische Realisierung sind allerdings nicht verfügbar. Zusammenfassend kann auf keine Erfahrungswerte über Hochverfügbarkeit bzw. Skalierbarkeit zurückgegriffen werden, da hier entsprechende Dokumentationen fehlen.

Für die Realisierung eines hochverfügbaren Rechnernetzes sind mehrere Szenarien denkbar, die verschiedene Vor- und Nachteile im Bezug auf die Bereitstellung eines Kolab-Servers haben. Eine verbreitete und kostengünstige Alternative stellt ein sogenannter *Active/Passive Cluster*¹¹⁸ in Verbindung mit einem gemeinsam genutzten Datenspeicher (*Shared Storage*¹¹⁹) dar. Ein Active/Passive Cluster besteht typischerweise aus zwei Clusterknoten, dabei übernimmt einer der beiden Knoten die Bereitstellung der Applikation, während der andere Knoten im Ruhezustand verweilt. Der gemeinsam genutzte Datenspeicher hält bei der Betrachtung des Kolab-Szenarios die Datenbasis der verschiedenen Kolab-Dienste vor. Beide Knoten verfügen zu administrativen Zwecken über eine eigene IP-Adresse, der aktive Knoten ist zusätzlich noch über eine Cluster IP-Adresse erreichbar, mittels derer die Clients den aktiven Clusterknoten und damit die Dienste ansprechen. Die Clusterknoten verfügen üblicherweise

¹¹⁶vgl. Kolab Project: The Kolab Project::HOWTOs; 2004 in: <http://kolab.org/howtos.html> – Zugriff am 14.6.2004.

¹¹⁷vgl. KDE e.V.: KDE@CeBIT 2003; 2003 in: <http://kde.feratech.com/announcements/cebit2003.php> – Zugriff am 14.6.2004.

¹¹⁸vgl. Soltau, M.: Unix/Linux Hochverfügbarkeit; Bonn 2000, S. 25ff..

¹¹⁹vgl. Soltau: Unix/Linux Hochverfügbarkeit, S. 25 ff..

über mehrere direkte Schnittstellen (*Private Cluster Interconnect* oder *Heartbeat*¹²⁰), um Informationen über den Status des Rechnerverbands austauschen zu können sowie den exklusiven Zugriff eines Knotens auf den Datenspeicher reglementieren zu können. Fällt nun der aktive Knoten hard- oder softwareseitig aus, bleiben Statusinformationen des aktiven Knoten über den Interconnect aus. Der passive Knoten startet daraufhin die Applikation oder Dienste und übernimmt die Cluster IP-Adresse. Somit übernimmt der passive Knoten die Rolle des aktiven Knotens, bekommt exklusiven Zugriff auf den gemeinsamen Datenspeicher und stellt aus Sicht der Clients die Verfügbarkeit des Servers für den Anwender transparent wieder her.¹²¹ Optional kann die Sicherung der Daten über ein dediziertes LAN erfolgen, um so die Netzwerkauslastung des produktiven LAN möglichst gering zu halten. Abbildung 4.2 soll ein mögliches Szenario aufzeigen.

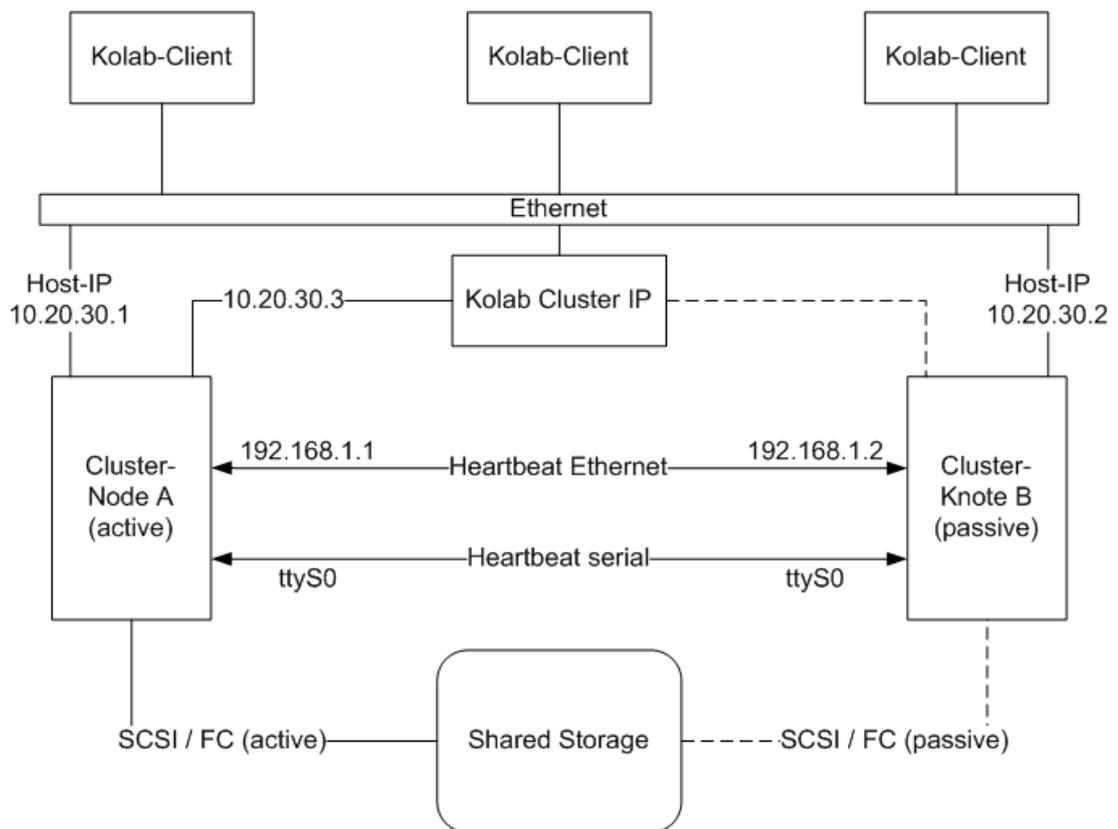


Abbildung 4.2: Active/Passive Cluster

¹²⁰Vgl. Soltau: Unix/Linux Hochverfügbarkeit, S. 25 ff..

¹²¹Vgl. Soltau: Unix/Linux Hochverfügbarkeit, S. 25 ff..

4.4 Installation eines Kolab High Availability Clusters

In diesem Abschnitt wird die Installation eines hochverfügbaren Kolab Clusters basierend auf Red Hat Enterprise Linux AS 3 nach dem oben beschriebenen Konzept des Active/Passive-Cluster beschrieben. Als Hardware dienen zwei Fujitsu Siemens RX300 Server in Verbindung mit einem Fujitsu Siemens S80 Storage Subsystem. Die Installation des Kolab-Servers wurde mit den zum Zeitpunkt der Anfertigung dieser Arbeit aktuellen und für Red Hat Enterprise Linux 3 angepassten Installationspaketen des ZfOS-Archivs durchgeführt. Da Red Hat Enterprise Linux 3 im Standardumfang nicht mit einer eigenen Clustersoftware¹²² ausgeliefert wird, wurden die für diese Betriebssystemversion angepassten Installationspakete der Clustersoftware *heartbeat* verwendet.

4.4.1 Hardwareplattform

Die verwendete Hardware verfügt über die in Tabelle 4.1 aufgeführten Spezifikationen:

2 x Fujitsu Siemens Primergy RX300	
CPU	2 x Intel Xeon 2,8 GHz
I/O-Schnittstellen	2 x seriell, 2 x Broadcom Gigabit Ethernet, 1 x Intel Gigabit Ethernet, 1 x Dual Fibre Channel SCSI (2Gbit)
Festplatten	2 x 36 GB Seagate Cheetah 10k, RAID1
Arbeitsspeicher	4096 MB
Fujitsu Siemens FibreCAT S80	
I/O-Schnittstellen	2 x Dual Fibre Channel SCSI (2Gbit)
Festplatten	8 x 73 GB Seagate Cheetah 10k, RAID5
Nettokapazität	437 GB

Tabelle 4.1: Hardwarespezifikation des Kolab HA-Clusters

Die Anbindung des Storage Subsystems ist redundant ausgelegt, jeweils ein Port der Dual Fibre Channel SCSI Karten ist mit einem der zwei Controller des Subsystems verbunden. Fällt einer der Controller aus, ist weiterhin die Anbindung vom Server zum Subsystem sichergestellt. Die Clusterkommunikation wurde sowohl über eine serielle Schnittstelle (`ttys0`) als auch über ein Crosslink Ethernet-Kabel (`eth1`) realisiert.

¹²²vgl. Red Hat, Inc.: Red Hat Cluster Suite; 2004 in: <http://www.redhat.com/software/rha/cluster/> – Zugriff am 24.8.2004.

Als Schnittstellen in das produktive LAN dienen jeweils das reale Interface `eth0` und auf dem aktiven Clusterknoten ein virtuelles Interface `eth0:0`, an das die Cluster-IP-Adresse gebunden ist. Die Server verfügen zusätzlich über eine Schnittstelle `eth2`, die eine Gigabit Ethernet Verbindung in ein Backup-LAN ermöglicht, welches ausschliesslich zur Sicherung der Daten genutzt wird. Die in der Testumgebung realisierte Anbindung an ein separates Backup-LAN ist optional, bietet aber im Hinblick auf Hochverfügbarkeit den Vorteil, dass die Auslastung des produktiven LAN nicht durch Backupvorgänge beeinträchtigt wird. Die Stromversorgung wird neben zwei redundanten Netzteilen pro Server auch durch eine unterbrechungsfreie Stromversorgung (USV) sichergestellt.

4.4.2 Installation des Betriebssystems

Als Betriebssystem wurde Red Hat Enterprise Linux AS 3 gewählt, da dieses Betriebssystem für die verwendete Hardware zertifiziert ist, also durch den Hersteller der Hardware unterstützt und mit systemspezifischen Treibern versorgt wird. Tabelle 4.2 zeigt die in dieser Beschreibung verwendeten Hostnamen, Domainnamen, IP-Adressen und Clusterrollen.

Systemparameter des Clusters			
Host A		Host B	
Hostname:	logos	Hostname:	osiris
DNS-Domain:	matrix.com	DNS-Domain:	matrix.com
IP/Subnet:	10.20.30.1/24	IP/Subnet:	10.20.30.2/24
Knoten A		Knoten B	
Nodename:	icarus-1	Nodename:	icarus-2
DNS-Domain:	–	DNS-Domain:	–
IP/Subnet:	192.168.1.1/24	IP/Subnet:	192.168.1.2/24
Rolle:	aktiv	Rolle:	passiv
Cluster-Alias			
Clustername:		icarus	
DNS-Domain:		matrix.com	
IP/Subnet:		10.20.30.3/24	

Tabelle 4.2: Clusterknoten

Nach der Installation des Betriebssystems wurden die folgenden Dienste deaktiviert, zum Teil weil sie nicht benötigt werden, zum Teil weil sie den Betrieb des Kolab Servers beeinträchtigen, wie z.B. `sendmail`:

```
[root@logos root]# chkconfig --level 2345 isdn off
[root@logos root]# chkconfig --level 2345 iptables off
[root@logos root]# chkconfig --level 2345 ip6tables off
[root@logos root]# chkconfig --level 2345 pcmcia off
[root@logos root]# chkconfig --level 2345 sendmail off
[root@logos root]# chkconfig --level 2345 rhnsd off
[root@logos root]# chkconfig --level 2345 cups off
[root@logos root]# chkconfig --level 2345 hpoj off
```

Die Konfiguration der LAN-Schnittstellen erfolgt unter Red Hat Linux durch die Anpassung der Dateien `/etc/sysconfig/network-scripts/ifcfg-eth<n>` sowie `/etc/sysconfig/network`:

```
[root@logos root]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=logos.matrix.com
GATEWAY=10.20.30.250

[root@logos root]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
# Intel Corp. | 82544EI Gigabit Ethernet Controller (Copper)
DEVICE=eth0
BOOTPROTO=static
BROADCAST=10.20.30.255
IPADDR=10.20.30.1
NETMASK=255.255.255.0
NETWORK=10.20.30.0
ONBOOT=yes
TYPE=Ethernet

[root@logos root]# cat /etc/sysconfig/network-scripts/ifcfg-eth1
# Broadcom Corporation | NetXtreme BCM5704 Gigabit Ethernet
DEVICE=eth1
BOOTPROTO=static
BROADCAST=192.168.1.255
IPADDR=192.168.1.1
NETMASK=255.255.255.0
NETWORK=192.168.1.0
ONBOOT=yes
TYPE=Ethernet
```

Im folgenden Schritt wird die Datei `/etc/hosts` angepasst, zum einen wird wie bereits beschrieben der Eintrag `localhost.localdomain` gelöscht, um die Funktionsfähigkeit von Kolab herzustellen, zum anderen werden die Daten der Hosts und der Clusterknoten aus oben genannter Tabelle eingetragen:

```
[root@logos root]# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1        localhost
10.20.30.1       logos.matrix.com      logos    # Host A
```

```
10.10.30.2    osiris.matrix.com    osiris # Host B
192.168.1.1    icarus-1              # Knoten A
192.168.1.2    icarus-2              # Knoten B
10.10.30.3    icarus.matrix.com    icarus # Cluster-Alias
```

Um die korrekte Funktionalität der Cluster Interconnect-Schnittstellen zu überprüfen, sollte auf beiden Knoten ein Funktionstest durchgeführt werden:

```
[root@logos root]# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=0 ttl=64 time=0.260 ms
```

```
[...]
```

Um die serielle Schnittstelle zu überprüfen, muss zunächst ein Knoten mittels des folgenden Befehls als Empfänger einer Nachricht definiert werden:

```
[root@osiris root]# cat < /dev/ttyS0
```

Von dem anderen Knoten kann daraufhin eine Nachricht über die serielle Schnittstelle versendet werden:

```
[root@logos root]# echo test > /dev/ttyS0
```

Auf dem als Empfänger definierten Knoten sollte nun die Meldung ‚test‘ auf der Konsole erscheinen. Diese Prüfung sollte mit vertauschten Sender/Empfänger-Rollen wiederholt werden. Die korrekte Grundkonfiguration der verschiedenen Schnittstellen ist notwendig für die spätere Konfiguration und Funktionalität der Clustersoftware, die in dem folgenden Abschnitt beschrieben wird.

4.4.3 Installation der Clustersoftware

Die für den Clusteraufbau gewählte Software heartbeat in der Version 1.0.4-2 basiert auf den Entwicklungen des Open Source Projekts Linux-HA.¹²³ In diesem Fall wurden die speziell für Red Hat Enterprise Linux AS 3 angepassten RPM-Pakete des Ultra

¹²³vgl. High-Availability Linux Project: Linux-HA Project Web Site; 2004 in: <http://linux-ha.org/> – Zugriff am 29.6.2004.

Monkey Projekts¹²⁴ für die Installation verwendet, welche im Downloadbereich¹²⁵ der Ultra Monkey Webseite verfügbar sind. Anhand der Installationsdokumentation¹²⁶ für Red Hat Enterprise Linux wurden die erforderlichen Pakete installiert. Zu beachten ist hierbei, dass die für die Installation von heartbeat erforderlichen Abhängigkeiten sowohl durch RPM-Pakete der Red Hat Linux Distribution als auch durch Ultra Monkey zu erfüllen sind. Die folgende Auflistung der installierten Pakete soll das Vorgehen verdeutlichen. Zunächst werden zwei Pakete der Red Hat Distribution installiert:

```
[root@logos Red Hat-RPMS]# rpm -ihv perl-Digest-SHA1-2.01-15.1.i386.rpm
perl-Digest-HMAC-1.01-11.1.noarch.rpm
warning: perl-Digest-SHA1-2.01-15.1.i386.rpm: V3 DSA signature: NOKEY, key ID db42a6
Preparing...                               ##### [100%]
 1:perl-Digest-SHA1                         ##### [ 50%]
 2:perl-Digest-HMAC                         ##### [100%]
```

Im Anschluss werden die heruntergeladenen RPM-Pakete von Ultra Monkey installiert:

```
[root@logos Ultramonkey-RPMS]# rpm -ihv *.rpm
Preparing...                               ##### [100%]
 1:perl-Net-SSLeay                           ##### [ 7%]
 2:heartbeat-pils                            ##### [ 14%]
 3:heartbeat-stonith                         ##### [ 21%]
 4:perl-IO-Socket-SSL                       ##### [ 29%]
 5:perl-XML-NamespaceSupport                ##### [ 36%]
 6:perl-XML-SAX                             ##### [ 43%]
 7:perl-Mail-IMAPClient                     ##### [ 50%]
 8:perl-Convert-ASN1                        ##### [ 57%]
 9:perl-Authen-SASL                         ##### [ 64%]
10:perl-ldap                                ##### [ 71%]
11:ipvsadm                                  ##### [ 79%]
12:heartbeat                                ##### [ 86%]
13:heartbeat-ldirectord                     ##### [ 93%]
14:libnet                                    ##### [100%]
```

Auf ein in der Installationsdokumentation empfohlenes Kernel-Upgrade zur Nutzung erweiterter Funktionalitäten im Hinblick auf netzwerkseitige Lastverteilung wurde bewusst verzichtet. Zum einen werden die erweiterten Funktionalitäten in diesem Fall nicht benötigt, zum anderen sind die Auswirkungen einer veränderten Kernelversion im Hinblick auf die Funktionsfähigkeit spezieller Treiber zur Anbindung des Subsystems unbekannt.

¹²⁴vgl. Ultra Monkey Project: ultra Monkey; 2004 in: <http://www.ultramonkey.org/> – Zugriff am 29.6.2004.

¹²⁵vgl. Ultra Monkey Project: ultra Monkey; 2004 in: <http://www.ultramonkey.org/download/2.0.1/rh.el.3.0/RPMS/> – Zugriff am 29.6.2004.

¹²⁶vgl. Ultra Monkey Project: Installation Notes: Ultra Monkey on Red Hat Enterprise Linux 3.0; 2004 in: <http://www.ultramonkey.org/2.0.1/installation-rh.el.3.0.ws.html> – Zugriff am 29.6.2004.

4.4.4 Konfiguration von heartbeat

Anhand der Konfigurationsdokumentation¹²⁷ des heartbeat-Dienstes wurden die Dateien `/etc/ha.d/ha.cf`, `/etc/ha.d/haresources` und `/etc/ha.d/authkeys` angelegt und mit den erforderlichen Parametern angepasst. Die folgende Auflistung soll die Konfigurationsparameter aufzeigen:

```
[root@logos ha.d]# cat ha.cf
debugfile /var/log/ha-debug      # Debug-Log
logfile /var/log/ha-log         # Log
keepalive 2                     # Pause zwischen Heartbeats = 2 Sek.
deadtime 10                     # Timeout bei Nicht-Rueckantwort = 10 Sek.
warntime 10                     # Timeout fuer Warnung = 10 Sek.
initdead 10                    # Timeout fuer Netzwerk nach Reboot = 10 Sek.
nice_failback on                # Uebernahme der Ressourcen bei Ausfall = ja
serial /dev/ttyS0               # Geraet fuer serielle Heartbeat-Verbindung
udpport 694                    # Kommunikationsport UDP = 694
bcast eth1                     # Heartbeat-Interface = eth1
mcast eth1 225.0.0.7 694 1 1   # Multicast Heartbeat Medium = eth1
node logos.matrix.com          # Node A = `uname -n`
node osiris.matrix.com         # Node B = `uname -n`
```

Die vom Cluster auszuführenden Schritte werden in der heartbeat-Konfigurationsdatei `/etc/ha.d/haresources` durch eine Zeile definiert. Die einzelnen Argumente und deren Optionen werden nacheinander beim Start oder Stop des heartbeat-Dienstes ausgeführt.

```
[root@logos ha.d]# cat haresources
# Cluster-Alias
# Cluster-IP/Subnetz/Interface
# Art der Ressource::Geraetenname::Mountpoint::Dateisystem
# Dienstname
icarus.matrix.com 10.20.30.3/24/eth0 Filesystem::/dev/sdb1::/kolab::ext3 kolab
```

Beim Start des Dienstes auf einem Knoten wird die Zeile von links nach rechts ausgewertet; dabei wird zunächst der Clustername und die IP-Adresse in Verbindung mit der zugehörigen Subnetzmaske und Interface übernommen. Als nächster Schritt wird mit dem Argument `Filesystem` des Typs `ext3` das Gerät `/dev/sdb1`, welches als gemeinsamer Datenspeicher dient, in den Mountpoint `/kolab` eingehangen. Als letzter Schritt beim Start des heartbeat-Dienstes wird das Skript `/etc/init.d/kolab` mit der Option `start` ausgeführt. Das Kolab Start-Skript startet nun die zuvor unter `/kolab` gemounteten Programme; der Kolab-Server ist danach für Clients

¹²⁷vgl. Ultra Monkey Project: High Availability: Single Virtual Service; 2004 in: <http://www.ultramonkey.org/2.0.1/topologies/ha-eg.html> – Zugriff am 29.6.2004.

nutzbar. Wird der heartbeat-Dienst gestoppt oder die Rollen des aktiven bzw. passiven Knoten getauscht, so werden die oben genannten Schritte in umgekehrter Reihenfolge ausgeführt.

Das in der Datei `/etc/ha.d/authkeys` hinterlegte Klartext-Passwort dient der sicheren Kommunikation zwischen den Clusterknoten. Dieses Passwort wird mit dem `sha1`-Algorithmus verschlüsselt und dient dem Kommunikationspartner als Verifizierung der Authentizität für eingehende Steuermeldungen, wie z.B. Statusmeldungen des Clusters. Die Datei ist mit Lese- und Schreibrechten für den User `root` versehen, sie darf also ausschliesslich durch den Super-User gelesen oder geschrieben werden, womit das Passwort gegen unerwünschten Zugriff durch andere User geschützt ist.

```
[root@logos ha.d]# cat authkeys
auth 2
2 sha1 PaSSWoRd
```

Die Installation und Konfiguration von heartbeat auf dem zweiten Knoten erfolgt simultan zu der geschilderten Vorgehensweise; dabei können die Konfigurationsdateien `ha.cf`, `haresources` und `authkeys` unverändert übernommen werden.

4.4.5 Installation von Kolab

Die Installation der in diesem Szenario gewählten Kolab Installationspakete des ZfOS-Archivs in der Version 20040217-2.0.0 erfolgt auf einem der beiden Knoten; als Datenspeicher für diese Installation dient dabei das Speicher-Subsystem, welches unter dem Mountpoint `/kolab` eingehängt wird. Die folgenden Abschnitte stellen Vorbereitungen für die Installation sowie den eigentlichen Installationsablauf dar.

Einhängen des Datenspeichers unter dem Mountpoint:

```
[root@logos /]# mkdir kolab
[root@logos /]# mount /dev/sdb1 /kolab
[root@logos /]# mount

[...]

/dev/sdb1 on /kolab type ext3 (rw)
```

Installation des Kolab-Servers:

```

[root@logos /]# cd /root/install/kolab/ix86-rhel3
[root@logos ix86-rhel3]# sh obmtool kolab
---- boot/build logos.matrix.com %kolab ----
bootstrap check/execution
did not find rpm executable, checking for binary sh
OpenPKG 2.0-RELEASE Binary Bootstrap Package, version 2.0.0
Built for prefix /kolab on target platform ix86-rhel3
++ hooking OpenPKG instance into system environment
++ fixating OpenPKG instance root directory "/kolab"
++ extracting OpenPKG binary distribution
++ installing OpenPKG binary distribution
++ fixating OpenPKG instance filesystem hierarchy
++ post-processing OpenPKG bootstrap installation
+-----+
| Congratulations!-
|
| You have successfully installed an OpenPKG 2.0-RELEASE instance
| under prefix /kolab on target platform ix86-rhel3.
|
| Details about this installed OpenPKG instance you can easily
| determine by running the following typical OpenPKG RPM query
| commands:
|
|     $ /kolab/bin/openpkg rpm -qa
|     $ /kolab/bin/openpkg rpm -qi openpkg
|     $ /kolab/bin/openpkg rpm -qlv openpkg
|
| The integrity of the whole OpenPKG instance you can check at any
| time by running the OpenPKG RPM verify command:
|
|     $ /kolab/bin/openpkg rpm -Va
|
| For installing software packages into this OpenPKG instance,
| just run the following two OpenPKG RPM build commands for each
| package:
|
|     $ /kolab/bin/openpkg rpm --rebuild /path/to/foo-*.src.rpm
|     $ /kolab/bin/openpkg rpm -Uvh /kolab/RPM/PKG/foo-*.rpm
|
| If you later want to remove a software package, just run:
|
|     $ /kolab/bin/openpkg rpm -e foo
|
| For removing the whole OpenPKG instance under prefix
| /kolab, just remove every package. Once you finally
| removed the package "openpkg", the whole OpenPKG instance
| will be unlinked from the system and removed, too.
|
| Thank you for flying OpenPKG...
|
|                                     Ralf S. Engelschall
|                                     The OpenPKG Project
|                                     openpkg@openpkg.org
+-----+
mv: cannot stat `openpkg-2.0.0-2.0.0.src.sh': No such file or directory

```

```

mv: cannot stat `openpkg-2.0.0-2.0.0.src.rpm': No such file or directory
install openpkg-2.0.0-2.0.0
install make-3.80-2.0.0
rebuild make-3.80-2.0.0

Preparing... #####
make #####

[...]

Preparing... #####
kolab #####

please run '/kolab/etc/kolab/kolab_bootstrap -b'
INSTALL: openpkg-2.0.0-2.0.0 make-3.80-2.0.0 binutils-2.14-2.0.0 gcc-3.3.3-2.0.0
fsl-1.4.0-2.0.0 mm-1.3.0-2.0.0 perl-5.8.3-2.0.0 perl-openpkg-5.8.3-2.0.0
perl-conv-5.8.3-2.0.0 readline-4.3.5-2.0.0 sharutils-4.2.1-2.0.0
ncurses-5.4.20040214-2.0.0 perl-term-5.8.3-2.0.0 perl-ds-5.8.3-2.0.0
perl-util-5.8.3-2.0.0 perl-mail-5.8.3-2.0.0 perl-crypto-5.8.3-2.0.0
perl-net-5.8.3-2.0.0 zlib-1.2.1-2.0.0 expat-1.95.7-2.0.0 perl-xml-5.8.3-2.0.0
perl-www-5.8.3-2.0.0 perl-time-5.8.3-2.0.0 openssl-0.9.7c-2.0.0
imap-2004rc6-2.0.0 perl-ssl-5.8.3-2.0.0 procmail-3.22-2.0.0 db-4.2.52.2-2.0.0
openldap-2.2.5-2.0.0 sasl-2.1.17-2.0.0 getopt-20030307-2.0.0 proftpd-1.2.9-2.0.0
pcre-4.5-2.0.0 gdbm-1.8.3-2.0.0 dbtool-1.6-2.0.0 postfix-2.0.18-2.0.0
perl-sys-5.8.3-2.0.0 perl-ldap-5.8.3-2.0.0 perl-db-5.8.3-2.0.0
perl-kolab-5.8.3-2.0.0 imapd-2.2.3-2.0.0 m4-1.4o-2.0.0 bison-1.35-2.0.0
flex-2.5.4a-2.0.0 libiconv-1.9.2-2.0.0 gettext-0.14.1-2.0.0 patch-2.5.9-2.0.0
sed-4.0.9-2.0.0 apache-1.3.29-2.0.0 kolab-20040217-2.0.0
MISSING: none
SURPLUS: none
SUMMARY: NODE=logos.matrix.com; DATE=2004-06-26/18:12:44; HASX11=; DONE

```

Ausführung des Kolab Bootstrap-Skripts:

```

[root@logos ix86-rhel3]# /kolab/etc/kolab/kolab_bootstrap -b

KOLAB BOOTSTRAP

Please enter Hostname [logos.matrix.com]:
proceeding with Hostname logos.matrix.com
Please enter your Maildomain [matrix.com]:
proceeding with Maildomain matrix.com
Generating default configuration:
  base_dn : dc=logos,dc=matrix,dc=com
  bind_dn : cn=manager,dc=logos,dc=matrix,dc=com
Please choose a manager password [hVADTpQqoNEzg]:admin
  bind_pw : admin
done modifying /kolab/etc/kolab/kolab.conf

IMPORTANT NOTE:
use login=manager and passwd=admin when you log into the webinterface!-

prepare LDAP database...
kill running slapd (if any)
OpenPKG: stop: openldap.

```

```

OpenPKG: stop: openldap.
temporarily start slapd
no dc=logos,dc=matrix,dc=com object found, creating one
no kolab config object in ldap, generating a reasonable default
mynetworkinterfaces: 127.0.0.0/8, 10.20.30.0/24, 192.168.1.0/24
LDAP setup finished

Create initial config files for postfix, apache, proftpd, cyrus imap, saslauthd
  running /kolab/etc/kolab/kolab -v -o -lldap://127.0.0.1:389/
NOTE: USE OF THIS SCRIPT IS DEPRECATED. Use '/kolab/sbin/kolabconf' in the future.
kolabconf - Kolab Configuration Generator

  Copyright (c) 2003 Code Fusion cc
  Copyright (c) 2003 Tassilo Erlewein, Martin Konold, Achim Frank

This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
OpenPKG: restart: openldap.
OpenPKG: stop: sasl.
/kolab/sbin/apachectl graceful: httpd not running, trying to start
Syntax error on line 25 of /kolab/etc/apache/apache.conf:
SSLCertificateFile: file '/kolab/etc/kolab/cert.pem' not exists or empty
/kolab/sbin/apachectl graceful: httpd could not be started
postfix/postfix-script: fatal: the Postfix mail system is not running
OpenPKG: restart: imapd.
OpenPKG: stop: proftpd.

kill temporary slapd

OpenPKG: stop: openldap.
generate self-signed certificate for hostname logos.matrix.com... done
New certificate has been installed under /kolab/etc/kolab/
kolab should now be ready to run
please run '/kolab/etc/rc all start'

```

Nach Beendigung der Installation müssen die durch das Installationskript erstellten Kolab Start/Stop-Skripte in den einzelnen Runleveln manuell entfernt werden, da die Steuerung der Kolab-Dienste ausschliesslich über heartbeat erfolgen soll:

```

[root@logos etc]# rm -f /etc/rc.d/rc0.d/K00kolab
[root@logos etc]# rm -f /etc/rc.d/rc1.d/K00kolab
[root@logos etc]# rm -f /etc/rc.d/rc2.d/S99kolab
[root@logos etc]# rm -f /etc/rc.d/rc3.d/S99kolab
[root@logos etc]# rm -f /etc/rc.d/rc4.d/S99kolab
[root@logos etc]# rm -f /etc/rc.d/rc5.d/S99kolab
[root@logos etc]# rm -f /etc/rc.d/rc6.d/K00kolab

```

Auf dem zweiten Knoten müssen nun noch einige Anpassungen vorgenommen werden, um die Funktionalität der Kolab-Dienste sicherzustellen. Im ersten Schritt werden die Benutzer und Gruppen, die durch die Installation auf dem ersten Knoten erstellt wurden, auf den zweiten Knoten übertragen. Dabei ist es wichtig, dass die Benutzer-

und Gruppen-IDs auf beiden Knoten identisch angelegt werden. Die notwendigen Einträge für die relevanten Benutzer und Gruppen können den Dateien `/etc/passwd` sowie `/etc/group` des ersten Knoten entnommen werden:

```
[root@osiris root]# groupadd -g 19414 kolab
[root@osiris root]# groupadd -g 19415 kolab-r
[root@osiris root]# groupadd -g 19416 kolab-n
[root@osiris root]# useradd -u 19414 -g 19414 -d /kolab \
-s /kolab/lib/openpkg/bash -c '/kolab OpenPKG (management)' kolab
[root@osiris root]# useradd -u 19415 -g 19415 -d /kolab \
-s /kolab/lib/openpkg/bash -c '/kolab OpenPKG (restricted)' kolab-r
[root@osiris root]# useradd -u 19416 -g 19416 -d /kolab \
-s /kolab/lib/openpkg/bash -c '/kolab OpenPKG (non-privileged)' kolab-n
```

Im nächsten Schritt werden weitere, für den Kolab-Server relevante Anpassungen vorgenommen; so wird die Standard-Shell der User mit den User-IDs 19414 bis 19416 in die Datei `/etc/shells` eingetragen, das Basisverzeichnis der Kolab Installation in der Datei `/etc/openpkg` angelegt, Kolab-spezifische Anpassungen an der Datei `/etc/crontab` vorgenommen sowie das Kolab Startskript auf den zweiten Knoten kopiert. Die nachfolgende Auflistung soll dies verdeutlichen:

Ergänzung der Datei `/etc/shells`:

```
[root@osiris root]# cat /etc/shells

[...]

/kolab/lib/openpkg/bash
```

Anlegen der Datei `/etc/openpkg` mit dem entsprechenden Eintrag:

```
[root@osiris root]# cat /etc/openpkg
/kolab
```

Anpassung der Datei `/etc/crontab` mit Kolab-spezifischen Einträgen:

```
[root@osiris root]# cat /etc/crontab

[...]

# <OpenPKG prefix=/kolab pkg=openpkg>
# chronological tasks of /kolab OpenPKG hierarchy
0 0 1 * * root [ -f /kolab/etc/rc ] && /kolab/etc/rc all monthly
0 0 * * 0 root [ -f /kolab/etc/rc ] && /kolab/etc/rc all weekly
0 0 * * * root [ -f /kolab/etc/rc ] && /kolab/etc/rc all daily
0 * * * * root [ -f /kolab/etc/rc ] && /kolab/etc/rc all hourly
*/15 * * * * root [ -f /kolab/etc/rc ] && /kolab/etc/rc all quarterly
# </OpenPKG>
```

Da der heartbeat-Dienst das Kolab-Startscript unter `/etc/rc.d/init.d/` benötigt, muss dieses noch auf den zweiten Knoten kopiert werden:

```
[root@osiris root]# scp logos:/etc/rc.d/init.d/kolab /etc/rc.d/init.d/
root@logos's password:
kolab                               100% 229      2.6MB/s  00:00
```

4.4.6 Test des Clusters

Nachdem alle notwendigen Vorkehrungen getroffen wurden, kann der heartbeat-Dienst und damit Kolab auf einem der beiden Knoten gestartet werden:

```
[root@logos root]# /etc/init.d/heartbeat start
Starting High-Availability services:
[ OK ]
```

Der Status der Kolab-Dienste kann mittels einer Prozessabfrage überprüft werden:

```
[root@logos root]# ps -afe |grep kolab
root      31926      1  0 15:55 ?        00:00:00 /kolab/libexec/openldap/slapd
root      31930      1  0 15:55 ?        00:00:00 /kolab/libexec/openldap/slurpd
root      32031      1  0 15:55 ?        00:00:00 /kolab/sbin/saslauthd -a ldap -n 2
root      32035 32031  0 15:55 ?        00:00:00 /kolab/sbin/saslauthd -a ldap -n 2
root      32133      1  0 15:55 ?        00:00:00 /kolab/sbin/apache
kolab-r   32231      1  0 15:55 ?        00:00:00 /kolab/bin/cyrmaster
kolab-n   32526 32133  0 15:55 ?        00:00:00 /kolab/sbin/apache
kolab-n   32527 32133  0 15:55 ?        00:00:00 /kolab/sbin/apache
kolab-n   32528 32133  0 15:55 ?        00:00:00 /kolab/sbin/apache
kolab-n   32529 32133  0 15:55 ?        00:00:00 /kolab/sbin/apache
kolab-n   32530 32133  0 15:55 ?        00:00:00 /kolab/sbin/apache
root       332      1  0 15:55 ?        00:00:00 /kolab/libexec/postfix/master
kolab     336     332  0 15:55 ?        00:00:00 pickup -l -t fifo -u
kolab     337     332  0 15:55 ?        00:00:00 qmgr -l -t fifo -u
kolab-n   433      1  0 15:55 ?        00:00:00 proftpd: (accepting connections)
root       532      1  1 15:55 ?        00:00:00 /kolab/bin/perl /kolab/sbin/kolabd
kolab-r   541 32231  0 15:55 ?        00:00:00 imapd -C /kolab/etc/imapd/imapd.conf
kolab-r   546 32231  0 15:55 ?        00:00:00 imapd -C /kolab/etc/imapd/imapd.conf
root       547     532  0 15:55 ?        00:00:00 /kolab/bin/perl /kolab/sbin/kolabd
root       548     532  0 15:55 ?        00:00:00 /kolab/bin/perl /kolab/sbin/kolabd
```

überprüfung der eingehängten Ressource mit Hilfe des Befehls `mount`:

```
[root@logos root]# mount

[...]

/dev/sdbl on /kolab type ext3 (rw)
```

überprüfung auf die aktivierte Cluster IP-Adresse:

```
[root@logos root]# ifconfig -a

[...]

eth0:0    Link encap:Ethernet  HWaddr [...]
          inet addr:10.20.30.3  Bcast:10.20.30.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Interrupt:18 Memory:f6410000-f6420000

[...]
```

Zusätzlich ist eine Überprüfung der belegten Ports sinnvoll; die Vorgehensweise wurde bereits in Kapitel 4.2.4 erläutert. Eine zusätzliche Informationsquelle zur Überprüfung der Clusterfunktionalität bietet das heartbeat-Ereignisprotokoll `/var/log/ha-log`:

```
[...] info: *****
[...] info: Configuration validated. Starting heartbeat 1.0.4
[...] info: nice_failback is in effect.
[...] info: heartbeat: version 1.0.4
[...] info: Heartbeat generation: 13
[...] info: Starting serial heartbeat on tty /dev/ttyS0 (19200 baud)
[...] info: UDP Broadcast heartbeat started on port 694 (694) interface eth1
[...] info: UDP multicast heartbeat started for group 225.0.0.7 port 694 interface
eth1 (ttl=1 loop=1)
[...]
[...] info: Local status now set to: 'up'
[...] info: pid 31491 locked in memory.
[...] info: pid 31483 locked in memory.
[...] info: Link logos.matrix.com:eth1 up.
[...] info: Link logos.matrix.com:eth1 225.0.0.7 694 1 1 up.
[...] WARN: node osiris.matrix.com: is dead
[...] WARN: No STONITH device configured.
[...] WARN: Shared resources (storage!- ) are not protected!-
[...] info: Resources being acquired from osiris.matrix.com.
[...] info: Local status now set to: 'active'
[...] Running /etc/ha.d/rc.d/status status
[...] info: /usr/lib/heartbeat/mach_down: nice_failback: acquiring foreign
resources
[...] info: mach_down takeover complete.
[...] info: mach_down takeover complete for node osiris.matrix.com.
[...] info: Resource acquisition completed.
[...] info: Running /etc/ha.d/rc.d/ip-request-resp ip-request-resp
[...] received ip-request-resp 10.20.30.3/24/eth0 OK yes
[...] info: Acquiring resource group: logos.matrix.com 10.20.30.3/24/eth0
Filesystem: /dev/sdb1::/kolab::ext3 kolab
[...] info: Running /etc/ha.d/resource.d/IPaddr 10.20.30.3/24/eth0 start
[...] info: /sbin/ifconfig eth0:0 10.20.30.3 netmask 255.255.255.0 broadcast
```

```

10.20.30.255
[...] info: Sending Gratuitous Arp for 10.20.30.3 on eth0:0 [eth0]
[...] /usr/lib/heartbeat/send_arp eth0 10.20.30.3 0030054625AD 10.20.30.3
ffffffffffff
[...] info: Running /etc/ha.d/resource.d/Filesystem /dev/sdb1 /kolab ext3 start
[...] info: Running /etc/init.d/kolab start
[...] /usr/lib/heartbeat/send_arp eth0 10.20.30.3 0030054625AD 10.20.30.3
ffffffffffff
[...] info: Local Resource acquisition completed. (none)
[...] info: local resource transition completed.
[...] WARN: TTY write timeout on [/dev/ttyS0] (no connection or bad cable?
[see documentation])

```

Nun kann auf dem zweiten Clusterknoten ebenfalls der heartbeat-Dienst gestartet werden:

```

[root@osiris root]# /etc/init.d/heartbeat start
Starting High-Availability services:
[ OK ]

```

Im heartbeat-Ereignisprotokoll des zweiten Knoten ist ersichtlich, dass der Cluster nun über die verschiedenen Interconnect-Schnittstellen kommuniziert und der Cluster einen aktiven Zustand erreicht:

```

[root@osiris root]# cat /var/log/ha-log

[...]

[...] info: Starting serial heartbeat on tty /dev/ttyS0 (19200 baud)
[...] info: UDP Broadcast heartbeat started on port 694 (694) interface eth1
[...] info: UDP multicast heartbeat started for group 225.0.0.7 port 694 interface
eth1 (ttl=1 loop=1)
[...] info: Local status now set to: 'up'
[...] info: Link logos.matrix.com:eth1 up.
[...] info: Status update for node logos.matrix.com: status active
[...] info: Link logos.matrix.com:eth1 225.0.0.7 694 1 1 up.
[...] WARN: process_clustermmsg: node [logos] failed authentication
[...] info: Local status now set to: 'active'
[...] info: Link osiris.matrix.com:eth1 up.
[...] info: Link osiris.matrix.com:eth1 225.0.0.7 694 1 1 up.
[...] info: Running /etc/ha.d/rc.d/status status
[...] info: remote resource transition completed.
[...] info: remote resource transition completed.
[...] info: Local Resource acquisition completed. (none)
[...] info: Link logos.matrix.com:/dev/ttyS0 up.

```

Die in dem Protokoll angezeigte Warnung

```
WARN: process_clustermsg: node [logos] failed authentication
```

ist nach Angaben der Linux-HA FAQ¹²⁸ zu ignorieren; hierbei handelt es sich um ein korruptes Datenpaket, das üblicherweise beim Start von heartbeat entsteht und die Warnmeldung auslöst.

Nachdem der Cluster erfolgreich initialisiert wurde, kann nun mit einem Failover-Test die Funktionalität des Clusters bei Ausfall eines Knotens überprüft werden. Dazu wird auf dem aktiven Knoten der heartbeat-Dienst heruntergefahren und das Ereignisprotokoll auf dem passiven Knoten überprüft. Um ein realistisches Ausfallszenario nachzustellen, kann der aktive Clusterknoten von der Stromversorgung getrennt werden um so die Funktionalität des Clusters zu prüfen. Nach dieser Prozedur können die zu Beginn dieses Kapitels genannten Methoden zur Überprüfung der korrekten Übernahme der Cluster-Ressourcen auf den zweiten, nun aktiven Knoten angewandt werden.

4.5 Backup und Restore

Die Sicherung des Datenbestands ist ein wichtiger Aspekt des Betriebs und im Hinblick auf die Sicherung von Datenbanken nicht trivial. Dieser Abschnitt erläutert die Datensicherung mit Hilfe von Systemwerkzeugen und gibt einen Überblick über die zu sichernden Dateien und zur Verfügung stehenden Mechanismen.

4.5.1 Sicherung der LDAP-Datenbank

Die vielfältigen Möglichkeiten zur Sicherung einer LDAP-Datenbank sind abhängig von der zur Verfügung stehenden Infrastruktur sowie von der verwendeten Backup-Software, vor allem aber von der gewünschten Verfügbarkeit, dem LDAP Datenbank-Backend sowie dem zugehörigem Datenbanktyp. Die Sicherung einer Datenbank kann inkonsistent sein, wenn zum Zeitpunkt der Sicherung ein Schreibvorgang auf die Datenbank erfolgt. Bei dem im Kolab Konzept vorgesehenen Backend *back-ldbm* kann bei

¹²⁸vgl. High-Availability Linux Project: Frequently Asked Questions; 2004 in: <http://linuxha.trick.ca/FAQ#head-faa017f16120a4ebd51944b1db87529a7cf52bfd> – Zugriff am 30.6.2004.

gestartetem LDAP-Dienst keine konsistente Datensicherung gewährleistet werden.¹²⁹ Um einen konsistenten Datenbestand zum Zeitpunkt der Datensicherung zu erreichen gibt es mehrere Möglichkeiten; in diesem Fall sollen zunächst drei Alternativen unter Berücksichtigung der zur Verfügung stehenden Mittel in Betracht gezogen werden. Generell empfiehlt es sich jedoch die Verzeichnisse `/kolab/var/openldap` sowie `/kolab/etc/openldap` in die Sicherung einzubeziehen um sowohl die Datenbank als auch die Konfigurationsdateien zu sichern.

4.5.1.1 Offline Backup

Als einfache Lösung zur Gewährleistung der Konsistenz kann auf dem Kolab-Server vor Beginn der Datensicherung der LDAP-Dienst beendet werden um Schreibvorgänge während der Datensicherung zu vermeiden. Dieses Verfahren wird allgemein als *offline backup* bezeichnet. In diesem Fall muss mindestens das Verzeichnis `/kolab/var/openldap/openldap-data` in die Sicherung mit einbezogen werden, denn dort befinden sich die Dateien der LDAP-Datenbank. Im Falle des Restores müssen diese Dateien wieder in das ursprüngliche Verzeichnis kopiert und danach der LDAP-Dienst gestartet werden.

4.5.1.2 Export der Daten

Eine weitere Möglichkeit zur Datensicherung ist der Export der LDAP-Datenbank in eine LDIF-Datei (siehe Kapitel 4.1.4), die mit dem Werkzeug `/kolab/sbin/slapcat` erzeugt und anschliessend gesichert werden kann.¹³⁰ Eine kurze Zusammenfassung einer möglichen Vorgehensweise der Datensicherung sowie der Datenwiederherstellung ist in einer Online-Dokumentation¹³¹ sowie in Kapitel 4.6.2 beschrieben.

4.5.1.3 Online Backup

Bei der dritten Möglichkeit kann die LDAP-Datenbank bei entsprechender Infrastruktur und der Forderung nach einer hohen Verfügbarkeit unter Verwendung des Replika-

¹²⁹vgl. OpenLDAP Foundation: openLDAP Faq-o-Matic: How do I backup my directory? 2004 in: <http://www.openldap.org/faq/data/cache/287.html> – Zugriff am 26.5.2004.

¹³⁰vgl. OpenLDAP Foundation: openLDAP 2.2 Administrator's Guide; 2004 in: <http://www.openldap.org/doc/admin22/dbtools.html#Creating%20a%20database%20off-line> – Zugriff am 26.5.2004.

¹³¹vgl. Juniper Networks: Backing Up the Directory; 2004 in: <http://www.juniper.net/techpubs/software/management/sdx/sdx400/sw-sdx-admin/download/directory-archiving.pdf> – Zugriff am 14.6.2004.

tions-Dienstes slurpd auf einen LDAP Slave-Server repliziert und dort nach Herunterfahren des LDAP-Dienstes slapd sowie des Replikations-Dienstes slurpd auf einem LDAP Slave-Server gesichert werden.¹³² Damit wird erreicht, dass der LDAP-Dienst des Kolab-Servers nicht heruntergefahren werden muss und die Datenbank auf dem LDAP Slave-Server gesichert werden kann. Dieses Datensicherungsszenario bietet sich im Zusammenhang mit einer hochverfügbaren HA-Lösung an, da die Verfügbarkeit des Kolab-Servers durch die Sicherung der LDAP-Datenbank nicht beeinträchtigt wird. Im Falle einer Datenrücksicherung müssen die gesicherten Datenbank-Dateien wieder in das Verzeichnis `/kolab/var/openldap/openldap-data` kopiert werden.

4.5.2 Sicherung der Postkörbe

Für die Sicherung der Postkörbe sollte in jedem Fall das Verzeichnis `/kolab/var/imapd` gesichert werden. Die Sicherung der Konfigurationsdateien erfolgt durch die Einbeziehung des Verzeichnisses `/kolab/etc/imapd`. Um eine konsistente Sicherung der Daten zu erreichen muss der Datenbestand idealerweise mit Hilfe eines *Snapshot*-Verfahrens¹³³ kopiert werden; dabei wird ähnlich einer Festplattenspiegelung eine konsistente 1:1-Kopie erzeugt, die dann gesichert werden kann. Hierbei ist allerdings zu beachten, ob das verwendete Dateisystem das Snapshot-Verfahren unterstützt. Wird kein Snapshot-Verfahren angewendet, können die relevanten Daten auch mit Hilfe von herkömmlichen Verfahren wie z.B. durch die Erstellung eines *tar*-Archivs bei einem nicht aktiven IMAP-Dienst gesichert werden. Soll ein Backup bei aktivem IMAP-Dienst erfolgen, können die Postkorb-Dateien ohne weitere Vorkehrungen gesichert werden, allerdings besteht die Gefahr, dass während des Backups Daten in den zu sichernden Dateien geändert werden und somit eine Inkonsistenz entsteht. In diesem Fall muss bei einem Restore eine mögliche Inkonsistenz mit dem Werkzeug `/kolab/bin/cyrreconstruct` behoben werden.^{134, 135}

¹³²vgl. Carter: LDAP System Administration, S. 87.

¹³³vgl. Batten, I.: cyrus server and backup; in: <http://www.mail-archive.com/info-cyrus@lists.andrew.cmu.edu/msg11908.html> – Zugriff am 30.5.2004.

¹³⁴vgl. Wilzopolski, A.: Zentralanbindung; in: <http://www.heise.de/ix/artikel/1999/06/137/> – Zugriff am 01.6.2004.

¹³⁵vgl. Mullet, D. und Mullet, K.: Managing IMAP; in: <http://www.oreilly.com/catalog/mimap/chapter/ch09.html#89986> – Zugriff am 26.7.2004.

4.6 Weitere Betriebsaspekte

4.6.1 Erweiterbarkeit

Kolab als flexibler Groupware Server offeriert aufgrund des Open Source basierten Ansatzes viele denkbare Alternativen¹³⁶ im Hinblick auf Erweiterungen. *AMaViS*¹³⁷ bietet eine Schnittstelle für Virens Scanner verschiedener Hersteller wie beispielsweise Network Associates, H+B EDV, Sophos, Kaspersky oder F-Secure. Diese Antiviren-Produkte sind im Gegensatz zu der Schnittstelle AMaViS allerdings kostenpflichtig. Das Ausfiltern von Spam-Nachrichten ist auf Basis von Postfix auf zwei verschiedene Arten möglich; zum einen beherrscht Postfix sog. *Header-* und *Bodychecks*¹³⁸, zum anderen kann die Software *SpamAssassin* als Postfix-Plugin mittels verschiedener Mechanismen wie z.B. Blacklists und Header- bzw. Textanalysen Spam-Nachrichten ausfiltern. Ergänzend ist die Nutzung der Skriptsprache Sieve zur Filterung von Spam-Nachrichten möglich (siehe Kapitel 3.5.2). Um eine Nutzung von Kolab ohne einen Fat-Client zu ermöglichen, kann ein webbasierter Thin-Client wie z.B. Horde¹³⁹ genutzt werden, welcher allerdings zur Zeit noch nicht die volle Funktionalität wie die eines Fat-Clients bietet und in dem folgenden Kapitel 5.4 noch näher untersucht wird. Eine praktische Erweiterung des Kolab-Servers wäre die Nutzung eines bestehenden *Active Directory*-Verzeichnisdienstes als Adressbuch sowie zur Authentifizierung. Hierbei besteht allerdings die Schwierigkeit, dass die im Active Directory verwendeten Schemata teilweise stark von den standardisierten LDAP-Schemata abweichen und in dieser Form nicht für Kolab nutzbar sind. Aufgrund des frei verfügbaren Quellcodes und offener Standards ist es allerdings ebenso möglich, erweiterte Funktionalitäten durch eigene Entwicklungen zu realisieren (siehe Kapitel 2.2).

4.6.2 Datenpflege

Der Kolab-Server bietet über das Webinterface eine komfortable Möglichkeit, die verschiedenen Dienste des Kolab-Servers zu administrieren, Benutzer zu verwalten, Grup-

¹³⁶vgl. Erfrakon: Kolab Server Technical Description; 2003 in: <http://kroupware.org/technical-1.0.1-html/c593.html> – Zugriff am 30.5.2004.

¹³⁷vgl. AMaViS: aMaViS - A Mail Virus Scanner; 2004 in: <http://www.amavis.org/> – Zugriff am 30.5.2004.

¹³⁸vgl. Hispalinux: anti-Spam Utilities; 2004 in: <http://www.hispalinux.es/~data/postfix/> – Zugriff am 30.5.2004.

¹³⁹vgl. The Horde Project: The Horde Project; 2004 in: <http://www.horde.org/about.php> – Zugriff am 31.5.2004.

pen anzulegen und Adressbücher zu pflegen. Zur Pflege eines umfangreichen LDAP-Datenbestands empfiehlt es sich, eine automatisierte Bearbeitung einer LDIF-Datei durchzuführen. Einige Hinweise dazu gibt der FAQ-Bereich der Kroupware Homepage.¹⁴⁰ Hierbei wird ähnlich verfahren wie bei der Erstellung eines Datenbank-Exports als Backup-Strategie (siehe Kapitel 4.5.1.2): Der Kolab-Server wird – um Schreibzugriffe während des Exports zu verhindern – gestoppt, anschliessend wird mittels des Werkzeugs `/kolab/sbin/slapcat` die Datenbank in eine LDIF-Datei exportiert. An dieser Datei werden nun mit Hilfe eines Texteditors oder Skripts die benötigten Änderungen vorgenommen. Der bisherige Datenbestand muss vor dem Import der geänderten Daten entfernt werden; dies geschieht, indem die unter `/kolab/var/openldap/openldap-data` befindlichen Dateien gelöscht oder verschoben werden. Im letzten Schritt werden die veränderten Daten mit dem Werkzeug `/kolab/sbin/slapadd` importiert und der Kolab-Server wieder gestartet. Dieses Verfahren wird auch in Kapitel 4.5 in einem anderen Zusammenhang erläutert. Eine Auflistung verdeutlicht die erforderlichen Schritte:

```
[root@niobe root]# /kolab/etc/rc all stop
OpenPKG: stop: openldap, sasl, apache, imapd, postfix, proftpd, kolab.
[root@niobe root]# /kolab/sbin/slapcat -f /kolab/etc/openldap/slapd.conf \
-l /tmp/dbdump.ldif
```

Nach dem Export des Datenbestandes der LDAP-Datenbank erfolgt nun die Bearbeitung der Datei `/tmp/dbdump.ldif` durch einen Texteditor oder ein Skript. Anschliessend werden die bestehenden Datenbankdateien gelöscht und die editierte LDIF-Datei wieder importiert:

```
[root@niobe root]# rm -f /kolab/var/openldap/openldap-data/*
[root@niobe root]# /kolab/sbin/slapadd -f /kolab/etc/openldap/slapd.conf \
-l /tmp/dbdump.ldif
[root@niobe root]# /kolab/etc/rc all start
OpenPKG: start: openldap, sasl, apache, imapd, openpkg, postfix, proftpd
OpenPKG: start: kolab.
```

Für grössere LDAP-Datenbanken wird in dem FAQ-Bereich der Kroupware Homepage eine regelmäßige Indizierung empfohlen, um die Performanz bei Suchvorgängen zu erhöhen.¹⁴¹ Dies kann z.B. durch einen Eintrag in die Datei `/var/spool/cron/root` durch den Super-User erfolgen:

```
00 6 * * * root /kolab/sbin/slapindex -b dc=foo,dc=bar
```

¹⁴⁰vgl. Kroupware Project: Kroupware Project Frequently-Asked Questions; 2003 in: <http://kroupware.org/faq/faq.html#Kolab%20Server2> – Zugriff am 14.6.2004.

¹⁴¹vgl. Kroupware Project: Kroupware Project Frequently-Asked Questions; 2004 in: <http://www.kroupware.org/faq/faq.html#Kolab%20Server5> – Zugriff am 26.5.2004.

4.6.3 Benutzerfreundlichkeit

Die Verwendung des Webinterface zur Erstellung von Abwesenheitsbenachrichtigungen oder persönlichen Adressbüchern ist für erfahrene Anwender ohne administrative oder fachtechnische Vorkenntnisse nach einer Einweisung durchaus zumutbar und erfordert keinen grösseren zeitlichen oder administrativen Aufwand. Der administrative Bereich des Kolab-Servers ist mittels des Webinterface intuitiv und komfortabel zu bedienen. Wichtige Funktionen wie die Benutzer- und Gruppenverwaltung, Administration der Dienste oder Verwaltung von Adressbüchern lassen sich mit geringem Aufwand durchführen; sind grössere Datenoperationen durchzuführen, so stehen auch andere Verfahren zur Verfügung (siehe Kapitel [4.6.2](#)).

4.6.4 Administrativer Aufwand

Der administrative Aufwand für die reine Installation eines Kolab-Servers ist von vielen Parametern abhängig, z.B. ob es sich um einen einzelnen Server oder ein Clustersystem handelt und ob die Installation mit Source-Paketen oder mit vorkompilierten Paketen durchgeführt wird. Die Pakete des ZfOS-Archivs bieten eine für den Administrator komfortable Möglichkeit, innerhalb weniger Minuten eine funktionstüchtige Kolab-Server Installation durchzuführen. Treten bekannte Fehler bei der Installation auf, lassen sich diese i.d.R. zügig beheben; treten bisher nicht bekannte Fehler auf, kann die Fehlersuche aufgrund der noch geringen Verbreitung des Kolab-Servers im betrieblichen Einsatz und der dementsprechend geringen Anzahl an Erfahrungsberichten bzw. Dokumentation sehr viel Zeit in Anspruch nehmen. Ist ein Kolab-Server erst einmal funktionsfähig, entsteht weiterhin Aufwand für die Benutzer- und Gruppenpflege. Sofern eine Groupware-Lösung nicht grundlegend neu eingeführt wird, muss außerdem in einem bestehenden betrieblichen Umfeld eine Migration des bestehenden Groupware-Systems durchgeführt werden, welche sich je nach den Möglichkeiten des Datenexports der bestehenden Lösung als einfach, oder auch schwierig und zeitaufwändig erweisen kann. Des weiteren ist fraglich, ob das Format des Datenexports der bestehenden Lösung direkt kompatibel zu dem Import-Formaten der LDAP- bzw. Mail-Datenbank des Kolab-Servers ist, oder ob mittels spezieller Werkzeuge zunächst tiefgreifende Veränderungen an dem Datenbestand vorgenommen werden müssen, um den Datenimport zu ermöglichen. Folglich ist festzuhalten, dass der administrative Aufwand für den einzelnen Fall betrachtet werden muss. Insbesondere wenn bestehende Systeme migriert werden sollen, ist eine umfangreiche und vorausschauende Planung in Verbindung mit ausführlichen Testläufen unumgänglich.

5 Praktische Betrachtung der Kolab-Clients

5.1 Kolab KDE-Client

5.1.1 Konzept und Plattform

Der im Rahmen des Kroupware Projekts entwickelte KDE Kolab-Client baut auf den Teilapplikationen der *Kontakt*-Suite des für viele Plattformen verfügbaren Desktop-Managers KDE auf (siehe Kapitel 3.5.3). Eine Zusammenstellung der unterstützten Funktionen des KDE Kolab-Clients findet sich in Tabelle 5.1.

Category	Sub-Category	KDE	Horde
Mail	IMAP	Disconnected	Yes
	POP3	Yes	No
Groupware (IMAP)	Calendar	Yes	Partial
	Task List	Yes	Yes
	Memos	Yes	Yes
	Contacts	Yes	Yes
	Meeting Requests (Recv)	Yes	No
	Meeting Requests (Send)	Yes	No
	Task Requests (Recv)	Yes	No
	Task Requests (Send)	Yes	No
	Free/Busy View	Yes	No
Address Book	IMAP	Yes	Yes
	LDAP	Yes	Yes
Future	IMAP IDLE	No	No

Tabelle 5.1: Funktionen der Kolab-Clients¹⁴²

Zu der Kontakt Applikations-Suite gehören die verschiedenen Komponenten *KMail*

¹⁴²vgl. Kolab.org: Kolab Clients - Feature Matrix; 2004 in: <http://kolab.org/client-features.html> – Zugriff am 9.5.2004

(E-Mail-Client), *KOrganizer* (Kalender), *KAddressBook* (Adressbuch), *KNotes* (Notizbuch), *KNode* (Newsreader) und *KDE PIM* (PDA Werkzeuge).¹⁴³ Der KDE Kolab-Client ist prinzipiell auf jedem KDE 3.1 Desktop lauffähig und wird somit von einer breiten Basis von unterschiedlichen Betriebssystemen unterstützt (siehe Kapitel 3.5.3). Zu dem Funktionsumfang gehört ein Konfigurationsassistent, der die verschiedenen Optionen zur Kommunikation mit dem Kolab-Server anbietet.¹⁴⁴ Der KDE Kolab-Client unterstützt als einziger der untersuchten Kolab-Clients die Synchronisation von Daten mit einem PDA. Abbildung 5.1 zeigt die Einrichtung eines Kalendereintrags mittels des KDE Kolab-Client.

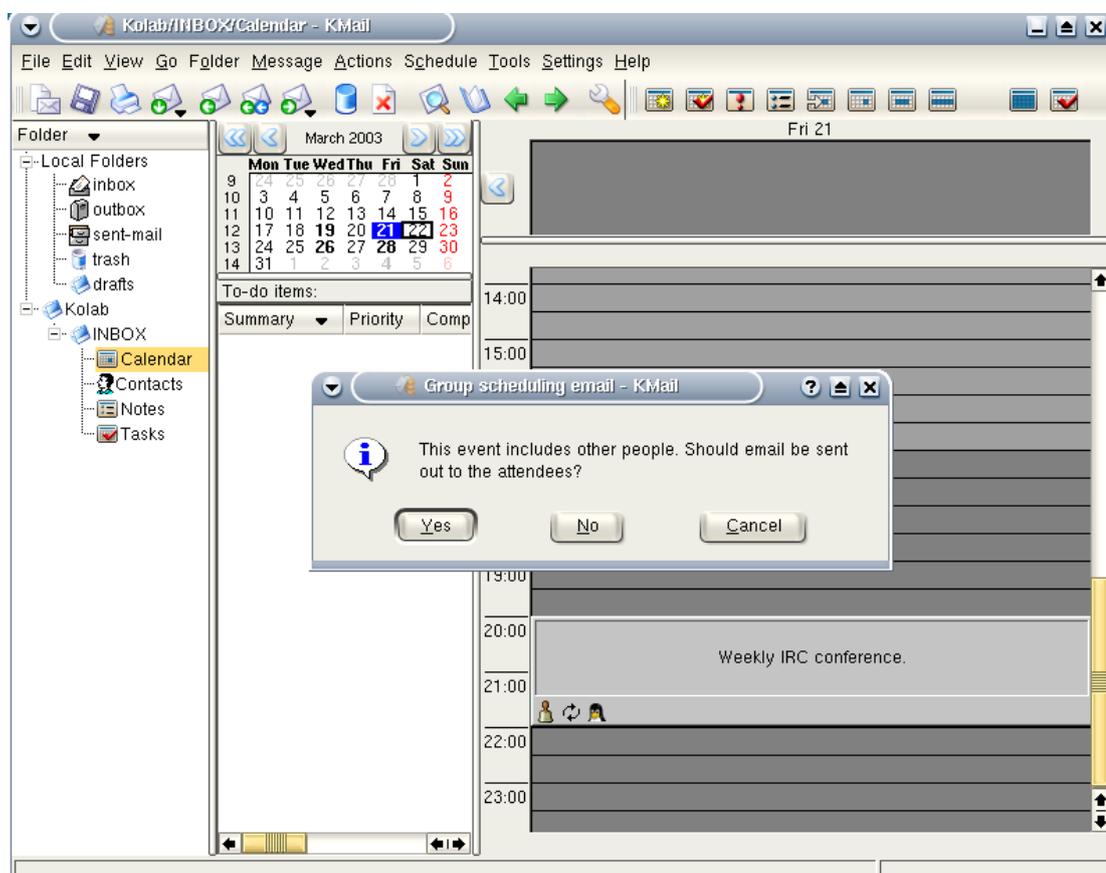


Abbildung 5.1: Kalender im KDE Kolab-Client¹⁴⁵

¹⁴³vgl. KDE e.V.: Components & Features; 2004 in: <http://kontakt.org/components.php> – Zugriff am 10.5.2004.

¹⁴⁴vgl. Kroupware.org: KDE Kolab-Benutzerhandbuch; 2004 in: http://kroupware.org/groupware_de-1.0.1-html/c38.html – Zugriff am 28.7.2004.

¹⁴⁵vgl. Kolab Project: Screenshot Gallery; 2004 in: <http://kolab.org/images/shot-kde-client-calendar1.png> – Zugriff am 4.8.2004

5.1.2 Installation

Die Installationspakete des KDE Kolab-Clients können von der Erfrakon Homepage¹⁴⁶ heruntergeladen und mittels der zugehörigen Installationsanleitung¹⁴⁷ installiert werden. Es ist zu beachten, dass vor Beginn der Installation die Softwarepakete *kdenetwork* und *kdepim* nicht installiert sind bzw. deinstalliert werden, da sonst Konflikte bei der Installation auftreten können. Das Paket *openldap-clients* hingegen muss vor Beginn der Installation bereits installiert sein. Die Installation des KDE Kolab-Clients sollte aufgrund eigener Untersuchungen nur durch einen erfahrenen Administrator durchgeführt werden, da bei der Installation häufig Fehler auftreten, die allerdings durch manuelle Anpassungen behoben werden können. Da keine vorkompilierten Binary-Pakete im RPM-Format zur Verfügung stehen, muss die Software für die jeweilige Plattform eigenständig kompiliert werden. Dieser Vorgang kann je nach der zugrundeliegenden Hardware einen längeren Zeitraum in Anspruch nehmen. Da diese Vorgehensweise bei einer größeren Anzahl von Arbeitsstationen unwirtschaftlich ist, können aus den Sourcecodes auch Installationspakete im RPM-Format erzeugt werden, die auf Arbeitsstationen mit geringem Zeit- und somit geringem Kostenaufwand installiert werden können.

5.1.3 Sicherheit

Bei dem Entwurf des KDE Kolab-Client wurde die Verwendung einer Public Key Infrastructure (PKI) – welche eine Verschlüsselung des E-Mail-Verkehrs mit Zertifikaten auf Applikationsschicht ermöglicht – vorgesehen. Diese im KDE Kolab-Client enthaltene Funktionalität basiert auf den Ergebnissen des ebenfalls von dem BSI ausgeschriebenen Projekts ägypten/Sphinx (siehe Kapitel 3.5.2). Die Nachrichtenübertragung kann auf Transportebene über eine SSL/TLS-verschlüsselte IMAP-Verbindung erfolgen.

5.1.4 Benutzerfreundlichkeit

Die Benutzerfreundlichkeit des KDE Kolab-Client ist für einen geübten Anwender der KDE Contact Suite aufgrund der bereits vorhandenen Erfahrung und gewohnten

¹⁴⁶Vgl. Erfrakon: KDE Kolab Client; 2004 in: <http://www.erfrakon.de/projects/kolab/download/> – Zugriff am 23.6.2004.

¹⁴⁷Vgl. Kroupware Project: Install Kolab KDE Client; 2004 in: <http://www.kroupware.org/howto-kolab-kde-client.html> – Zugriff am 23.6.2004.

Umgebung gegeben. Unerfahrene Anwender benötigen eine Einweisung in die vorhandenen Funktionen und Verfahren.

5.2 Aethera

Aethera ist ebenso wie der KDE Kolab-Client ein Groupware Fat-Client und wird von der Firma theKompany.com aktuell in der Version 1.1.0 kostenlos angeboten.¹⁴⁸ Dieser Client unterstützt das Kolab-Server Konzept, und dessen Entwickler verfolgen das Ziel, zukünftig die häufig betrieblich genutzte Kombination Outlook/Exchange durch Aethera/Kolab ersetzen zu können.¹⁴⁹ Abbildung 5.2 zeigt die Nutzung der Mail Sektion des Aethera-Clients.

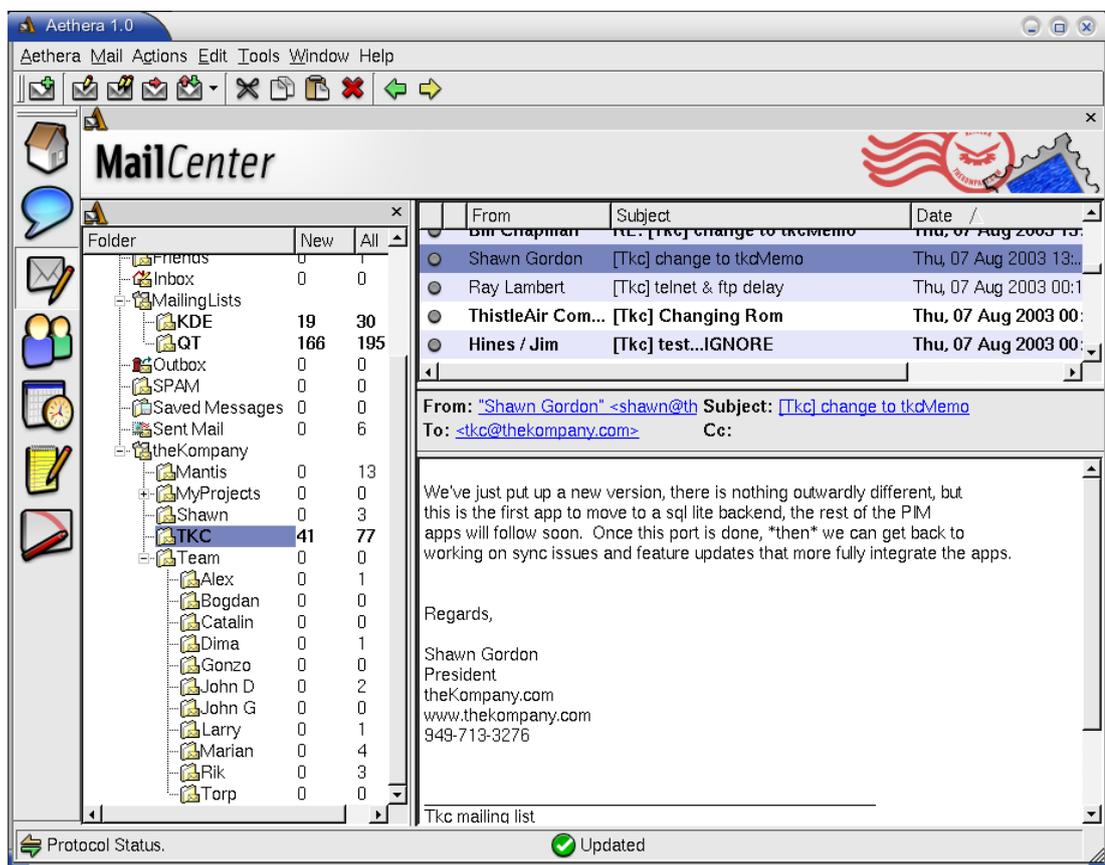


Abbildung 5.2: Die Mail Sektion im Aethera-Client¹⁵⁰

¹⁴⁸vgl. theKompany.com: aethera: PIM, PDR, Messaging and Groupware: Introduction; 2004 in: <http://www.thekompany.com/projects/aethera/> – Zugriff am 28.7.2004.

¹⁴⁹vgl. theKompany.com: aethera: PIM, PDR, Messaging and Groupware: Overview; 2004 in: <http://www.thekompany.com/projects/aethera/overview.php3> – Zugriff am 28.7.2004.

¹⁵⁰vgl. theKompany.com: aethera: Screenshots; 2004 in: http://www.thekompany.com/projects/aethera/images/aethera_1.png – Zugriff am 4.8.2004

5.2.1 Konzept und Plattform

Zum Zeitpunkt der Entstehung dieser Arbeit ist Aethera für die Plattformen Windows Me/XP, Linux und Mac OS-X erhältlich. Der Kolab-Client Aethera bietet bereits bei der Einrichtung eines Benutzerkontos die Möglichkeit, zwischen verschiedenen alternativen Zugriffsarten auf einen Groupware Server zu wählen, darunter auch die Einrichtung eines Benutzerkontos in Verbindung mit einem Kolab-Server. Der Aethera Client unterstützt die Protokolle POP3, IMAP und SMTP, sowohl verschlüsselt als auch unverschlüsselt. Hinzu kommen Funktionen wie persönliche Kalender, Notizen und Adressbücher. Optional werden kostenpflichtige Erweiterungen für *Instant Messaging*, *Whiteboards* und VoIP (Voice over IP) angeboten.¹⁵¹

5.2.2 Installation

Die im Rahmen dieser Arbeit durchgeführten Installationen unter Windows 2000, XP und Fedora Linux Core 1 sind ohne größeren Aufwand oder Kenntnisse über das Produkt durch den Anwender oder Administrator durchführbar. Im Gegensatz zu dem KDE Kolab-Client sind die für Linux verfügbaren Installationspakete sowohl als Sourcepakete als auch im RPM-Format erhältlich, wodurch eine verteilte Installation auf mehreren Arbeitsstationen in einem betrieblichen Umfeld erleichtert wird.

5.2.3 Sicherheit

Aethera unterstützt ebenso wie der KDE Kolab-Client die Verschlüsselung der Daten auf Transportebene, allerdings nicht die Verschlüsselung auf Applikationsebene mittels PKI-Zertifikaten.

5.2.4 Benutzerfreundlichkeit

Der Aethera Client verursacht auf den Plattformen Windows 2000/XP und Fedora Linux Core 1 eine hohe Ressourcenauslastung, wodurch das zügige Arbeiten erschwert wird. Der Aufbau der Oberfläche ist für ungeübte Anwender gewöhnungsbedürftig und erfordert eine Einarbeitung. Werden Änderungen an der Konfiguration des Clients vorgenommen, so muss dieser neu gestartet werden.

¹⁵¹vgl. theKompany.com: aethera: PIM, PDR, Messaging and Groupware: Overview.

5.3 Outlook mit Connector

Der Groupware-Client Microsoft Outlook wird normalerweise in Verbindung mit einem Microsoft Exchange Groupware-Server eingesetzt. Wird ein Connector verwendet, so kann Outlook auch in Verbindung mit einem Kolab-Server genutzt werden. Es stehen mehrere kostenpflichtige Connectoren verschiedener Hersteller zur Verfügung, so z.B. die Produkte *Bynari InsightConnector*¹⁵², *Toltec Connector*¹⁵³ sowie der *Konsec Connector*.¹⁵⁴ In den FAQ der Kroupware Homepage wird der Toltec-Connector favorisiert: „Currently most success reports are available using the Toltec Connector from a South African company.“¹⁵⁵ Abbildung 5.3 zeigt die Terminverwaltung über Outlook mittels des Toltec Connectors.

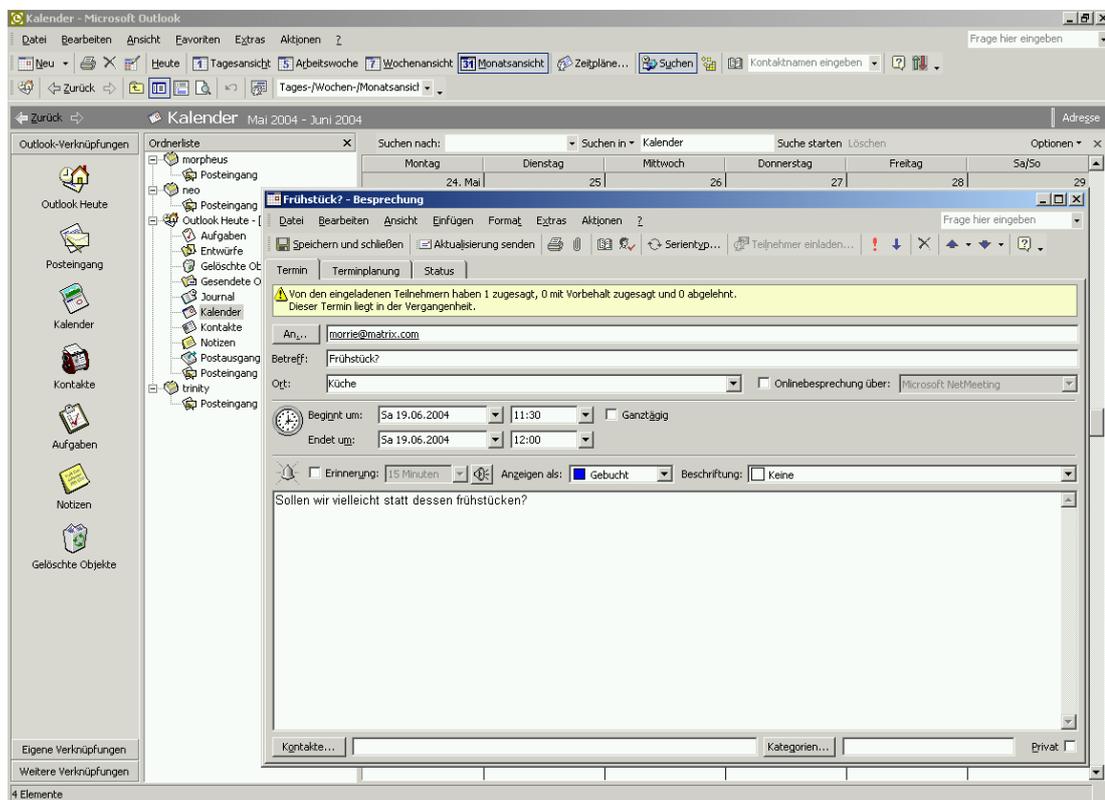


Abbildung 5.3: Terminplanung in Outlook

¹⁵²vgl. Bynari, Inc.: Insight Connector; 2004 in: <http://www.bynari.net/index.php?id=7> – Zugriff am 4.8.2004.

¹⁵³vgl. Radley Network Technologies CC: Toltec Groupware Connector; 2004 in: <http://www.toltec.co.za/> – Zugriff am 4.8.2004.

¹⁵⁴vgl. KONSEC: MS Outlook Konsec-Konnektor; 2004 in: <http://konsec.de/KON/de/konnektor.html> – Zugriff am 4.8.2004.

¹⁵⁵vgl. Kroupware Project: Kroupware Project Frequently-Asked Questions; 2004 in: <http://www.kroupware.org/faq/faq.html#KDE%20Client0> – Zugriff am 4.8.2004.

5.3.1 Konzept und Plattform

Der Outlook 2000 Groupware-Client kann unter Windows NT, Me, 2000 und XP genutzt werden. Für die Nutzung von Outlook 2000 ist – wie im vorherigen Abschnitt beschrieben – ein proprietärer Connector notwendig. Die Nutzung von Outlook als Client des zu entwickelnden Open Source Groupware-Servers war Bedingung der Ausschreibung des BSI (siehe Kapitel 3.1).

5.3.2 Installation

Microsoft Outlook 2000 gehört zum Lieferumfang des Microsoft Exchange Servers und ist Bestandteil von Microsoft Office 2000. Der Client kann über die Microsoft Office-Komponentenverwaltung auch nachträglich installiert werden. Um die Nutzung in Verbindung mit einem Kolab-Server zu ermöglichen, muss einer der genannten Connector-Plugins installiert und lizenziert werden. Bei dem in dieser Arbeit verwendeten Connector des Herstellers Toltec wurde ein für 30 Tage gültiger Lizenzschlüssel verwendet.

5.3.3 Sicherheit

Outlook unterstützt in Kombination mit Kolab ähnlich wie der Aethera-Client Sicherheit auf Transportebene durch SSL/TLS-verschlüsselte Verbindungen, jedoch keine Verwendung von PKI-Zertifikaten zur Verschlüsselung auf Applikationsebene. Aufgrund der hohen Verbreitung von Microsoft Outlook und dessen bekannten Sicherheitsproblemen existieren für diese Schwachstellen auch eine Vielzahl von Verfahren, mit denen diese Schwachstellen ausgenutzt werden können. Diese werden zwar durch Verwendung des Kolab Groupware-Servers reduziert, allerdings nicht ausgeschlossen.

5.3.4 Benutzerfreundlichkeit

Der Outlook-Client gehört aufgrund seiner hohen Verbreitung und Akzeptanz bei Anwendern (siehe Kapitel 3.5.1) zu den Clients, die ohne grösseren Schulungsaufwand eingesetzt werden können. Aufgrund der häufig vorhandenen Erfahrungen der Anwender im Umgang mit Microsoft Office-Produkten bietet der Client eine gewohnte und überschaubare Arbeitsoberfläche. Insgesamt ist dieser Client als benutzerfreundlich

zu betrachten; für geübte Microsoft-Anwender erschliessen sich die Funktionen ohne größeren Aufwand.

5.4 Horde Webclient

Die von dem Horde Projekt¹⁵⁶ entwickelte Software bietet eine webbasierte Plattform, die in Verbindung mit Kolab genutzt werden kann. Der Webclient Horde besteht aus mehreren Teilapplikationen des Horde Projekts, so z.B. Horde IMP (Webmail-Modul) und Horde Turba (Adressbuch-Modul), die für die Nutzung der Funktionen des Kolab-Servers notwendig sind. Die Funktionalitäten beschränken sich in diesem Zusammenhang auf das Empfangen und Versenden von E-Mail, die Nutzung globaler und persönlicher Adressbücher, die Erstellung eigener Ordner und Definition eigener Filterregeln (siehe Tabelle 5.1). Zur Veranschaulichung des Horde Webclients ist in Abbildung 5.4 die Verwaltung von E-Mail dargestellt.

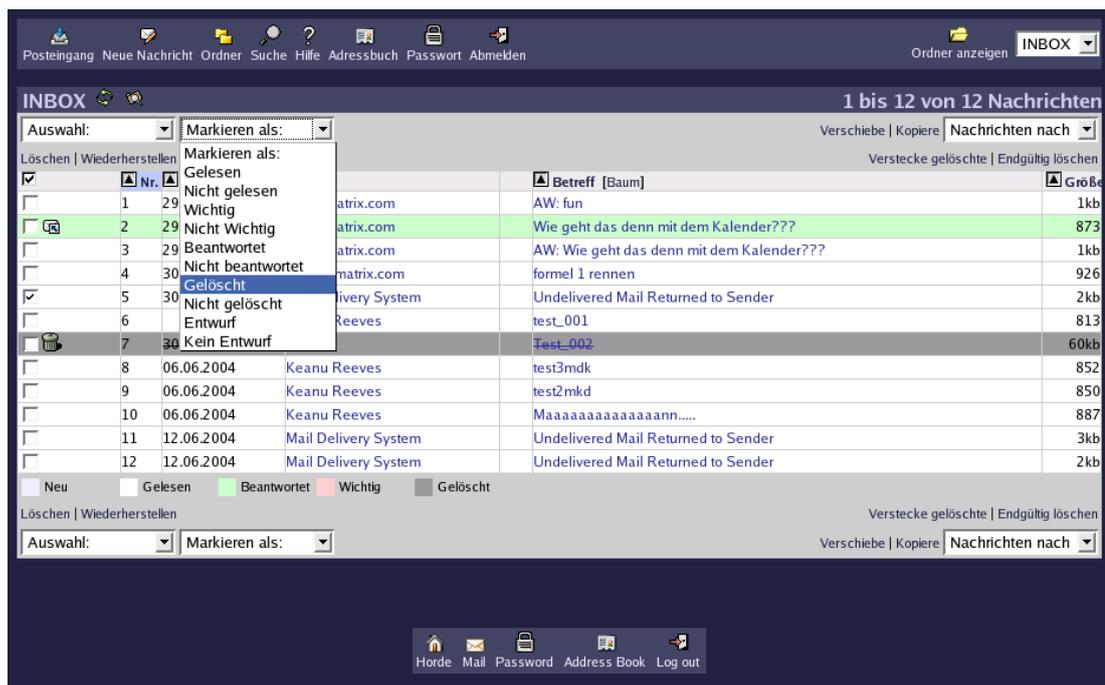


Abbildung 5.4: E-Mail-Verwaltung im Horde Webclient

Der Zugriff auf den Kolab-Server erfolgt nach der Installation von Horde mittels eines Webbrowsers. Die Funktionen des Horde Webclient in Verbindung mit Kolab sind für

¹⁵⁶vgl. The Horde Project: Horde User's FAQ; 2004 in: <http://www.horde.org/faq/user/general/index.php#g3> – Zugriff am 4.8.2004.

typische Groupware-Funktionen nicht ausreichend; jedoch ist der Zugriff mittels Webbrowser eine Alternative für reisende Anwender, deren Zugriffsmöglichkeit auf die Nutzung eines Webbrowsers beschränkt ist.

5.4.1 Konzept und Plattform

Das von dem Projekt verfolgte Konzept basiert auf der Verwendung von PHP-Modulen in Verbindung mit den von Kolab gebotenen Diensten wie Webserver und Mailserver. Die Software ist auf allen Unix-Varianten funktionsfähig, auf denen auch der Betrieb des Webservers Apache und der Skriptsprache PHP möglich ist.¹⁵⁷

5.4.2 Installation

Für die Nutzung von Horde ist es zunächst notwendig, über funktionstüchtige Apache- und PHP4-Installationen zu verfügen. Die Installation von Horde ist auf dem Kolab-Server durchzuführen; hier muss das heruntergeladene Softwarepaket im Dokumentenverzeichnis des Webservers entpackt werden. Zusätzlich müssen noch einzelne Module konfiguriert werden, um die Kolab-Dienste nutzen zu können. Eine ausführliche Installationsanleitung bieten die FAQ-Seiten des Horde Projekts.¹⁵⁸ Die Linux-Distribution Mandrake 10 bietet neben den Kolab Softwarepaketen im RPM-Format auch Pakete für Horde an. Deren Installation ist einfach durchzuführen; Konfigurationsarbeiten zur Nutzung der Kolab-Dienste über einen Webbrowser sind bei dieser Alternative nicht notwendig.

5.4.3 Sicherheit

Die Nutzung des Horde Webclient wird über eine SSL/TLS-verschlüsselte Verbindung realisiert und bietet dadurch Sicherheit auf Transportebene. Eine Verschlüsselung von Nachrichten mit Zertifikaten ist nicht möglich.

¹⁵⁷vgl. The Horde Project: Horde Administrator's FAQ; 2004 in: <http://www.horde.org/faq/admin/general/index.php#g12> – Zugriff am 4.8.2004.

¹⁵⁸vgl. The Horde Project: Horde Administrator's FAQ.

5.4.4 Benutzerfreundlichkeit

Die Arbeitsoberfläche des Horde Webclient ist klar gegliedert und erfordert einen geringen Einarbeitungsaufwand für den Anwender. Aufgrund des geringen Funktionsumfangs ist dieser Client nur für eine eingeschränkte Nutzung der Kolab-Dienste verwendbar, bietet aber die Möglichkeit, Zugang zu den Diensten eines Kolab-Servers über das Internet zu erhalten. Für den Zugriff auf einen Kolab-Server wird lediglich ein aktueller Webbrowser benötigt.

6 Wirtschaftliche Aspekte

6.1 Kostenbetrachtung

Ein wichtiger Aspekt bei der Entscheidung, ob Kolab als Open Source Groupware-Lösung eingesetzt werden soll, ist der Kostenfaktor. Für die Nutzung eines Kolab-Servers fallen im Gegensatz zu kommerziellen Lösungen keine Lizenzkosten an, selbstverständlich aber Betriebskosten für die Installation, Administration und Pflege des Systems (siehe Kapitel 4.6.4). Soll eine bestehende Groupware-Lösung migriert werden, entstehen Planungs- und Entwicklungskosten für die Planung, Durchführung und Nachbearbeitung der Migration. Wird eine bestehende Groupware-Umgebung migriert und soll ein anderer Groupware-Client zum Einsatz kommen, müssen auch Kosten für die Schulung der Benutzer im Umgang mit dem neuen Client betrachtet werden. Personalkosten für qualifizierte Mitarbeiter für die Einführung und Betrieb der Kolab Groupware-Lösung sollten ebenfalls betrachtet werden. Werden auf dem Server optionale Komponenten wie Virens Scanner (siehe Kapitel 4.6.1) eingebunden, sind laufende Kosten für Software in die Kalkulation mit einzubeziehen. Soll als Kolab-Client ein proprietäres Produkt wie Outlook eingesetzt werden, muss ein kostenpflichtiger Connector pro Arbeitsstation mit in die Anschaffungskosten einberechnet werden. Trotz der grossen Verbreitung von Outlook ist dieses kostenpflichtige Produkt nicht in jedem Unternehmen vorhanden und es fallen bei der Anschaffung Lizenzkosten an. Kosten für Infrastruktur, Hardware-Supportverträge und Datensicherung fallen sowohl bei einer kommerziellen als auch bei einer Open Source-Lösung gleichermaßen an. Um eine abschliessende Kostenbetrachtung aufstellen zu können, sind viele weitere Vor- und Nachteile von Open Source Software im Allgemeinen und die daraus resultierenden Einsparungen bzw. Mehrkosten – soweit quantifizierbar – einzubeziehen.

6.2 TCO-Betrachtung

Kostenbetrachtungen und -vergleiche von Open Source Software werden durch die Erstellung einer *Total Cost of Ownership*-Analyse (TCO) vorgenommen. Die Kostenanalyse anhand der TCO-Methode beinhaltet bei IT-Systemen üblicherweise die folgenden Punkte:¹⁵⁹

- Beschaffung
 - Erhebung der Anforderungen
 - Finanzierungsplan (Leasing, Kauf, Miete)
 - Kosten für Hard- und Software
 - Lieferkosten
- Betrieb
 - Disposition
 - Kosten der Inbetriebnahme
 - Kosten für technischen Support
 - Schulungskosten
 - Anteilige Kosten der Infrastruktur
- Außerstandsetzung
 - Kosten der Datenübernahme auf Nachfolgesysteme
 - Kosten für physischen Abtransport der Hardware

Eine detaillierte Aufschlüsselung der Berechnungsgrundlagen kann an dieser Stelle nicht aufgeführt werden, da das TCO-Verfahren zu den Geschäftsgeheimnissen der Gartner Group gehört. Für den Bereich Open Source Groupware stehen kaum veröffentlichte Studien zur Verfügung, speziell für Kolab als Open Source Groupware-Lösung existiert keine solche Analyse. Eine Studie des Marktforschungsunternehmens Soreon¹⁶⁰ bestätigt Open Source Groupware-Lösungen je nach Unternehmensgröße ein Einsparungspotential von bis zu 83% im Vergleich zu kommerziellen Lösungen wie Microsoft Exchange oder Lotus Domino.¹⁶¹ Aufgrund der unsicheren Informa-

¹⁵⁹vgl. Hang, J. und Hohensohn, D. H.: Eine Einführung zum Open Source Konzept aus Sicht der wirtschaftlichen und rechtlichen Aspekte; in: http://now.c-lab.de/veroeffentlichungen/einfuehrung/Anforderungskatalog_Teil_final.pdf – Zugriff am 4.8.2004.

¹⁶⁰vgl. Soreon Research: Soreon Research; 2004 in: <http://www.soreon.de/site1/> – Zugriff am 2.8.2004.

¹⁶¹vgl. SYSTEMS 2004: Einsparungen bis zu 25 % mit Microsoft-Alternativen; 2004 in: http://www.systems-world.de/id/8329/CMEntries_ID/29886 – Zugriff am 2.8.2004.

tionslage im Bezug auf Kostenanalysen von Open Source Software und Kolab kann an dieser Stelle keine objektive und fundierte Aussage über die Vor- und Nachteile des Einsatzes einer Kolab Groupware-Lösung getroffen werden.

6.3 Anreize für öffentliche Organe und KMU

Aufgrund von Rationalisierungsmaßnahmen im öffentlichen Bereich werden zunehmend Computersysteme in Stadtverwaltungen und Ämtern auf Open Source Software umgestellt. Die Initiatoren erhoffen sich durch die Ablösung der meist Windows-basierten Systeme neben Kosteneinsparungen und Herstellerunabhängigkeit auch erhöhte Sicherheit und Flexibilität. International bekannte Beispiele für Open Source-Migrationsprojekte bilden die Stadtverwaltungen von Schwäbisch Hall¹⁶² und München¹⁶³. Die von der Stadt München eingesetzte Groupware-Lösung basiert auf den Produkten der Unternehmen Critical Path (E-Mail) und Oracle (Kalender)¹⁶⁴, die jedoch mittelfristig im Verlauf des Open Source Migrationsprojekts *LiMux* durch eine Open Source Groupware-Lösung abgelöst werden soll. Während bei solchen Migrationen etablierte Open Source Software auf Server- sowie Desktop-Systemen zum Einsatz kommen, fehlt es noch an etablierten Lösungen für den Bereich der Groupware. Kolab gehört neben anderen Produkten bei solchen Überlegungen zu einer interessanten Alternative; der ehemalige Bundesbeauftragte für den Datenschutz Joachim Jacob zog den Einsatz von Kolab für Desktopsysteme bereits in Erwägung.¹⁶⁵ Die aktuelle Diskussion über die Gefahren von Softwarepatenten im Zusammenhang mit Open Source Software wirft allerdings neue Fragen auf. Zu der TCO-Betrachtung des Münchener Open Source Projekts *LiMux* berichtet der Vizepräsident von Gartner Research Andrea Di Maio: „Die Patentfrage mag den Münchenern klar gemacht haben, dass sie die Kosten und Risiken unterschätzt haben, als sie den TCO des *LiMux*-Projektes kalkulierten.“^{166, 167}

¹⁶²vgl. Ilg, P.: Umstieg auf Linux: Schwäbisch Hall macht es vor; in: <http://www.silicon.de/cpo/ts-plattformen/detail.php?nr=12594> – Zugriff am 4.8.2004.

¹⁶³vgl. Landeshauptstadt München Direktorium: *LiMux - Die IT-Evolution*; 2004 in: <http://www.muenchen.de/Rathaus/referate/dir/limux/89256/> – Zugriff am 4.8.2004.

¹⁶⁴vgl. Wolowicz, D. E.: Das Projekt *LiMux* stellt sich vor; in: http://www.muenchen.de/vip8/prod2/mde/_de/rubriken/Rathaus/bb_dir/limux/publikationen/aktionswoche.pdf – Zugriff am 7.8.2004, S. 9.

¹⁶⁵vgl. Krempf, S.: Der Bundesdatenschutzbeauftragte holt den Pinguin ins Haus; in: <http://www.heise.de/newsticker/meldung/33110> – Zugriff am 5.8.2004.

¹⁶⁶vgl. Borchers, D.: TCO und Patente: Gartner zur Münchener Linux-Migration; in: <http://www.heise.de/newsticker/meldung/50040> – Zugriff am 13.8.2004.

¹⁶⁷vgl. Maio, A. D.: Patent Issues Aren't the Only Cause for Munich's Linux Delay; in: http://www4.gartner.com/resources/122200/122264/patent_issues_a.pdf – Zugriff am 13.8.2004.

Für kleine und mittlere Unternehmen ist der Einsatz von Open Source Software laut einer Studie des Bundesministeriums für Wirtschaft und Arbeit (BMWA) aufgrund der Einsparung von Lizenzkosten sinnvoll. Einen beispielhaften Kostenvergleich von Open Source Software und proprietärer Software sowie Hinweise zum Einsatz von Open Source Software bietet ein Leitfaden des BMWA¹⁶⁸, der speziell an kleine und mittlere Unternehmen sowie Behörden adressiert ist.

¹⁶⁸Vgl. Bundesamt für Wirtschaft und Technologie: open-Source-Software Leitfaden; 2001 in: <http://bmwi-softwarepaket.de/gruender/pdf/broschueren/Open-Source-Software.pdf> – Zugriff am 9.8.2004, S. 25ff..

7 Ausblick und Fazit

7.1 Ausblick

Das im März 2004 gestartete Nachfolgeprojekt *Proko2* (Project for Kolab2) wurde von einem unbekanntem Auftraggeber beauftragt und soll die folgenden Ziele erreichen:¹⁶⁹

Kolab-Server:

- Integration eines Viren- und Spam-Filters
- Einführung von Speicherplatzbeschränkungen für Benutzer (Quotas)
- Nutzung mehrerer E-Mail-Adressen und Sendebestätigungen
- Nutzung verschiedener LDAP-Server
- Ausbaufähigkeit zu einem räumlich verteilten System

Kolab-Clients:

- Integration der KDE Kolab-Client Funktionalitäten in Kontact
- Optionale Entwicklung eines eigenständigen Windows Kolab-Clients in Verbindung mit standardisierten Schnittstellen und Datenformaten, um die parallele Verwendung von KDE Kolab-Clients und Windows Kolab-Clients zu ermöglichen
- Realisierung von Gruppen in Verbindung mit ACL und gemeinsam genutzten Verzeichnissen
- Nutzung mehrerer Benutzerkonten in einem Client

¹⁶⁹vgl. Reiter, B.: Proko2 is Good News Towards Kolab2; in: <http://www.kolab.org/pipermail/kolab-users/2004-April/000092.html> – Zugriff am 9.8.2004.

- Realisierung von gemeinsam genutzten Kalenderzugriffen und Projektfunktionalitäten
- Verbesserte Funktionalität hinsichtlich Abwesenheitsbenachrichtigungen und abgelaufenen Terminen

Kolab in der Version 2 wird voraussichtlich noch im Jahr 2004 veröffentlicht werden. Die neue Version des Kolab-Servers soll ausserdem als hochverfügbares System betrieben werden können. Konkrete Informationen zur Implementation sind allerdings bisher nicht verfügbar. Die Installationsroutine der Kolab2-Testversion bietet bereits die Möglichkeit, einen LDAP Slave-Server zu definieren. Des weiteren ist die webbasierte Administrationsoberfläche überarbeitet worden, in der auch die graphische Administration der neuen Funktionalitäten, wie z.B. Benutzer-Quota oder Spam/Viren-Filter, enthalten sind. Die Installation der zumeist aktualisierten Versionen der Kolab-Komponenten basiert auf der OpenPKG-Version 2.1, die im Juli 2004 veröffentlicht wurde. Die Funktionalitäten des Kolab KDE-Client sollen zukünftig in den Funktionsumfang der KDE Kontakt-Suite übergehen.¹⁷⁰ Aufgrund der Migration der Kolab KDE-Client Funktionalitäten in die Kontakt-Suite ist zu erwarten, dass sich das Interesse und damit auch die Verbreitung von Kolab als Open Source Groupware-Lösung zunehmen wird. Der Kolab-Server und der KDE Kolab-Client sind bisher nur in die Distribution von Mandrake Linux aufgenommen worden, in Zukunft könnten weitere Distributoren diese Open Source Groupware-Lösung in ihren Distributionsumfang aufnehmen. Als weiteres Ziel des Kolab-Projektes sollen die teilweise unübersichtlichen Verweise der Kroupware- und Kolab-Webseiten^{171, 172} transparenter und zentraler gestaltet werden.

7.2 Fazit

Diese Arbeit erläutert die konzeptionellen und praktischen Aspekte von Kolab als Open Source Groupware-Lösung und untersucht diese Aspekte aus betrieblicher Sicht. Dabei wird das Ziel verfolgt, dem fachlich versierten Publikum wichtige Details des Kolab-Projekts darzustellen und verschiedene Möglichkeiten für den betrieblichen Einsatz aufzuzeigen.

¹⁷⁰vgl. KDE e.V.: KDE 3.3 Feature Plan; 2004 in: <http://developer.kde.org/development-versions/kde-3.3-features.html> – Zugriff am 13.8.2004.

¹⁷¹vgl. Kolab Project: The Kolab Project::Home.

¹⁷²vgl. Kroupware Project: Kroupware Project; 2004 in: <http://www.kroupware.org/> – Zugriff am 24.8.2004.

Zur Erreichung dieses Ziels werden die Grundzüge von Groupware und CSCW dargestellt, die einzelnen Komponenten des Kolab-Servers detailliert betrachtet und deren Aufgaben im Kolab-Konzept erläutert. Weiterhin wird ein Konzept zur Realisierung eines Hochverfügbarkeits-Clusters vorgestellt und die verfügbaren Kolab-Clients im Hinblick auf verschiedene Aspekte analysiert. Abschliessend werden in dieser Arbeit die Kosten des Einsatzes eines Kolab-Servers in Verbindung mit Kolab-Clients aufgeführt und die Attraktivität von Open Source Groupware für den öffentlichen Sektor aufgrund von möglichen Kosteneinsparungen kritisch analysiert.

Das Konzept des Kolab-Projekts ist einfach und effektiv: Die Entwicklungen anderer Open Source Software-Projekte werden geschickt miteinander kombiniert und durch Entwicklung eigener Komponenten wie z.B. Administrationsoberfläche, Kolab-Backend und KDE Kolab-Client-Funktionen zu einer Open Source Groupware-Lösung vereint. Hinsichtlich des betrieblichen Einsatzes des Kolab-Servers in Verbindung mit Kolab-Clients wie Outlook, Kolab KDE-Client oder Alternativen müssen im Vergleich zu kommerziellen Lösungen noch einige Abstriche hinsichtlich Funktionalität und Benutzerfreundlichkeit gemacht werden. Für grössere Unternehmen ist die Migration zu Kolab nur bedingt sinnvoll, da im Vergleich zu proprietären Lösungen ein geringerer Funktionsumfang unterstützt wird, die notwendigen Migrationsverfahren von der bestehenden Lösung zu Kolab einen grösseren Planungsaufwand erfordern und sich die u.U. notwendige Einführung eines Kolab-Clients als schwierig gestalten kann. Zum Zeitpunkt der Erstellung dieser Arbeit sind keine Dokumentationen zu einer Migration von einer bestehenden Groupware-Lösung zu Kolab verfügbar. Aufgrund der Komplexität des Kolab-Konzepts sind auf administrativer Seite fundierte Kenntnisse der Komponenten für den Betrieb erforderlich. Ist die Einführung einer neuen Groupware-Lösung geplant, ist Kolab je nach den bestehenden Anforderungen durchaus eine sinnvolle Alternative zu proprietären Produkten und im Hinblick auf zukünftige Entwicklungen als eine strategisch ernstzunehmende Open Source Groupware-Lösung im Bereich der Client/Server-Konzepte. Wünschenswert für zukünftige Kolab-Versionen sind z.B. die Entwicklung eines freien Kolab-Clients für Windows-basierte Systeme und eines freien Connectors für Outlook, die Integration eines Open Source Instant Messengers sowie die Möglichkeit der Verwendung von Gruppenkalendern.

Nachdem Linux und Open Source Software auf Servern in vielen Bereichen zu einer akzeptierten und geschätzten Alternative zu Microsoft-Produkten geworden ist, zeichnet sich bereits eine zunehmende Bereitschaft des Einsatzes auf Desktop-Systemen

ab. Eine dabei zum Einsatz kommende, sichere, stabile und etablierte Open Source Groupware-Lösung mit einem betrieblich sinnvollen Funktionsumfang existiert bisher nicht.

Einer der entscheidenden Vorteile des Kolab Konzepts ist, dass eine Vielzahl verschiedener Clients unter zahlreichen Betriebssystemen unterstützt wird, darunter auch der weit verbreitete Microsoft Outlook-Client. Weiterhin werden in dem Konzept praxiserprobte und zuverlässige Software-Module verwendet, die in ihrem Entwicklungsstatus in weiten Teilen einen de facto-Standard im Bereich der Open Source Software darstellen.

Kolab entwickelt sich aus betrieblicher Sicht zu einer attraktiven Alternative, dessen Entwicklung bisher von einer noch kleinen Entwicklergruppe vorangetrieben wird. Mit dem Kreis der Nutzer von Kolab und deren Erfahrungsberichten entwickelt sich – nicht zuletzt durch die im März dieses Jahres eingeführte Kolab-User Diskussionsliste – eine für Open Source Software typische Gemeinschaft, in der Anwender und Entwickler gemeinsam über Probleme, Verbesserungen und Ideen diskutieren.

Glossar

Backup: Englisch es Synonym für Datensicherung.

Bootstrap: Initiale Einbindung oder Konfiguration von Software in einer vom Betriebssystem abgekapselten, von der Software selbst erstellten Umgebung.

Bulletin Board System: Diese Art von Kommunikation kann für Diskussionsforen oder elektronische Marktplätze genutzt werden und wird oft als webbasiertes schwarzes Brett bezeichnet.

Chat: Eine textbasierte Möglichkeit der entfernten Kommunikation in Echtzeit.

Connector: Dient der Anbindung eines proprietären Groupware-Clients an einen Kolab-Server.

CVS: Das Concurrent Versions System dient der Versionsverwaltung von Quellcode oder Dokumenten.

Daemon: „In the context of UNIX® systems, daemons are process that run in the background attending to various tasks without human intervention.“¹⁷³

Datenbank-Backend: siehe LDAP-Backend.

Fat-Client: Ein gesondertes Anwendungsprogramm zur Nutzung von serverbasierten Diensten, welches weite Teile der Systemlogik implementiert und den Server i.d.R. nur als Datenspeicher nutzt.

Free/Busy: Kalenderoption für die Anzeige von Frei/Belegt Zeiten.

Instant Messenger: Eine Client-Software, die in Verbindung mit einem Server u.a. die Möglichkeiten bietet, Textnachrichten in Echtzeit auszutauschen und Dateien zu versenden.

¹⁷³vgl. The FreeBSD Project: The BSD Daemon; 2004 in: <http://www.freebsd.org/copyright/daemon.html> – Zugriff am 5.8.2004.

Kolab-Backend: Ein auf der Skriptsprache Perl basierendes Skript zur Steuerung der einzelnen Dienste.

Kolab-Client: Ein Kolab-Client dient der Nutzung der durch Kolab bereitgestellten Groupware-Funktionen, es existieren mehrere Implementierungen.

Kolab-Komponenten: Die verschiedenen Einzeldienste und Module des Kolab-Serverkonzepts.

Kolab-Server: Das aus einzelnen Serverkomponenten bestehende Gesamtsystem.

Kroupware: Die frühere Bezeichnung von Kolab und Name des vom BSI ausgeschriebenen Projekts.

LDAP-Backend: Schnittstelle von LDAP zur verwendeten Datenbank.

LDAP-Datenbank: Eine Datenbank, die von dem auf dem LDAP Protokoll basierenden Verzeichnisdienst zur Haltung von Verzeichnisdaten dient.

LDAP-Dienst: Ein Verzeichnisdienst der auf dem LDAP Protokoll basiert.

LDAP-Slave Server: Ein Server zur zusätzlichen Vorhaltung von Verzeichnisdaten, üblicherweise werden Verzeichnisdaten nur auf einem Master-Server geändert und auf einen Slave-Server repliziert.

LDAP-Verzeichnisdienst: Synonym für LDAP-Dienst.

Legacy-Client: Ein aus technischer Sicht veralteter E-Mail-Client.

maildir-Format: Das maildir-Format ist das Datenbankformat des Cyrus-IMAPd zur Speicherung von E-Mails.

Mountpoint: Logische Stelle im Dateisystem, an der ein Dateisystem in den Verzeichnisbaum eingebunden wird.

MTA: Ein Message Transfer Agent oder Mail Transport Agent (MTA) dient der Zwischenspeicherung und Transport von E-Mail.

Open Source Software: Der Begriff Open Source Software umfasst viele unterschiedliche Lizenzmodelle. Die Anforderungen die ein Lizenzmodell mindestens erfüllen muss, um als Open Source Software klassifiziert werden zu können, sind durch drei wesentliche Merkmale charakterisiert.¹⁷⁴

¹⁷⁴Wikipedia Project: open Source; 2004 in: http://de.wikipedia.org/wiki/Open_Source – Zugriff am 18.8.2004.

- „Software liegt in einer für den Menschen lesbaren und verständlichen Form vor.“
- „Software darf beliebig kopiert, verbreitet und genutzt werden.“
- „Software darf verändert und in der veränderten Form weitergegeben werden.“

PKI: Eine Public Key Infrastructure ist ein System zur sicheren Identifizierung von Kommunikationspartnern mit kryptographischen Mitteln.

Plugin: Zusätzliche Erweiterung eines Programms durch ein Software-Modul.

Quota: Eine durch den Systemadministrator definierbare, serverbasierte Speicherplatzbegrenzung für Benutzer

Restore: Englisches Synonym für Datenrücksicherung.

Snapshot: Dieses Verfahren dient zur Erstellung einer 1:1-Kopie eines Datenbestandes.

Storage Subsystem: Ein Speichersystem.

Thin-Client: Im Zusammenhang mit Kolab dient ein Thin-Client der Nutzung von serverbasierten Diensten über ein Webinterface.

Trouble Ticket System: Ein Trouble Ticket System ermöglicht die elektronische Aufnahme, Zuweisung und Weiterleitung von Problem-Tickets, die mit einer Art elektronischer Laufzettel zur Problemlösung charakterisierbar sind.

Unix: Der in dieser Arbeit verwendete Begriff Unix steht für die Gruppe der Unix-artigen Betriebssysteme¹⁷⁵ und nicht für das Warenzeichen der Open Group.

Video Conferencing: Ermöglicht eine entfernte audiovisuelle Kommunikation mittels Bild und Ton.

VoIP: Der Begriff Voice over IP bezeichnet Telefonie über IP-Netze.

Webinterface: Browserbasierte Benutzerschnittstelle eines Programmes.

¹⁷⁵Vgl. Lévénéz, E.: Unix History; in: <http://www.levenez.com/unix/> – Zugriff am 25.8.2004.

Literaturverzeichnis

Buchquellen

Andresen, F.: Leeren verboten! in: Linux Magazin 9 2004, S. 78–79.

Burger, C.: Groupware - Kooperationsunterstützung für verteilte Anwendungen; Heidelberg 1997.

Carter, G.: LDAP System Administration; Sebastopol 2003.

Hunt, C.: TCP/IP; Köln 1998.

Klünter, D. und Laser, J.: LDAP verstehen, OpenLDAP einsetzen; Heidelberg 2003.

Kronsbein, M. und Weinert, T.: PHP4; Düsseldorf 2001.

Kuppinger, M.: Windows 2000 Server Das Handbuch; Unterschleißheim 2000.

Soltau, M.: Unix/Linux Hochverfügbarkeit; Bonn 2000.

Stickel, E.: Informationsmanagement; München 2001.

Teufel, S. et al.: Computerunterstützung für die Gruppenarbeit; Bonn 1995.

Internetquellen

- Albest: Error in slapd.conf.template; in: <http://eforum.de/viewtopic.php?t=114> – Zugriff am 21.6.2004.
- AMaViS: aMaViS - A Mail Virus Scanner; 2004 in: <http://www.amavis.org/> – Zugriff am 30.5.2004.
- Batten, I.: cyrus server and backup; in: <http://www.mail-archive.com/info-cyrus@lists.andrew.cmu.edu/msg11908.html> – Zugriff am 30.5.2004.
- Borchers, D.: TCO und Patente: Gartner zur Münchener Linux-Migration; in: <http://www.heise.de/newsticker/meldung/50040> – Zugriff am 13.8.2004.
- Bowman, G.: Collaborative Groupware Software; in: <http://www.svpal.org/~grantbow/groupware.html> – Zugriff am 31.7.2004.
- Brinck, T.: Usability First Groupware Introduction; in: <http://www.usabilityfirst.com/groupware/intro.txt> – Zugriff am 4.5.2004.
- Bundesamt für Sicherheit in der Informationstechnik: Sphinx Open Source; 2004 in: <http://www.bsi.de/aufgaben/projekte/sphinx/aegypten/opensour.htm> – Zugriff am 10.6.2004.
- Bundesamt für Sicherheit in der Informationstechnik: Startseite; 2004 in: <http://www.bsi.de/> – Zugriff am 9.5.2004.
- Bundesamt für Wirtschaft und Technologie: open-Source-Software Leitfaden; 2001 in: <http://bmwi-softwarepaket.de/gruender/pdf/broschueren/Open-Source-Software.pdf> – Zugriff am 9.8.2004.
- Bynari, Inc.: Insight Connector; 2004 in: <http://www.bynari.net/index.php?id=7> – Zugriff am 4.8.2004.
- Cancro, A. und Poulin, M.: Citadel/UX FAQ; in: <http://www.citadel.org/citadel-faq.php#sneezlesnorf> – Zugriff am 31.7.2004.
- Chu, H.: RE: Backend databases – what are the differences? in: <http://www.openldap.org/lists/openldap-software/200209/msg00167.html> – Zugriff am 11.5.2004.
- Citadel: Citadel/UX a messaging and collaboration platform for BBS and groupware applications; 2004 in: http://uncensored.citadel.org/viewcvs/viewcvs.cgi/*checkout*/citadel/docs/citadel.html?rev=HEAD&content-type=text/html#Introduction – Zugriff am 31.7.2004.

- Citadel: Citadel/UX a messaging and collaboration platform for BBS and groupware applications; 2004 in: http://uncensored.citadel.org/viewcvs/viewcvs.cgi/*checkout*/citadel/docs/citadel.html?rev=HEAD&content-type=text/html#Installation – Zugriff am 31.7.2004.
- Citadel: Citadel/UX: Flexible, powerful, community-oriented groupware; 2004 in: <http://www.citadel.org/> – Zugriff am 31.7.2004.
- Clemm, G. et al.: Web Distributed Authoring and Versioning (WebDAV) Access Control Protocol; in: <ftp://ftp.rfc-editor.org/in-notes/rfc3744.txt> – Zugriff am 14.7.2004.
- Code Fusion CC and Radley Network Technologies CC: Kolab Bootstrap Process; 2004 in: <http://ftp.intevation.de/kolab/contrib/kolab-bootstrap.pdf> – Zugriff am 20.5.2004.
- Crispin, M.: Internet Message Access Protocol - Version 4rev1; in: <ftp://ftp.rfc-editor.org/in-notes/rfc3501.txt> – Zugriff am 21.5.2004.
- Croombs, D.: Kolab on mandrake 10.0; in: <http://www.kolab.org/pipermail/kolab-users/2004-June/000534.html> – Zugriff am 21.6.2004.
- Dierks, T. und Allen, C.: The TLS Protocol Version 1.0; in: <ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt> – Zugriff am 8.8.2004.
- eGroupWare: eGroupWare - Enterprise Collaboration; 2004 in: <http://www.egroupware.org> – Zugriff am 31.7.2004.
- eGroupWare: Requirements to install eGW; 2004 in: <http://www.egroupware.org/requirements> – Zugriff am 31.7.2004.
- Erfrakon: Free Software Groupware Project - Architecture Paper; 2003 in: <http://kroupware.org/architecture-1.1/x124.html> – Zugriff am 13.7.2004.
- Erfrakon: Free Software Groupware Project - Architecture Paper; 2003 in: <http://kroupware.org/architecture-1.1/x133.html> – Zugriff am 13.7.2004.
- Erfrakon: Free Software Groupware Project - Architecture Paper; 2003 in: <http://kroupware.org/architecture-1.1/x154.html> – Zugriff am 14.7.2004.
- Erfrakon: Kolab Server Technical Description; 2003 in: <http://kroupware.org/technical-1.0.1-html/c593.html> – Zugriff am 30.5.2004.

- Erfrakon: Kolab Server Technical Description; 2003 in: <http://kroupware.org/technical-1.0.1-html/c421.html> – Zugriff am 13.7.2004.
- Erfrakon: Kolab Server Technical Description; 2003 in: <http://kroupware.org/technical-1.0.1-html/c368.html> – Zugriff am 13.7.2004.
- Erfrakon: Kolab Server Technical Description; 2003 in: <http://kroupware.org/technical-1.0.1-html/c27.html> – Zugriff am 13.7.2004.
- Erfrakon: Kolab Web Administration Technical Description; 2003 in: <http://kroupware.org/administration-1.0-html/x181.html> – Zugriff am 14.7.2004.
- Erfrakon: Kolab Web Administration Technical Description; 2003 in: <http://kroupware.org/administration-1.0-html/c44.html> – Zugriff am 15.7.2004.
- Erfrakon: Erfrakon: Erlewein, Frank, Konold und Partner; 2004 in: <http://erfrakon.de/> – Zugriff am 9.5.2004.
- Erfrakon: KDE Kolab Client; 2004 in: <http://www.erfrakon.de/projects/kolab/download/> – Zugriff am 23.6.2004.
- Erfrakon: Protocols; 2004 in: <http://www.kroupware.org/architecture-1.1/c87.html#AEN90> – Zugriff am 1.6.2004.
- Fielding, R. et al.: Hypertext Transfer Protocol - HTTP/1.1; in: <ftp://ftp.rfc-editor.org/in-notes/rfc2616.txt> – Zugriff am 21.5.2004.
- Grudin, J.: CSCW History and Focus; in: <http://www.ics.uci.edu/~grudin/Papers/IEEE94/IEEEComplastsb.html> – Zugriff am 13.5.2004.
- Hang, J. und Hohensohn, D. H.: Eine Einführung zum Open Source Konzept aus Sicht der wirtschaftlichen und rechtlichen Aspekte; in: http://now.c-lab.de/veroeffentlichungen/einfuehrung/Anforderungskatalog_Teil_final.pdf – Zugriff am 4.8.2004.
- High-Availability Linux Project: Frequently Asked Questions; 2004 in: <http://linuxha.trick.ca/FAQ#head-faa017f16120a4ebd51944b1db87529a7cf52bfd> – Zugriff am 30.6.2004.
- High-Availability Linux Project: Linux-HA Project Web Site; 2004 in: <http://linux-ha.org/> – Zugriff am 29.6.2004.
- Hispalinux: anti-Spam Utilities; 2004 in: <http://www.hispalinux.es/~data/postfix/> – Zugriff am 30.5.2004.

- Ilg, P.: Umstieg auf Linux: Schwäbisch Hall macht es vor; in: <http://www.silicon.de/cpo/ts-plattformen/detail.php?nr=12594> – Zugriff am 4.8.2004.
- Intevation GmbH: Intevation; 2004 in: <http://www.intevation.de/> – Zugriff am 9.5.2004.
- Intevation GmbH: Kroupware/Kolab - Freie Software Groupware; 2004 in: <http://www.intevation.de/projects/kroupware.de.html> – Zugriff am 9.5.2004.
- Juniper Networks: Backing Up the Directory; 2004 in: <http://www.juniper.net/techpubs/software/management/sdx/sdx400/sw-sdx-admin/download/directory-archiving.pdf> – Zugriff am 14.6.2004.
- KDE e.V.: KDE@CeBIT 2003; 2003 in: <http://kde.feratech.com/announcements/cebit2003.php> – Zugriff am 14.6.2004.
- KDE e.V.: Components & Features; 2004 in: <http://kontakt.org/components.php> – Zugriff am 10.5.2004.
- KDE e.V.: Distributions shipping KDE; 2004 in: <http://www.kde.org/download/distributions.php> – Zugriff am 12.5.2004.
- KDE e.V.: FAQ; 2004 in: <http://kontakt.kde.org/faq/#KontaktKolabKroupwareIgetconfusedWhatstheDeal> – Zugriff am 9.5.2004.
- KDE e.V.: KDE 3.3 Feature Plan; 2004 in: <http://developer.kde.org/development-versions/kde-3.3-features.html> – Zugriff am 13.8.2004.
- Klarälvdalens Datakonsult AB: KMail and mutt as Sphinx clients for German authorities; 2002 in: <http://www.klaralvdalens-datakonsult.se/?page=projects&sub=aegypten> – Zugriff am 15.7.2004.
- Klarälvdalens Datakonsult AB: Startseite; 2004 in: <http://www.klaralvdalens-datakonsult.se/> – Zugriff am 9.5.2004.
- Klensin, J.: Simple Mail Transfer Protocol; in: <ftp://ftp.rfc-editor.org/in-notes/rfc2821.txt> – Zugriff am 21.5.2004.
- Kolab Project: The Kolab Project::Home; 2004 in: <http://kolab.org/> – Zugriff am 21.7.2004.
- Kolab Project: The Kolab Project::HOWTOs; 2004 in: <http://kolab.org/howtos.html> – Zugriff am 14.6.2004.

- Kolab Project: Screenshot Gallery; 2004 in: <http://kolab.org/images/shot-kde-client-calendar1.png> – Zugriff am 4.8.2004.
- Kolab.org: Kolab Clients - Feature Matrix; 2004 in: <http://kolab.org/client-features.html> – Zugriff am 9.5.2004.
- Kolab.org: The Kolab-users Archives; 2004 in: <http://kolab.org/pipermail/kolab-users/> – Zugriff am 25.7.2004.
- Konold, M.: No Password Encryption? in: <http://www.kolab.org/pipermail/kolab-users/2004-May/000415.html> – Zugriff am 10.6.2004.
- Konold, M.: Quick Install Manual Kolab 1.0.4; in: <http://www.erfrakon.de/projects/kolab/download/kolab-server-1.0/src/QIM> – Zugriff am 15.5.2004.
- KONSEC: MS Outlook Konsec-Konnektor; 2004 in: <http://konsec.de/KON/de/konnektor.html> – Zugriff am 4.8.2004.
- Kreml, S.: Der Bundesdatenschutzbeauftragte holt den Pinguin ins Haus; in: <http://www.heise.de/newsticker/meldung/33110> – Zugriff am 5.8.2004.
- Kroupware Project: Design Criteria; 2003 in: <http://kroupware.org/administration-1.0-html/c24.html> – Zugriff am 11.6.2004.
- Kroupware Project: Kroupware Project Frequently-Asked Questions; 2003 in: <http://www.erfrakon.de/projects/kolab/documentation/faq/faq.html#Kolab%20Server1> – Zugriff am 10.6.2004.
- Kroupware Project: Kroupware Project Frequently-Asked Questions; 2003 in: <http://kroupware.org/faq/faq.html#Kolab%20Server2> – Zugriff am 14.6.2004.
- Kroupware Project: Install Kolab KDE Client; 2004 in: <http://www.kroupware.org/howto-kolab-kde-client.html> – Zugriff am 23.6.2004.
- Kroupware Project: Kroupware Project; 2004 in: <http://www.kroupware.org/> – Zugriff am 24.8.2004.
- Kroupware Project: Kroupware Project Frequently-Asked Questions; 2004 in: <http://www.kroupware.org/faq/faq.html#Kolab%20Server0> – Zugriff am 26.5.2004.
- Kroupware Project: Kroupware Project Frequently-Asked Questions; 2004 in: <http://www.kroupware.org/faq/faq.html#Kolab%20Server5> – Zugriff am 26.5.2004.

- Kroupware Project: Kroupware Project Frequently-Asked Questions; 2004 in: <http://www.kroupware.org/faq/faq.html#KDE%20Client0> – Zugriff am 4.8.2004.
- Kroupware.org: KDE Kolab-Benutzerhandbuch; 2004 in: http://kroupware.org/groupware_de-1.0.1-html/c38.html – Zugriff am 28.7.2004.
- Kuri, J.: Open-Source-Groupware Kolab ist fertig; in: <http://www.heise.de/newsticker/meldung/38907> – Zugriff am 9.5.2004.
- Landeshauptstadt München Direktorium: LiMux - Die IT-Evolution; 2004 in: <http://www.muenchen.de/Rathaus/referate/dir/limux/89256/> – Zugriff am 4.8.2004.
- Lévénéz, E.: Unix History; in: <http://www.levenez.com/unix/> – Zugriff am 25.8.2004.
- Maior, A. D.: Patent Issues Aren't the Only Cause for Munich's Linux Delay; in: http://www4.gartner.com/resources/122200/122264/patent_issues_a.pdf – Zugriff am 13.8.2004.
- MandrakeSoft: Want to download Mandrakelinux? 2004 in: <http://www.mandrakelinux.com/en/ftp.php3> – Zugriff am 25.7.2004.
- Mullet, D. und Mullet, K.: Managing IMAP; in: <http://www.oreilly.com/catalog/mimap/chapter/ch09.html#89986> – Zugriff am 26.7.2004.
- Myers, J.: Local Mail Transfer Protocol; in: <ftp://ftp.rfc-editor.org/in-notes/rfc2033.txt> – Zugriff am 1.8.2004.
- Myers, J.: Simple Authentication and Security Layer (SASL); in: <ftp://ftp.rfc-editor.org/in-notes/rfc2222.txt> – Zugriff am 04.07.2004.
- Myers, J. und Rose, M.: Post Office Protocol - Version 3; in: <ftp://ftp.rfc-editor.org/in-notes/rfc1939.txt> – Zugriff am 21.5.2004.
- Newman, C.: Using TLS with IMAP, POP3 and ACAP; in: <ftp://ftp.rfc-editor.org/in-notes/rfc2595.txt> – Zugriff am 21.5.2004.
- OpenLDAP Foundation: man slappasswd; 2000 in: http://gd.tuwien.ac.at/linuxcommand.org/man_pages/slappasswd8.html – Zugriff am 10.6.2004.
- OpenLDAP Foundation: openLDAP; 2004 in: <http://www.openldap.org/> – Zugriff am 11.5.2004.
- OpenLDAP Foundation: openLDAP 2.2 Administrator's Guide; 2004 in: <http://www.openldap.org/doc/admin22/dbtools.html#Creating%20a%20database%20off-line> – Zugriff am 26.5.2004.

- OpenLDAP Foundation: openLDAP 2.2 Administrators Guide: Replication with slurpd; 2004 in: <http://www.openldap.org/doc/admin22/replication.html> – Zugriff am 11.5.2004.
- OpenLDAP Foundation: openLDAP Faq-o-Matic: How do I backup my directory? 2004 in: <http://www.openldap.org/faq/data/cache/287.html> – Zugriff am 26.5.2004.
- phpCollab: phpCollab Features; 2004 in: <http://www.php-collab.com/documentation/features.htm> – Zugriff am 1.8.2004.
- phpCollab: phpCollab Home / News; 2004 in: <http://www.php-collab.com/> – Zugriff am 1.8.2004.
- phpCollab: phpCollab Installation Guide; 2004 in: <http://www.php-collab.com/documentation/install.htm> – Zugriff am 1.8.2004.
- phpGroupWare: phpGroupWare; 2004 in: <http://www.phpgroupware.org/> – Zugriff am 31.7.2004.
- phpGroupWare: phpGroupWare; 2004 in: <http://docs.phpgroupware.org/html/install/prerequisites.html> – Zugriff am 31.7.2004.
- Postel, J. und Reynolds, J.: File Transfer Protocol; in: <ftp://ftp.rfc-editor.org/in-notes/rfc959.txt> – Zugriff am 21.5.2004.
- Prochnow, S.: Problem mit Kolab + FreeBSD 4.9 + no worthy mechs found; in: <http://www.kolab.org/pipermail/kolab-users/2004-June/000515.html> – Zugriff am 21.6.2004.
- Radley Network Technologies CC: Toltec Groupware Connector; 2004 in: <http://www.toltec.co.za/> – Zugriff am 4.8.2004.
- Red Hat, Inc.: Red Hat Cluster Suite; 2004 in: <http://www.redhat.com/software/rha/cluster/> – Zugriff am 24.8.2004.
- Reibold, H.: eGroupWare 1.0 kompakt; in: <http://www.bomots.de/egroupware/index.htm> – Zugriff am 31.7.2004.
- Reibold, H.: eGroupWare 1.0 kompakt; in: <http://www.bomots.de/egroupware/kap11.htm> – Zugriff am 31.7.2004.
- Reiter, B.: Proko2 is Good News Towards Kolab2; in: <http://www.kolab.org/pipermail/kolab-users/2004-April/000092.html> – Zugriff am 9.8.2004.

- Rescorla, E.: HTTP Over TLS; in: <ftp://ftp.rfc-editor.org/in-notes/rfc2818.txt> – Zugriff am 21.5.2004.
- RPM Community: RPM HOWTO; 1999 in: <http://www.rpm.org/RPM-HOWTO/#INTRO> – Zugriff am 10.7.2004.
- Soreon Research: Soreon Research; 2004 in: <http://www.soreon.de/site1/> – Zugriff am 2.8.2004.
- Stoermer, M.: perl, sasl or cyrus problem? in: <http://www.kolab.org/pipermail/kolab-users/2004-June/000525.html> – Zugriff am 21.6.2004.
- Stoermer, M.: SOLVED: Y Error: Unable to authenticate with Cyrus admin interface, Error = “; in: <http://kolab.org/pipermail/kolab-users/2004-June/000546.html> – Zugriff am 27.6.2004.
- SYSTEMS 2004: Einsparungen bis zu 25 % mit Microsoft-Alternativen; 2004 in: http://www.systems-world.de/id/8329/CMEntries_ID/29886 – Zugriff am 2.8.2004.
- The FreeBSD Project: The BSD Daemon; 2004 in: <http://www.freebsd.org/copyright/daemon.html> – Zugriff am 5.8.2004.
- The Horde Project: Horde Administrator’s FAQ; 2004 in: <http://www.horde.org/faq/admin/general/index.php#g12> – Zugriff am 4.8.2004.
- The Horde Project: The Horde Project; 2004 in: <http://www.horde.org/about.php> – Zugriff am 31.5.2004.
- The Horde Project: Horde User’s FAQ; 2004 in: <http://www.horde.org/faq/user/general/index.php#g3> – Zugriff am 4.8.2004.
- The Mozilla Organization: SSL/TLS; 2002 in: <http://www.mozilla.org/projects/security/pki/nss/ssl/> – Zugriff am 9.8.2004.
- The OpenPKG Project: Security; 2003 in: <http://www.openpkg.org/security.html> – Zugriff am 10.7.2004.
- The OpenPKG Project: openPKG Cross Platform Unix Software Packaging; 2004 in: <http://www.openpkg.org/> – Zugriff am 11.5.2004.
- The Radicati Group, Inc.: European MS Exchange Outlook Penetration and Forecast, 2004-2008; 2004 in: <http://www.radicati.com/reports/single.shtml> – Zugriff am 7.8.2004.

- The Radicati Group, Inc.: IBM Lotus Messaging Software, Market Analysis, 2004-2008; 2004 in: <http://www.radicati.com/reports/single.shtml> – Zugriff am 7.8.2004.
- theKompany.com: aethera: PIM, PDR, Messaging and Groupware: Introduction; 2004 in: <http://www.thekompany.com/projects/aethera/> – Zugriff am 28.7.2004.
- theKompany.com: aethera: PIM, PDR, Messaging and Groupware: Overview; 2004 in: <http://www.thekompany.com/projects/aethera/overview.php3> – Zugriff am 28.7.2004.
- theKompany.com: aethera: Screenshots; 2004 in: http://www.thekompany.com/projects/aethera/images/aethera_1.png – Zugriff am 4.8.2004.
- Ultra Monkey Project: High Availability: Single Virtual Service; 2004 in: <http://www.ultramonkey.org/2.0.1/topologies/ha-eg.html> – Zugriff am 29.6.2004.
- Ultra Monkey Project: Installation Notes: Ultra Monkey on Red Hat Enterprise Linux 3.0; 2004 in: <http://www.ultramonkey.org/2.0.1/installation-rh.el.3.0.ws.html> – Zugriff am 29.6.2004.
- Ultra Monkey Project: ultra Monkey; 2004 in: <http://www.ultramonkey.org/> – Zugriff am 29.6.2004.
- Ultra Monkey Project: ultra Monkey; 2004 in: <http://www.ultramonkey.org/download/2.0.1/rh.el.3.0/RPMS/> – Zugriff am 29.6.2004.
- University of Washington: Message Access Paradigms and Protocols; 1995 in: <ftp://ftp.cac.washington.edu/imap/imap.vs.pop> – Zugriff am 14.7.2004.
- Wahl, M., Howes, T. und Kille, S.: Lightweight Directory Access Protocol (v3); in: <ftp://ftp.rfc-editor.org/in-notes/rfc2251.txt> – Zugriff am 21.5.2004.
- Walzebuck, F.: [Kroupware] kolab on SuSE 8.1, Problems (Bugreport); in: <https://mail.kde.org/pipermail/kroupware/2003-March/001282.html> – Zugriff am 21.6.2004.
- Wikipedia Project: Hypertext Transfer Protocol; 2004 in: <http://de.wikipedia.org/wiki/HTTP> – Zugriff am 14.7.2004.
- Wikipedia Project: Internet Message Access Protocol; 2004 in: <http://de.wikipedia.org/wiki/IMAP> – Zugriff am 14.7.2004.

- Wikipedia Project: Local Mail Transfer Protocol; 2004 in: <http://en.wikipedia.org/wiki/LMTP> – Zugriff am 1.8.2004.
- Wikipedia Project: open Source; 2004 in: http://de.wikipedia.org/wiki/Open_Source – Zugriff am 18.8.2004.
- Wikipedia Project: POP3; 2004 in: <http://de.wikipedia.org/wiki/POP3> – Zugriff am 14.7.2004.
- Wilzopolski, A.: Zentralanbindung; in: <http://www.heise.de/ix/artikel/1999/06/137/> – Zugriff am 01.6.2004.
- Wolowicz, D. E.: Das Projekt LiMux stellt sich vor; in: http://www.muenchen.de/vip8/prod2/mde/_de/rubriken/Rathaus/bb_dir/limux/publikationen/aktionswoche.pdf – Zugriff am 7.8.2004.
- Zen for Open Source: Brewing Facts Kolab; 2004 in: <ftp://ftp.zfos.org/brew/kolab/BIN/kolab-20040217-2.0.0/ix86-fedora1/README> – Zugriff am 25.7.2004.
- Zen for Open Source: Zen for Open Source; 2004 in: <http://www.zfos.org/> – Zugriff am 15.5.2004.
- Zen for Open Source: Zen for Open Source; 2004 in: <ftp://ftp.zfos.org/brew/kolab/BIN/kolab-20040217-2.0.0/ix86-fedora1/> – Zugriff am 15.5.2004.
- Zen for Open Source: Zen for Open Source; 2004 in: <ftp://ftp.zfos.org/brew/kolab/BIN/kolab-20040217-2.0.0/ix86-fedora1/README> – Zugriff am 15.5.2004.

Ehrenwörtliche Erklärung

Hiermit versichere ich, dass die vorliegende Arbeit von mir selbständig und ohne unerlaubte Hilfe angefertigt worden ist, insbesondere, dass ich alle Stellen, die wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen sind, durch Zitate als solche kenntlich gemacht habe. Ferner erkläre ich mich damit einverstanden, dass die Arbeit der Öffentlichkeit zugänglich gemacht wird.

Magnus Stoermer

Düsseldorf, den 7. Oktober 2004