5.

6.

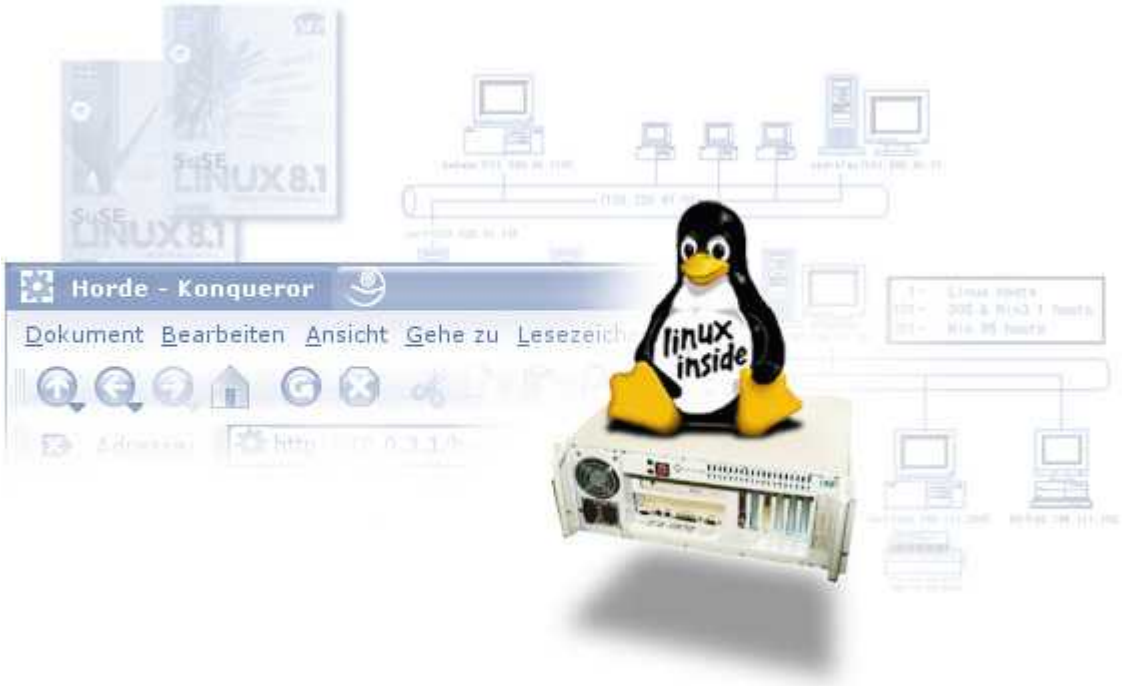
Firma Abele Informatik
Imbergstr. 29
87452 Krugzell

David Mayr
Sallerstr. 5
87435 Kempten

Dokumentation zur Projektarbeit

Fachinformatik/Systemintegration 2003

Installation und Integration eines Linux Kommunikations-Servers in ein heterogenes Netzwerk.



5.
6.

Inhalt / Gliederung

Hinweis: *viele der verwendeten Fachbegriffe und Abkürzungen finden Sie im Glossar erklärt.*

7.
8.

1. Projektbeschreibung

In ein bestehendes heterogenes LAN mit ca. 25 Clients und 4 Servern (MS-Windows NT/2000 und Novell-Netware) soll ein Linux-Kommunikations-Server integriert werden. Dieser soll neben Internet-Gateway über SDSL mit Firewall noch folgende Dienste für das gesamte Netzwerk anbieten:
HTTP-/FTP-Proxy, Web-Server mit PHP, DNS, SMTP-Server, IMAP-Server, MySQL und Webmail.
Der Server soll durch eine sichere Verbindung übers Internet wartbar sein. Ausserdem soll eine tägliche Gesamtsicherung von sich selbst auf einem anderen Server abgelegt und mit Software-RAID1 gegen Datenverlust durch Festplattenschaden abgesichert werden.

2. Projektplanung

Zur Planung des Projektes wurde die nachfolgende „Ist-/Soll-Analyse" durchgeführt.

2.1 Ist-Analyse

Bei dem Kunden, der Firma „Haslach Blechbearbeitung GmbH", existiert ein, von der Firma Abele Informatik geplantes, eingerichtetes und seit mehreren Jahren gewartetes Netzwerk. Dieses beinhaltet einen Hauptserver mit dem Betriebssystem Windows 2000 Server, einen älteren Novell-Netware Server, einen Windows NT Server und ca. 25 Arbeitsstationen mit Windows NT und Windows 2000. Bisher wurde die Internetanbindung des Kunden über einen Linux-Router mit veralteter Hardware, durch ISDN-Einwahl realisiert und eMails wurden an einigen wenigen Arbeitsplätzen direkt mit den eMail-Clients aus dem Internet abgeholt.
Da die Einwahl mit ISDN ins Internet durch den regelmässigen, zeitversetzten eMail-Abruf von mehreren Arbeitsplätzen recht kostenintensiv und ineffizient ist und auch die Geschwindigkeit der Daten- und eMail-Übertragung bei den aufkommenden Datenmengen nicht mehr schnell genug war, wurde die Firma Abele Informatik um Abhilfe gebeten.

2.2 Soll-Konzept

Seit kurzem bietet der regionale Telekommunikationsanbieter „AK-Schwaben" eine SDSL-Standleitung für den Standort des Kunden an, welche mit 256Kbit (Up- und Downstream) den Bandbreitenanforderungen unseres Kunden genügt. Da eine solche Dauer-Internetanbindung auch ein nicht zu vernachlässigendes Risiko durch Angriffe von „Hackern" aus dem Internet darstellt, sollte das gesamte Netzwerk durch eine Firewall in Form eines restriktiven Paketfilters geschützt werden. Ausserdem wurde, um die übertragene Datenmenge möglichst gering zu halten und die Geschwindikeit beim Surfen und Herunterladen von Dateien im Internet zu erhöhen, ein Proxyserver für HTTP- und FTP-Zugriffe verwendet.

Nachdem die Mitarbeiter des Kunden häufig nicht an Ihrem eigenen Arbeitsplatz-PC arbeiten, aber trotzdem ihre eMails lesen und beantworten müssen, war ein IMAP-Server, der die eMails regelmässig zentral vom Anbieter abholt, mit WebMail-Interface die geeignetste eMail-Lösung. Der IMAP-Server bietet zusätzlich die Möglichkeit, von jedem PC aus mit einem gängigem eMail-Client ohne das manuelle Kopieren von Mailboxdateien auf den selben zentralen eMail-Bestand zuzugreifen – auch im parallelen Einsatz zum WebMailer.

7.
8.

Aufgrund der Tatsache, dass recht viele PCs nach Aufbau des Servers angepasst werden mussten, und dabei jeweils mehrmals der Hostname bzw. die IP-Adresse des Servers eingegeben werden musste, wurde ein DNS-Server eingesetzt. Damit war es möglich sogenannte Aliase, also z. B. kürzere Hostnamen, zu verwenden um somit viel Schreibarbeit bei der Einrichtung der Clients zu sparen.

3. Projektumsetzung

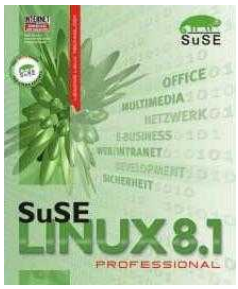
3.1 Installation des Servers

3.1.1 Aufbau der Hardware

Als Hardware für den Linux-Server kamen folgende Komponenten zum Einsatz:

Gehäuse: 19" Rack-Gehäuse
CPU: AMD Duron 1000 Mhz
RAM: 256 MB SDRAM
Graphikkarte: ATI Rage XL AGP
Festplatten: 2 x IBM IC35L040AVER07-0 (40 GB)
NIC: SiS900 10/100 Mbit/s (onboard) und Intel 82544EI 1000 Mbit/s

Der Aufbau der Hardware erfolgte im Hardware-Labor der Firma Abele Informatik. Anschliessend wurden grundlegende Prüfungen wie ein ausgiebiger Speichertest (mit dem Programm „memtest86") und ein Dauer-Belastungstest durchgeführt.



3.1.2 Grundinstallation SuSE Linux

Als Betriebssystem kam SuSE Linux in der Version 8.1 zum Einsatz. Die Installation wurde in unserem Hause durchgeführt. Dabei wurden die beiden Festplatten wie folgt partitioniert:

1. Festplatte:

Gerät	*Dateisystem*	*Grösse*	*Mountpunkt*	*Partitionstyp*
/dev/hda1	reiserfs	72.261 KB	/boot	Linux (83)
/dev/hda2	Raid (reiserfs)	5.245.222 KB	/ (teil v. /dev/md0)	Linux raid autodetect (fd)
/dev/hda3	(swap)	265.072 KB	(swap)	Linux swap (82)
/dev/hda4	Raid (reiserfs)	34.620.075 KB	/DATEN (-> /dev/md1)	Linux raid autodetect (fd)

2. Festplatte:

Gerät	*Dateisystem*	*Grösse*	*Mountpunkt*	*Partitionstyp*
/dev/hdc1	reiserfs	65.992 KB	/boot.2nd	Linux (83)
/dev/hdc2	Raid (reiserfs)	5.243.112 KB	/ (teil v. /dev/md0)	Linux raid autodetect (fd)
/dev/hdc3	(swap)	262.584 KB	(swap)	Linux swap (82)
/dev/hdc4	Raid (reiserfs)	34.637.400 KB	/DATEN (-> /dev/md1)	Linux raid autodetect (fd)

Bei der Partitionierung mittels YaST, dem Installations- und Konfigurationstool von SuSE Linux, wurde ein

7.
8.

Software-RAID Level 1 eingerichtet. Dadurch werden alle Daten bei jedem Schreibzugriff auf beide Festplatten redundant gespeichert. Im Folgenden ist die Zuordnung der physikalischen Partitionen zu den logischen RAID1-Arrays aufgelistet:

```
Array 1 =    /dev/md0:    raid-disk 0 = /dev/hda2
                          raid-disk 1 = /dev/hdc2
Array 2 =    /dev/md1:    raid-disk 0 = /dev/hda4
                          raid-disk 1 = /dev/hdc4
```

Bei der Software-Auswahl wurde die Grundauswahl „Minimales graphisches System" verwendet, mit den Standard-Packetselektionen "LAMP, „Netzwerk" und „KDE-Desktop"erweitert und mit den folgenden Einzelpacketauswahlen ergänzt:

`mc`	- ein Konsolenbasierter Dateimanager mit Editor
`cyrus-imapd`	- der Cyrus IMAP-Server
`phpMyAdmin`	- Webbasierte Administrationsoberfläche für den MySQL-Server
`amavis-postfix`	- ein eMail-Virenscanner für den Postfix SMTP-Server

Nach dem nun folgenden ca. 15-minütigen Kopiervorgang wurden die installierten Netzwerkkarten automatisch erkannt und vorerst mit DHCP konfiguriert, womit der Server schon vollen Internetzugang in unserem Hardware-Labor hatte und das Online-Update ausgeführt werden konnte.

3.2 Konfiguration der Serverdienste

In den nun folgenden Punkten werden die einzelnen, zur Verwirklichung des Soll-Konzeptes nötigen, Serverdienste eingerichtet. Wenn im folgenden Konfigurationsdateien bearbeitet wurden, geschah das als Benutzer „root" zumeist mit dem Texteditor „`mcedit`".

3.2.1 Konfiguration des HTTP/FTP-Proxy Squid

Um den Squid-Proxy zu konfigurieren, wurde die Datei `/etc/squid/squid.conf` bearbeitet. Da die Standardeinstellung für den Zwischenspeicher (Cache) bei nur 100 MB liegt, wurde dieser Wert auf 512 MB erhöht. Dazu wurde die mit „`#cache_dir`" beginnende Zeile gesucht und zu folgender Zeile abgeändert:

```
cache_dir  ufs  /var/squid/cache  512  16  256
```

Als nächstes wurde eine sogenannte Access-Control-List eingerichtet, um vor unerlaubter Verwendung des Proxys aus dem Internet zu schützen. Im „ACL"-Abschnitt der Squid-Konfigurationsdatei wurde dafür folgende Zeile eingefügt:

```
acl  localnet  src  192.168.102.0/255.255.255.0
```

Damit Squid weiss, was er der ACL „localnet" erlauben darf, wurde im darunterliegenden Abschnitt folgende Zeilen eingefügt:

```
http_access  allow  localnet
http_access  deny   all
```

Da diese Zeilen von Squid von oben nach unten abgearbeitet werden, und er die erste zutreffende Regel anwendet, kann der Proxy nur noch von Clients aus dem Netzwerk 192.168.102.0/255.255.255.0 verwendet werden.

Um Squid anschliessend zu starten wurde der Befehl „`rcsquid start`" ausgeführt. Um später gemachte

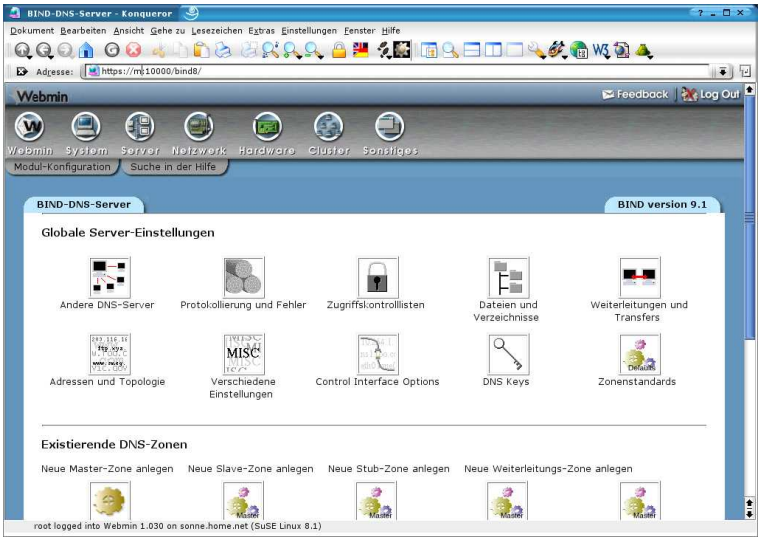
7.
8.

Änderungen dieser Konfiguration anzuwenden, muss Squid mit dem Befehl „`rcsquid reload`“ angewiesen werden seine Konfiguration neu zu laden. Damit der Proxy auch beim nächsten Bootvorgang automatisch startet, wurde mit dem Befehl „`yast runlevel`“ Squid zu den Runleveln 3 und 5 hinzugefügt.

3.2.2 Konfiguration des DNS-Servers BIND

Um eine netzwerkinterne Namensauflösung und einige Aliase zur kürzeren und damit schnelleren Schreibweise von Hostnamen zu ermöglichen wurde der DNS-Server BIND Version 9.1 konfiguriert und verwendet.

Da SuSE mit ihrer Linux-Distribution kein Konfigurationswerkzeug für den DNS-Server mitliefert, wurde das webbasierte universelle Konfigurations-werkzeug Webmin von http://www.webmin.com heruntergeladen und installiert.
Damit wurden dann zunächst die DNS-Server des ISP als Weiterleitung-DNS eingetragen, die BIND zur Namensauflösung von Hostnamen verwendet, die er selbst nicht kennt.
Anschliessend wurde eine Masterzone mit dem Namen der netzinternen Domain, sowie eine Reverse-Lookup Masterzone mit dem Namen „192.168.102“ angelegt.



Das webbasierte universelle Konfigurations-Tool Webmin im DNS-Modul.

Dann mussten noch die Zuordnungsdaten für Hostnamen/IP-Adressen in die eben angelegten Zonen eingetragen werden. Es wurden vorerst nur die Hostnamen und IP-Adressen der beim Kunden vorhandenen Server und ein Alias „m“ für den Linux-Server eingetragen.
Abschliessend musste noch der DNS-Server mit dem Befehl „`rcnamed start`“ gestartet werden. Bei nachträglichen Änderungen müssen die neuen Einstellung entweder durch klicken in Webmin auf „Änderungen zuweisen“, oder durch Ausführen des Befehls „`rcnamed reload`“ aktiviert werden. Damit der DNS-Server auch beim nächsten Bootvorgang automatisch startet, wurde mit dem Befehl „`yast runlevel`“ der Dienst „named“ zu den Runleveln 3 und 5 hinzugefügt.

3.2.3 Konfiguration des SMTP-Servers Postfix

7.
8.

Die Postfix-Grunkonfiguration wurde zuerst mit dem SuSE-Programm YaST erstellt und hinterher manuell angepasst. Zusätzlich wurde hier auch gleich das Programm Fetchmail zum eMail-Abruf externer POP-Server konfiguriert. Dazu wurde mit „`yast mail`" das interaktive Programm YaST im Mail-Konfigurationsmodus gestartet und folgende Einstellungen(*) vergeben:

Ausgehender Mailserver = smtp.puretec.de
Ausgehende Details:
Domain für den Header 'Von' = kundendomain.de
DomainNamen für lokale Mailzustellung = kundendomain.de, localdomain.net, linuxserver, localhost, localhost.kundendomain.de, localhost.localdomain.net, linuxserver.localdomain.net
Mail von root weiterleiten an = mayr
Eingehende Details -> Herunterladen
-> Hier wurden die abzurufenden externen POP3-Konten eingetragen.

Da unser Kunde bei seinem ISP ein sogenanntes Multidrop- bzw. Catchall-Konto hat, in dem alle eMails an seine Domain „`kundendomain.de`" landen, muss noch in der eben von YaST erstellten Datei `/etc/fetchmailrc` der Eintrag für den lokalen Benutzer auf „`root *`" umgestellt werden. Die Datei `/etc/fetchmailrc` sieht jetzt, mit Beispielwerten, wie folgt aus:

```
poll pop.puretec.de aka kundendomain.de proto POP3 : user "popuser" pass "geheim" is "root *" ;
```

Dadurch werden die abgeholten eMails automatisch an das, dem vorderen Teil der eMailadresse (vor dem „@"-Zeichen) entsprechende, lokale eMail-Postfach abgelegt. Das heisst, wenn später ein neuer eMail-Benutzer eingerichtet werden soll, muss dieser nur lokal, und nicht auch beim ISP eingerichtet werden.

Um eMails regelmässig abholen zu lassen, ist noch ein Eintrag im Task-Scheduler CRON nötig. Zuvor sollte aber die bisherige Fetchmail-Konfiguration mit dem Befehl „`fetchmail --fetchmailrc /etc/fetchmailrc -v -v`" getestet werden. Fetchmail gibt dann genaue Meldungen über Fortschritt und Erfolg auf der Konsole aus. Für den Task-Scheduler CRON wird einfach an die Datei /etc/crontab die folgende Zeile angehängt:

```
*/2 * * * *  root  fetchmail --fetchmailrc /etc/fetchmailrc --silent --syslog  >/dev/null
```

Anschliessend wird zum Laden der neuen CRON-Konfiguration der Befehl „`rccron reload`" eingeben. Mit diesem Eintrag werden ab sofort alle mit YaST zuvor konfigurierten POP-Konten alle zwei Minuten abgerufen und dem lokalen SMTP-Server Postfix zugestellt.

Standardmässig legt der SMTP-Server Postfix alle, für die lokale eMail-Domain eingegangenen, eMails auf dem Server unter dem Verzeichnis `/var/spool/mail` ab. Von dort aus werden normalerweise die eMails von Standard-Mailserverprogrammen, wie z.B. dem einfachen POP-Server "qpopper" abgeholt und an den Client weitergegeben.
Da in diesem Projekt aber der weit leistungsfähigere POP- und IMAP-Server Cyrus zum Einsatz kommt, und dieser die eingehenden eMails in einem anderen Verzeichnis und Format vom SMTP-Server erwartet, muss der SMTP-Server Postfix dafür eigens konfiguriert werden.

(*) Aus datenschutzrechtlichen Gründen wurden in dieser Dokumentation Beispielwerte verwendet.

Die Firma SuSE hat für diese Konfiguration dafür in ihrem Konfigurationsprogramm YaST leider keine Einstellungsmöglichkeit gegeben, deshalb müssen im folgenden einige Konfigurationsdateien "von Hand" bearbeitet

werden. Eine englische Anleitung hierfür ist auch in der Datei `/usr/share/doc/packages/cyrus-imapd/README.SuSE` nachzulesen. Zunächst muss sichergestellt werden, dass YaST die manuell bearbeiteten Konfigurationsdateien hinterher nicht mehr überschreibt. Dazu wird in der Datei `/etc/sysconfig/mail` die Variable `MAIL_CREATE_CONFIG` auf `"no"` gestellt. In der Postfix-Konfigurationsdatei `/etc/postfix/main.cf` muss der Wert für `"mailbox_transport"` auf `"lmtp:unix:public/lmtp"`, und der Wert von `"myhostname"` auf `"kundendomain.de"` gesetzt werden. Die beiden Zeilen sehen dann so aus:

```
mailbox_transport = lmtp:unix:public/lmtp
myhostname = kundendomain.de
```

Damit die gemachten Änderungen gleich aktiv werden, muss noch Postfix seine Konfigurationsdateien mit dem Befehl „`rcpostfix reload`" neu laden. Damit der SMTP-Server auch beim nächsten Bootvorgang automatisch startet, wurde mit dem Befehl „`yast runlevel`" Postfix zu den Runleveln 3 und 5 hinzugefügt.

3.2.4 Konfiguration des IMAP-Servers Cyrus

Damit der IMAP-Server Cyrus die eMails, die ihm von Postfix zugestellt werden, auch richtig in Empfang nimmt, muss in der Cyrus-Konfigurationsdatei `/etc/cyrus.conf` in dem Abschnitt "SERVICES" die Zeile

```
lmtp          cmd="lmtpd" listen="lmtp" prefork=0
```

und alle anderen Zeilen die mit `"lmtp"` beginnen durch die Zeile folgende Zeile ersetzt werden:

```
lmtpunix      cmd="lmtpd" listen="/var/spool/postfix/public/lmtp" prefork=1
```

Anschliessend muss für den System-Benutzer "cyrus", unter dessen Benutzerkennung der IMAP-Server Cyrus läuft, ein Passwort mit dem Kommando „`saslpasswd2 cyrus`" eingerichtet werden. Der Cyrus IMAP-Server benötigt zusätzlich noch das Programm „saslauthd", welches mit „`rcsaslauthd start`" gestartet, und mit „`yast runlevel`" für die Runlevel 3 und 5 zum automatischen Start beim Booten eingetragen wird. Ausserdem musste ab jetzt Cyrus mit dem Befehl „`rccyrus start`" gestartet sein, damit fortgefahren werden konnte.

Mithilfe des interaktiven Konsolen-Programmes "cyradm" werden anschliessend die einzelnen Mailboxen angelegt:

```
cyradm  --user cyrus  --server localhost
```

Bei Aufruf dieses Befehls wird das Passwort verlangt, welches zuvor vergeben wurde. Nun befindet man sich an der Eingabeaufforderung von "cyradm". Am Anfang der Zeile steht der Prompt "<localhost>". Dort kann man sich über die verfügbaren Befehle mit Eingabe von "help" informieren. Zum Anlegen einer Mailbox mit den gängigen Unterordnern folgen die Befehle für einen Beispielbenutzer:

```
cm 'user.beispielbenutzer'
cm 'user.beispielbenutzer.Papierkorb'
cm 'user.beispielbenutzer.Entwuerfe'
cm 'user.beispielbenutzer.Gesendete Nachrichten'
```

Wie aus der Hilfe mit "help" ersichtlich ist, ist "cm" die Kurzform von "createmailbox" und "lm" die Kurzform von "listmailbox". Der Befehl "lm" müsste jetzt folgende Ausgabe liefern:

```
user.beispielbenutzer (\HasChildren)
user.beispielbenutzer.Entwuerfe (\HasNoChildren)
user.beispielbenutzer.Gesendete Nachrichten (\HasNoChildren)
user.beispielbenutzer.Papierkorb (\HasNoChildren)
```

Mit dem Befehl "exit" kann "cyradm" wieder verlassen werden.

Jetzt müssen noch die Passwörter für die einzelnen eMail-Benutzer/-Mailboxen vergeben werden. Der Cyrus-

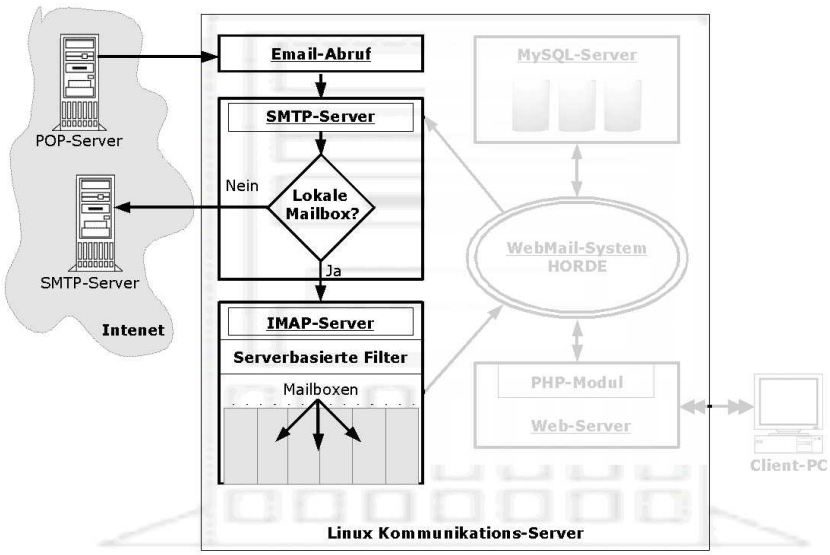
7.
8.

Server ist ein sogenannter "sealed-server", das heisst er arbeitet mit einer eigenen Benutzerverwaltung die nichts mit den normalen Linux-Benutzern zu tun hat. Deshalb müssen auch nicht zwingend Benutzerkonten mit z.B. YaST angelegt werden. Stattdessen wird einfach ein Passwort für eine Mailbox mit dem Befehl "saslpasswd2" angelegt:

```
saslpasswd2 -c beispielbenutzer
```

Der Benutzername muss, wie hier im Beispiel, mit dem Namen der zuvor mit "cyradm" angelegten Mailbox übereinstimmen. Damit der IMAP-Server auch beim nächsten Bootvorgang automatisch startet, wurde mit dem Befehl „`yast runlevel`" Cyrus zu den Runleveln 3 und 5 hinzugefügt.

Der technische Weg einer eMail soll in nebenstehender Graphik veranschaulicht werden.



3.2.5 Konfiguration des HTTP-Servers Apache mit PHP-Modul

Damit der WebServer Apache bei externem Zugriff vom Internet auch den Hostnamen verwendet mit dem er in der URL angesprochen wurde (und nicht mit seinem lokalen Hostnamen) muss in der Datei `/etc/httpd/httpd.conf` die Option "`UseCanonicalName`" auf "`Off`" gestellt werden. Ansonsten würde der Webmailer bei Zugriff aus dem Internet nicht funktionieren.

Um zu ermöglichen, dass der, in PHP geschriebene, Webmailer Horde, auf welchen ich später näher eingehen werde, auch Dateien, die grösser als 2 MB sind, per eMail-Anhang versenden kann, muss man in der Datei "`/etc/php.ini`" den Wert für "`upload_max_filesize`" auf z.B. "`10M`" stellen.

Ausserdem hat sich in der Testphase gezeigt, dass für grosse Anhänge auch mehr, als die standardmässig eingetellten 8MB, Arbeitsspeicher für PHP erlaubt werden müssen. Dazu muss in der gleichen Datei der Wert für "`memory_limit`" auf z.B. "`32M`" geändert werden. Damit waren in der Testphase eMail-Anhänge mit 10MB problemlos möglich.

Abschliessend musste noch der Webserver-Server mit dem Befehl „`rcapache start`" gestartet werden. Bei nachträglichen Änderungen müssen die neuen Einstellungen durch Ausführen des Befehls „`rcapache reload`" aktiviert werden. Damit der Webserver-Server auch beim nächsten Bootvorgang automatisch startet, wurde mit dem Befehl „`yast runlevel`" Apache zu den Runleveln 3 und 5 hinzugefügt.

3.2.6 Konfiguration des SQL-Servers MySQL

7.
8.

Nachdem der MySQL-Server bereits bei der Paketauswahl anfangs mitinstalliert wurde, muss er jetzt erstmal mit dem Befehl „rcmysql start“ getstartet werden. Daraufhin werden die Grund-Datenbanken initialisiert und man wird aufgefordert, ein Passwort für den Datenbank-Administrator "root" mit dem folgenden Befehl zu vergeben:

```
mysqladmin -u root password "geheim"
```

Um die MySQL-Datenbank auch vernünftig verwalten zu können, bietet sich das PHP-basierte Programm phpMyAdmin an. Dieses muss noch in der Datei /srv/www/htdocs/phpMyAdmin/config.inc.php angepasst werden. Es muss zum einen der Wert für "$cfg['Servers'][$i]['auth_type']" auf "http" gestellt werden, und zum anderen bei "$cfg['PmaAbsoluteUri']" der absolute URL unter dem phpMyAdmin erreichbar sein soll eingegeben werden - in diesem Fall „http://192.168.102.250/phpMyAdmin/“.

Bei nachträglichen Änderungen müssen die neuen Einstellung durch Ausführen des Befehls „rcmysql reload“ aktiviert werden. Damit der MySQL -Server auch beim nächsten Bootvorgang automatisch startet, wurde mit dem Befehl „yast runlevel“ MySQL zu den Runleveln 3 und 5 hinzugefügt.

3.2.7 Konfiguration des Webmailers Horde mit seinen Modulen

Als Webmailer wird das freie Projekt "Horde" verwendet. Es ist modular aufgebaut und in PHP geschrieben. Die Projekthomepage findet man unter http://www.horde.org. Es gibt das Grundmodul/Framework "Horde" und eine Reihe weiterer darauf aufbauender Module. Im folgenden sind die bei diesem Projekt eingesetzten Module mit Download-URL aufgelistet:

Grundmodul "Horde":	ftp://ftp.horde.org/pub/horde/tarballs/horde-2.1.tar.gz
WebMail "IMP":	ftp://ftp.horde.org/pub/imp/tarballs/imp-3.1.tar.gz
Notizblock "Mnemo":	ftp://ftp.horde.org/pub/mnemo/tarballs/mnemo-1.0.tar.gz
Aufgabenliste "Nag":	ftp://ftp.horde.org/pub/nag/tarballs/nag-1.0.tar.gz
Adressbuch "Turba":	ftp://ftp.horde.org/pub/turba/tarballs/turba-1.1.tar.gz
Kalender "Kronolith":	ftp://ftp.horde.org/pub/kronolith/tarballs/kronolith-1.0.tar.gz

Die Datei "horde-2.1.tar.gz" wird nach "/srv/www/htdocs/" in ein neues Verzeichnis "horde" entpackt. Alle weiteren Module werden in ein jeweils darunterliegendes Verzeichnis mit dem Namen des jeweiligen Moduls entpackt.

Da die in der SuSE-Distribution mit dem PHP-Interpretermodul für den Apache-Webserver gelieferte PEAR-Erweiterung für Horde nicht aktuell genug ist, muss eine aktualisierte Version unter

```
ftp://ftp.horde.org/pub/horde/tarballs/pear-4.1.0.tar.gz
```

heruntergeladen werden, und nach "/usr/share/php/" entpackt werden.

Da Horde und die Module ihre Einstellungen und teilweise ihre Daten in einer MySQL-Datenbank speichern sollen, werden die hierfür benötigten Tabellen mir den folgenden Befehlen angelegt:

7.
8.

```
mysql --user=root --password       </srv/www/htdocs/horde/scripts/db/mysql_create.sql
mysql --user=root --password horde </srv/www/htdocs/horde/mnemo/scripts/drivers/mnemo_memos.sql
mysql --user=root --password horde </srv/www/htdocs/horde/nag/scripts/drivers/nag_tasks.sql
mysql --user=root --password horde </srv/www/htdocs/horde/turba/scripts/drivers/turba.sql
mysql --user=root --password horde </srv/www/htdocs/horde/kronolith/scripts/drivers/kronolith.sql
```

Jedes Modul hat ein eigenes Konfigurations-Unterverzeichnis mit dem Namen "`config`", welche hier alle nochmal aufgelistet sind:

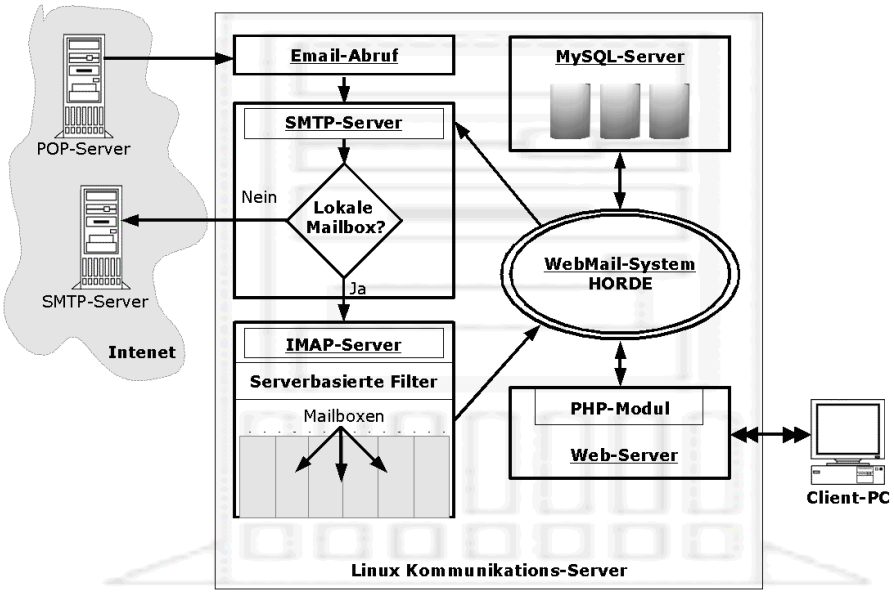
```
/srv/www/htdocs/horde/config/
/srv/www/htdocs/horde/imp/config/
/srv/www/htdocs/horde/mnemo/config/
/srv/www/htdocs/horde/nag/config/
/srv/www/htdocs/horde/turba/config/
/srv/www/htdocs/horde/kronolith/config/
```

In jedem dieser Verzeichnisse gibt es Vorlage-Konfigurationsdateien mit der Endung ".dist". Diese mussten alle einmalig zu Dateien ohne diese ".disk"-Endung kopiert werden. Das geschieht am einfachsten damit, dass man den folgenden Befehl in jedem der o.g. Verzeichnisse ausführt:

```
for foo in *.dist; do cp $foo `basename $foo .dist`; done
```

Anschliessend müssen die durch das Kopieren neu erstellten Dateien bearbeitet werden. Dabei müssen u.a. die MySQL-Zugangsdaten, Voreinstellungen der Module und Daten über den verwendeten IMAP-Server eingegeben werden. Da diese Konfigurationsdateien zum einen sehr umfangreich und zum anderen aber auch recht ausführlich mit Kommentaren und Beschreibungen versehen sind, verzichte ich an dieser Stelle auf eine Schritt-für-Schritt Anleitung.

Die nebenstehende Graphik soll das Zusammenspielen aller beim eMail-System betroffenen Komponenten darstellen.



3.3 Integration beim Kunden

7.
8.

3.3.1 Einbinden ins LAN

Beim Kunden wurde der Server in einen der drei 19"-Schränke eingebaut und per vorhandener USV mit Strom versorgt. In dem vorhandenen privaten Klasse-C IP-Netz 192.168.102.0/255.255.255.0 bekam der Linux-Server die IP-Adresse 192.168.102.250. Diese wurde mithilfe des Befehls „yast lan" für die Intel 82544EI 1000Mbit/s-Netzwerkkarte (`/dev/eth1`) eingetragen. Bei den Routing-Einstellungen im YaST LAN-Modul wurde noch das IP-Forwarding aktiviert, damit IP-Packete von der LAN-Netzwerkschnittstelle zur SDSL-Schnittstelle geroutet werden können.

3.3.2 Internetanbindung mit SDSL

Zur Anbindung an die 256Kbit-SDSL-Leitung beim Kunden war neben der physikalischen Kabelverbindung, die vom ISP mit einem speziellen Endgerät bereits fertig vorbereitet wurde, nur die Vergabe einer vom ISP vergebenen IP-Adresse und des Standardgatewayeintrags nötig. Diese Werte wurden mithilfe des Befehls `„yast lan"` für die SiS900 100Mbit/s-Netzwerkkarte (`/dev/eth0`) eingetragen.

3.3.3 Konfiguration der Firewall

Um den Server und das gesamte Firmennetzwerk vor Angriffen aus dem Internet zu schützen wurde mit Hilfe von YaST eine Firewall eingerichtet. Dazu wurde mit dem Befehl `„yast firewall"` das entspechende interaktive Modul gestartet und jeder Zugriff vom Internet ausser Anfragen an Port 80 (http) und 22 (ssh) verboten. Über den http-Port 80 ist der Webserver und damit das WebMail-System Horde erreichbar, über den ssh-Port 22 soll mit verschlüsselten ssh-Sitzungen eine sichere Fernwartung ermöglicht werden. Damit von den Clients auch andere Internetverbindungen als das mit dem Squid-Proxyserver ermöglichten „Internet-Surfen" genutzt werden können, wurde Masquerading für das gesamte Netzwerk eingeschaltet.

3.3.4 Netzwerk-Systemsicherung

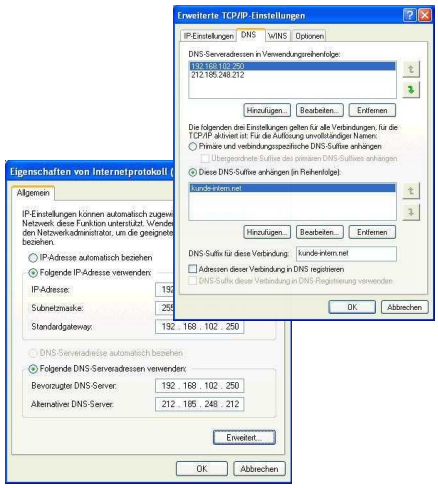
Um bei einem, durch das Software-RAID1 sehr unwahrscheinlichen, Totalausfall mit komplettem Datenverlust schnell wieder den kompletten Server lauffähig zu machen, wurde ein kleines Shell-Script geschrieben (`/usr/local/bin/mkbackup`), das mit Hilfe des Task-Schedulers Cron nächtlich den kompletten Server in einige komprimierte TAR-Archive sichert und vorerst lokal ablegt. Anschliessend werden die Sicherungs-Archivdateien auf eine dafür eingerichtete Datei-Freigabe des vorhandenen Windows 2000 Server mit Bandsicherungslaufwerk kopiert. Dieser wiederum sichert dann die Dateien bei seiner anschliessenden nächtlichen Sicherung mit den anderen Sicherungsjobs auf eine Bandkassette. Sollte man in die Verlegenheit kommen, wirklich den ganzen Server zurücksichern zu müssen, kann man einfach mit einem Linux-Rettungssystem von CD (z.B. mit der Knoppix-CD) booten, die evtl. neuen Festplatten wieder entsprechend von Hand partitionieren und die Sicherungsarchive übers Netzwerk kopieren und entpacken.

3.4 Konfiguration der Clients

Die hier beschriebenen Client-Einstellungen wurde an einem PC einem Kollegen gezeigt und erklärt, woraufhin er die

7.
8.

restlichen PCs auf die gleiche Weise konfigurierte.



3.4.1 Netzwerkeinstellungen

Da die Windows-Clients bereits im IP-Netzwerk konfiguriert waren, mussten nur folgende Einstellungen ergänzt bzw. angepasst werden:

Gateway = `192.168.102.250`

DNS-Server = `192.168.102.250`

DNS-Suffix = `localdomain.net`

bei Windows 2000 Clients zusätzlich:

Deaktivieren von: „Adressen dieser Verbindung in DNS registrieren"

„Diese DNS-Suffixe anhängen": `localdomain.net`

3.4.2 Browsereinstellungen

Damit die Internet-Browser der Clients (hier Internet Explorer) auch den Proxy-Server verwenden, musste „m" (oder die IP-Adresse des Linuxservers) als Proxyserver und der Squid-Port 3128 eingestellt werden. Als Startseite des Browsers wurde http://m eingestellt – das im DNS-Server hinterlegte kurze Alias für den Linuxserver.

4 Systemtest

Zum Abschluss wurden noch die folgenden Tests durchgeführt, um sicherzustellen, dass alles wie gewünscht funktioniert:

Anmelden am WebMailer HORDE und Versenden einiger interner eMails,

Versenden einiger externer Test-eMails (ins Internet).

Empfang von zuvor extern versendeter Nachrichten.

Portscan von einem PC aus dem Internet zum Testen der Firewall.

5 Abnahme und Einweisung

Die Abnahme des Servers erfolgte von Frau Haslach-Dann, der Junior-Geschäftsführerin des Kunden. Ihr wurde die erhöhte Geschwingikeit des Internetzuganges und des eMail-Versandes demonstriert, und die wichtigsten Funktionen des intuitiven WebMailers Horde gezeigt. Ihre Zufriedenheit bestätigte sie mit Ihrer Unterschrift auf dem, bei der Firma Abele Informatik üblichen, Servicebericht.

9.
10.

6 ANHANG

6.1 Zeitplan der Projektarbeit

	geplant	benötigt
Ist / Soll Analyse der Problemstellung, Projektkonzeption	2h	1,5h
Hardware-Aufbau des Servers und Grundinstallation SuSE Linux mit RAID-0, inklusive Systemtests	3h	2,5h
Aufbau des Servers beim Kunden (19"-Technik), Einbindung ins TCP/IP-LAN und Anbindung ans Internet per SDSL mit Firewall (Paketfilter)	3h	2h
Konfiguration des Serverdienstes HTTP-/FTP-Proxy, DNS-Server	1h	1,5h
Einrichten des Webservers mit PHP, SMTP-Server und IMAP Server-Dienst	4h	3h
Erstellen einer Sicherungslösung mit TAR und SMBclient	2h	2h
Installation und Konfiguration von MySQL und einer Webmail-Lösung	4h	3,5h
Anpassung/Umstellung der Email-Clients	2h	2h
Kurzeinweisung und Übergabe an den Kunden	2h	1h
Erstellen der Dokumentation	12h	16h
Summe	35h	35h

6.2 Selbständigkeitserklärung

Ich versichere, dass ich das Projekt und die dazugehörige Dokumentation selbständig und ohne fremde Hilfe angefertigt, alle Stellen, die wörtlich oder annähernd wörtlich aus Veröffentlichungen entnommen, als solche kenntlich gemacht habe. Die Arbeit hat in dieser Form keiner anderen Prüfungsinstitution vorgelegen.

_____ _____

Ort, Datum Unterschrift des Prüfungsteilnehmers

6.3 Kurzhilfe zur Mailverwaltung

Mailboxen verwalten (interaktiv; hilfe mit help): `cyradm --user cyrus localhost`

Mailboxen auflisten: `lm`

Mailbox anlegen: `cm user.beispielmailbox`

Mailbox löschen: `dm user.beispielmailbox`

Mail-Benutzer/-Passwörter verwalten

Mail-Benutzer anzeigen: `sasldblistusers2`

Mail-Passwort/-Benutzer anlegen: `saslpasswd2 -c USERNAME`

Mail-Passwort/-Benutzer loeschen: `saslpasswd2 -d USERNAME`

Mail-Passwort/-Benutzer aendern: `saslpasswd2 USERNAME`

Aliases und Verteilerlisten

Aliases und Verteilerlisten verwalten: `mcedit /etc/newaliases ; newaliases`

Logdateien

Logdateien beobachten: `tail -f -n 50 /var/log/messages /var/log/mail`

Mail-Warteschlange anzeigen

Warteschlange anzeigen: `mailq`

6.4 Glossar

ACL: Access Control List – Methode um Zugriffsrechte möglichst flexibel gestalten zu können.

Aliase: im Zusammenhang mit eMail werden diese zum Umschreiben von Empfängeradressen im **SMTP**-Server verwendet. Dadurch kann ein und dieselbe Mailbox zwei eMail-Adressen haben, oder eMails an eine Adresse an viele Adressaten weiterverteilt werden.

BIND: Berkeley Internet Name Daemon – **DNS**-Implementation der Universität von Berkeley.

Catchall: entspricht **Multidrop**

CPU: Central Processing Unit – Prozessor, und damit Herzstück eines PCs.

DHCP: Dynamic Host Configuration Protocol – Protokoll, mit dem Netzwerk-Clients sich die eigene Netzwerkkonfiguration (u.a. IP-Adresse, Gateway,**DNS**,...) von einem DHCP-Server per Rundruf im Netzwerk holen.

DNS: Domain Name Service – Internet-Dienst, der mithilfe einer dezentralen Datenbank Hostnamen zu IP-Adressen (und umgekehrt) übersetzt.

Firewall: meist ein als Packetfilter realisierter Schutz von Angriffen aus nicht vertrauenswürdigen Netzwerken.

FTP: File Transfer Protocol – Protokoll zur Übermittlung von Dateien über Netzwerke, meist übers Internet.

HTML: Hyper Text Markup Language - Seitenbeschreibungssprache für Internetseiten.

HTTP: Hyper Text Transfer Protokoll - Protokoll zur Übermittlung von Webseiten im **HTML**-Format und

anderen Daten.

IMAP: Abk. für „Interactive Mail Access Protokoll" - Protokoll zum Verwalten, Lesen und Archivieren von Zentralen Mailboxen/eMail-Beständen.

ISP: Abk. für „Internet Service Provider", Anbieter von u.a. Internetzugang, eMail-Dienste, ..

KDE: K Desktop Enwironment – fortgeschrittene OpenSource-Desktopumgebung und Windowmanager.

Knoppix: Freie Linux-Distribution, welche komplett von CD läuft und auf beinahe jeder PC-Harware ohne manuelle Konfiguration direkt nach dem ersten Start einsatzbereit ist.

LAMP: Abk. für die Kombination von Linux, dem Apache-Webserver, dem **MySQL**-Server und **PHP**

LAN: Local Area Network – auf Gebäude räumlich begrenztes Netzwerk.

Masterzone : sh. **Zone**

Masquerading: entspricht **NAT**

Multidrop: Beim **ISP** eingerichtete **POP**-Mailbox, aus der die eMails an mehrere Empfängeradressen abgeholt werden können.

MySQL: weit verbreitete OpenSource-Implementation eines SQL-Servers.

NAT: Network Address Translation – Verfahren zum Verbergen mehrerer Hosts hinter einem Router mit nur einer öffentlichen IP-Adresse. Dabei merkt sich der Router bei einem ausgehenden Packet die IP/Port-Kombination (Socket) des interenen Hosts, schreibt Absenderport/-IP um und macht diese Umschreibung beim Antwortpacket zum interenen Host rückgänig.

NIC: Network Interface Card – Netzwerk-Steckkarte.

PEAR: PHP Extension and Application Repository – Erweiterungen zu **PHP**

PHP: Pre- Homepage Processor – Programmiersprache die von einem Interpreter (meist als Webserver-Modul) ausgeführt wird und mit Hilfe eines Webserver HTML-Daten an einen Browser sendet bzw. von ihm empfängt.

POP: Post Office Protocol – einfaches Protokoll zum Abrufen von eMails von Mail(box)-Servern.

Proxy: eng. „Stellvertreter" - empfängt Netzwerkanfragen eines bestimmten Protokolls von einem Clients, führt diese Anfragen an andere Server selbst aus und liefert die Antwort an den Client zurück. Im Falle eines **HTTP**-Proxy kann dieser z.B. auch angefragte Internetseiten Zwischenspeichern und Protokollieren.

RAID: Redundant Array of Inexpensive Disks – Verbund mehrerer Datenträger zur Redundanten, und damit sichereren Speicherung von Daten.

RAM: Random Access Memory – Arbeitsspeicher eines PC.

ReiserFS: Hochentwickeltes OpenSource Linux-/Unix-Dateisystemformat mit Journaling-Funktionen.

Reverse-Lookup: im Zusammenhang mit **DNS** werden beim Reverse-Lookup IP-Adressen zu Hostnamen ausfelöst/übersetzt.

SASL: Simple Authentication and Security Layer.

SDSL: Symmetric Digital Subscriber Line - Datenübertragungsstandard für breitbandige Internetzugänge mit synchroner Up- und Downstreamgeschwindigkeit.

SMTP: Simple Mail Transfer Protocol – Standard-Protokoll, das zum Versenden und Weiterleitenvon eMails im Internet verwendet wird.

Software-RAID: Implementation einer RAID-Steuerung in den Betriebssystemkern – im Gegensatz zu Hardware-RAID, das meist in die Datenträger-Controller Chips integriert ist.

9.
10.

SSH: Secure Shell – sicheres (verschlüsseltes) Fern-loginprogramm mit weitreichenden Möglichkeiten zur sicheren Fernwartung von vorwiegend UNIX-/LINUX-Hosts.

Swap: Auslagerungs-Speicher. Wird unter Linux auf eine eigene Partition gespeichert um den logischen Arbeitsspeicher zu erweitern.

URL: Uniform Ressource Locator – einheitliche, universelle Schreibweise von Netzwerkressourcen. Im Falle einer Internetadresse wäre zum Beisiel `http://www.davey.de` die URL meiner Homepage oder `ftp://ftp.kde.org` die URL des **FTP**-Servers vom KDE-Projekt.

WebMail: ein komplett per Browser bedienbarer eMail-Client, der deshalb u. a. keine standortspezifische Konfiguration zur Verwendung benötigt.

Webserver: Stellt Daten über das **HTTP**-Protokoll im Netzwerk zur Verfügung.

Zone: Durch Zonen werden im Zusammenhang mit **DNS** Hierarchie- und Verwaltungs-einheiten/-bereiche organisiert.

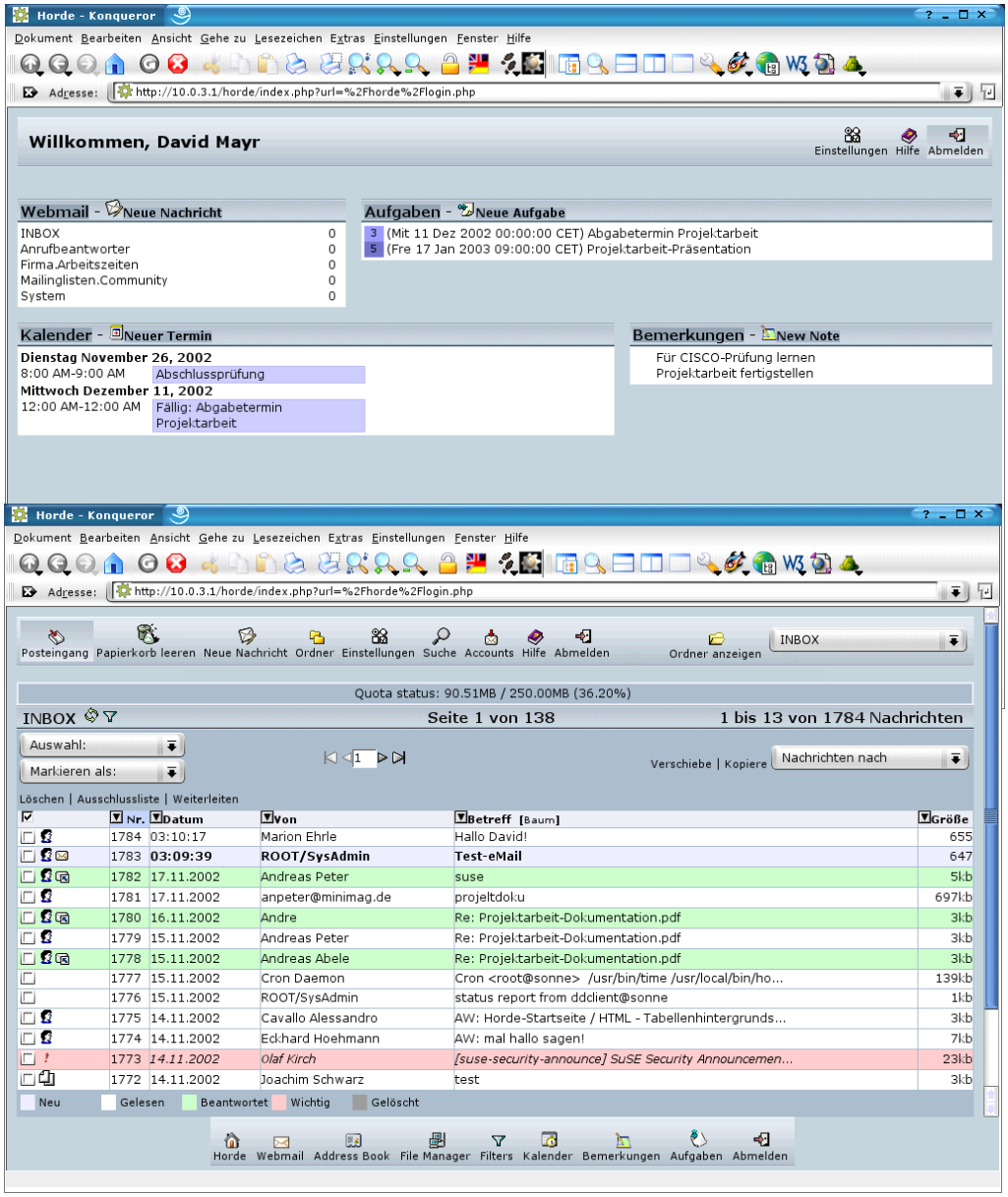
6.5 Quellenangaben

Homepage der Firma „SuSE AG“:	http://www.suse.de
Homepage des Linux-Kernels:	http://www.kernel.org
Homepage des Cyrus IMAP Servers:	http://asg.web.cmu.edu/cyrus/imapd
Homepage des SMTP-Servers Postfix:	http://www.postfix.org
Homepage des POP-/IMAP-Clients Fetchmail:	http://www.tuxedo.org/~esr/fetchmail
Homepage des DNS-Servers BIND:	http://www.isc.org/products/BIND
Homepage des HTTP-/FTP-Proxy Squid:	http://www.squid-cache.org
Homepage des Web-Servers Apache:	http://www.apache.org
Homepage der Programmiersprache PHP:	http://www.php.net
Homepage des WebMailers Horde/IMP:	http://www.horde.org

Man-Pages der jeweiligen Programme/Server (Aufruf mit „`man programmname`“)
Dokumentations-Verzeichnis unter `/usr/share/doc/packages` des Servers

6.6 Screenshots / Bilder

Die Willkommenseite von Horde mit einer Übersicht über die wichtigsten Modul-Daten.

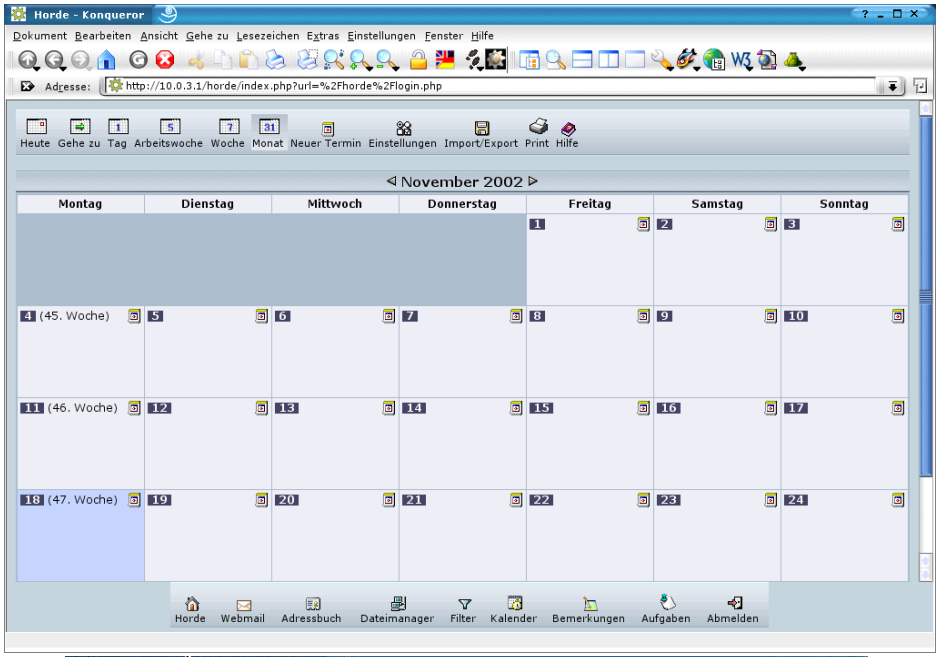


Das WebMail-Modul „IMP" von Horde in der Nachrichten-übersicht.

9.

10.

Das Kalendermodul von Horde in der Monatsübersicht.



Der Dialog zum Erstellen einer neuen eMail mit IMP, dem WebMail-Modul von Horde.