

Erweiterte Administration des Cyrus Mail-Dienstes

Thema:	Administration des Mail-Dienstes Cyrus mit den Werkzeugen cyradm, cyrreconstruct und cyrdeliver
Datum:	31. März 2009
Seitenzahl:	11
Versionsnummer:	2972
Autoren:	Univention GmbH feedback@univention.de

Inhaltsverzeichnis

1	Einleitung	3
2	Verwaltung von Postfächern mit cyradm	3
2.1	Arbeiten mit Postfächern	4
2.2	Access Control Lists (ACLs)	6
2.3	Mail-Quota	8
2.4	Übertragung von Postfächern und globalen Mail-Ordnern auf andere Mail-Server	8
3	Sicherung und Wiederherstellung von Postfächern	8
4	Erneute Zustellung von E-Mails	10

1 Einleitung

Cyrus ist das in UCS verwendete Mail-System. Die Administration des IMAP-Server-Systems erfolgt über das UCS-Managementsystem. Postfächer von Benutzern und globale Mail-Ordner werden in Univention Directory Manager verwaltet und die lokale Konfiguration des Mail-Systems über Univention Configuration Registry-Variablen angepasst. Einige administrative Aufgaben lassen sich allerdings nur auf der Kommandozeile erledigen.

Die Verwaltung der Postfächer von Benutzern und globalen Mail-Ordnern erfolgt über das Kommandozeilen-Werkzeug `cyradm` (Abschnitt 2). Mit `cyradm` lassen sich Postfächer editieren, Zugriffsrechte von Benutzern auf Postfächer und Ordner ändern, Postfächer löschen, Quotas einstellen und komplette Postfächer auf andere Server verschieben.

Nur in Ausnahmefällen sollte es erforderlich sein, mit `cyradm` manuelle Änderungen an den Postfächern von Benutzern oder an globalen Mail-Ordnern vorzunehmen. Die meisten in diesem Dokument beschriebenen Einstellungen – mit Ausnahme des Löschens und des Übertragens von Postfächern – können unmittelbar im Mail-Client eines Benutzers vorgenommen werden oder erfolgen automatisch über das UCS Managementsystem.

Hat ein Benutzer versehentlich E-Mails aus seinem Postfach gelöscht, müssen diese häufig aus einem Backup wiederhergestellt werden. Mit dem Cyrus Mail-Dienst wird das Kommandozeilenwerkzeug `cyrrconstruct` (Abschnitt 3) ausgeliefert, mit dem die bei der Wiederherstellung erforderliche Aktualisierung der internen Cyrus-Datenbanken vorgenommen wird.

In manchen Situationen kann es erforderlich sein, E-Mails erneut zuzustellen, die von anderen Programmen wie Anti-Viren- oder Anti-Spam-Software isoliert wurden. Für diesen Zweck kann das Programm `cyrdeliver` verwendet werden (Abschnitt 4).

2 Verwaltung von Postfächern mit `cyradm`

`cyradm` kann sowohl von Benutzern mit Systemverwaltungsrechten wie **root** als auch von Benutzern ohne besondere Berechtigungen aufgerufen werden. Normale Benutzer erhalten lediglich Zugriff auf ihre eigenen Postfächer und dürfen nur Rechte ändern, die vorher von einem privilegierten Benutzer freigegeben worden ist. Benutzer mit Systemverwaltungsrechten können über `cyradm` auf alle Postfächer und globale Mail-Ordner zugreifen.

Nach dem Aufruf von `cyradm` auf der Kommandozeile wird eine Sitzung gestartet, in der Befehle eingegeben werden können. `cyradm` sendet die eingegebenen Befehle über das IMAP-Protokoll an den Mail-Server. Das bedeutet, dass beim Aufruf von `cyradm` der Name des Mail-Servers angegeben werden muss, und dass der Mail-Dienst erreichbar sein muss.

`cyradm` verwendet standardmäßig den Namen des angemeldeten Benutzers, um auf den Mail-Server zuzugreifen. Andere Benutzernamen können mit der Option `-u` gewählt werden. Gültige Namen sind **root** und **cyrus** als privilegierte Benutzer (nur gültig in Verbindung mit dem Server-Namen **localhost**) und alle E-Mail-Adressen. Bei Aufruf von `cyradm`

muss das jeweilige Passwort zu dem Benutzernamen oder der E-Mail Adresse eingegeben werden. Nach erfolgreicher Anmeldung erhält man einen Eingabeprompt, an dem die in den folgenden Abschnitten beschriebenen Befehle eingegeben werden können. Durch Eingabe des Fragezeichens oder des Befehls help können alle gültigen Befehle angezeigt werden:

```
testuser@mailserver2:~\$ cyradm -u testuser@firma.de mailserver2.firma.de
IMAP Password:
mailserver2.firma.de> quit
testuser@mailserver2:~\$ cyradm -u root localhost
IMAP Password:
localhost> ?
authenticate, login, auth authenticate to server
chdir, cd change current directory
createmailbox, create, cm create mailbox
deleteaclmailbox, deleteacl, dam remove ACLs from mailbox
deletemailbox, delete, dm delete mailbox
disconnect, disc disconnect from current server
exit, quit exit cyradm
help, ? show commands
info display mailbox/server metadata
listacl, lam, listaclmailbox list ACLs on mailbox
listmailbox, lm list mailboxes
listquota, lq list quotas on specified root
listquotaroot, lqr, lqm show quota roots and quotas for mailbox
mboxcfg, mboxconfig configure mailbox
reconstruct reconstruct mailbox (if supported)
renamemailbox, rename, renm rename (and optionally relocate) mailbox
server, servername, connect show current server or connect to server
setaclmailbox, sam, setacl set ACLs on mailbox
setinfo set server metadata
setquota, sq set quota on mailbox or resource
version, ver display version info of current server
xfermailbox, xfer transfer (relocate) a mailbox to a different server
```

2.1 Arbeiten mit Postfächern

2.1.1 Anzeigen von Postfächern – lm

Mit dem Kommando `lm` lassen sich alle Postfächer und darin enthaltene Ordner sowie globale Mail-Ordner auflisten.

```
localhost> lm
user/busch/Spam@firma.de (\HasNoChildren)
user/busch@firma.de (\HasChildren)
user/heckler/Aufgaben@firma.de (\HasNoChildren)
user/heckler/Journal@firma.de (\HasNoChildren)
user/heckler/Kalender@firma.de (\HasNoChildren)
user/heckler/Kontakte@firma.de (\HasNoChildren)
user/heckler/Notizen@firma.de (\HasNoChildren)
user/heckler/Spam@firma.de (\HasNoChildren)
```

```
user/heckler@firma.de (\HasChildren)
user/koch/Aufgaben@firma.de (\HasNoChildren)
user/koch/Entw&APwrfe@firma.de (\HasNoChildren)
user/koch/Gel&APYschte Objekte@firma.de (\HasNoChildren)
user/koch/Gesendete Objekte@firma.de (\HasNoChildren)
user/koch/Journal@firma.de (\HasNoChildren)
user/koch/JunkE-Mail@firma.de (\HasNoChildren)
user/koch/Kalender@firma.de (\HasNoChildren)
user/koch/Kontakte@firma.de (\HasNoChildren)
user/koch/Notizen@firma.de (\HasNoChildren)
user/koch/Postausgang@firma.de (\HasNoChildren)
user/koch/Posteingang@firma.de (\HasNoChildren)
user/koch/Spam@firma.de (\HasNoChildren)
user/koch@firma.de (\HasChildren)
user/testuser/Spam@firma.de (\HasNoChildren)
user/testuser@firma.de (\HasChildren)
user/sauer/Spam@firma.de (\HasNoChildren)
user/sauer@firma.de (\HasChildren)
user/spam/Spam@firma.de (\HasNoChildren)
user/spam@firma.de (\HasChildren)
```

Soll die Suche eingeschränkt werden, können Wildcards benutzt werden:

```
localhost> lm *mey*
user/meyer/Spam@firma.de (\HasNoChildren)
user/meyer@firma.de (\HasChildren)
```

2.1.2 Anlegen von Postfächern und Ordnern – cm

Mit dem Kommando `cm` werden neue Postfächer oder Ordner innerhalb eines Postfachs erstellt. Das Anlegen des Postfachs eines Benutzers erfolgt automatisch, wenn in Univention Directory Manager an einem Benutzer-Objekt eine E-Mail Adresse eingetragen wird.

Ein globaler Mail-Ordner wird angelegt, indem beim Aufruf von `cm` anstelle des Präfixes **user** das Präfix **shared** angegeben wird. Globale Mail-Ordner liegen nicht innerhalb des Postfachs eines Benutzers und sind für die gemeinsame Benutzung gedacht. Eine Besonderheit stellen globale Ordner dar, die unter Verwendung von Toltec Connector in Microsoft Outlook und im Kolab-WebClient Horde verwendet werden sollen. Diese Ordner müssen unterhalb des 'user'-Namensraums angelegt werden.

```
localhost> cm user/mailadmin@firma.de
localhost> cm user/mailadmin@firma.de/reports
localhost> cm shared/messeberichte@firma.de
localhost> cm user/mailordner@firma.de
localhost> cm user/mailordner/mailordner@firma.de
```

2.1.3 Löschen von Postfächern und Ordnern – dm

Mit dem Befehl `dm` wird das gesamte Postfach gelöscht. Auch Ordner, die innerhalb dieses Postfachs angelegt wurden, werden entfernt. Das manuelle Löschen von Postfächern

ist erforderlich, wenn ein Benutzer in Univention Directory Manager gelöscht wurde, da hierbei keine Verzeichnisse des Benutzers, also auch das Postfach des Benutzers, nicht entfernt werden. Bevor ein Postfach entfernt werden kann (auch bei Verwendung von `cyradm` als privilegierter Benutzer), müssen Zugriffsrechte für den angemeldeten Benutzer auf das zu löschende Postfach gesetzt werden (siehe Abschnitt 2.2.2, Setzen von ACLs sam). Einzelne Ordner werden aus einem Postfach entfernt, indem beim Aufruf von `dm` der Ordner angegeben wird.

```
localhost> dm user/mailadmin@firma.de
localhost> dm user/testuser/backup@firma.de
```

2.1.4 Umbenennen von Postfächern – `renm`

Das Umbenennen von Postfächern erfolgt durch den Befehl `renm` unter Angabe des aktuellen und des neuen Namen des Postfachs. Bei Postfächern von Benutzern, die in Univention Directory Manager verwaltet werden, muss am BenutzerObjekt die E-Mail Adresse entsprechend angepasst werden.

```
localhost> renm user/testuser@firma.de user/usertest@firma.de
```

2.2 Access Control Lists (ACLs)

Eine ACL beschreibt die Zugriffsrechte eines Benutzers auf ein Postfach oder auf Ordner innerhalb des Mail-Systems. An einem Postfach können mehrere ACLs konfiguriert sein. Durch ACLs lässt sich bestimmen, ob ein Benutzer ein Postfach in seinem Mail-Client überhaupt sehen darf, ob er Schreibrechte hat oder nicht oder ob er dieses und in dem Postfach existierende Ordner löschen darf.

2.2.1 Anzeigen von ACLs – `lam`

Das Kommando `lam` listet alle zu einem Postfach oder einem Ordner gehörenden ACLs auf. Die erste Spalte stellt den betreffenden Benutzernamen dar, während die zweite Spalte die für diesen Benutzer geltenden Zugriffsrechte anzeigt jedes Zeichen steht für eine Berechtigung. Steht in der ersten Spalte **anyone**, so handelt es sich bei der darauf folgenden ACL um die Berechtigung, mit der alle Benutzer außer den namentlich aufgeführten auf das Postfachs zugreifen können, beispielsweise 'Nur lesen'.

```
localhost> lam user/testuser@firma.de
testuser@firma.de lrswipcda
anyone lrs
```

Im aufgeführten Beispiel bedeutet die Zeichenfolge 'lrswipcda', dass der Benutzer 'testuser@firma.de' vollständige Berechtigungen auf das Postfach hat. Alle anderen Benutzer dürfen nur lesend auf das Postfach zugreifen. Die einzelnen Zeichen und ihre Bedeutung:

l (lookup)	Für Benutzer ist das Postfach sichtbar
r (read)	Lesen, abrufen von E-Mails, suchen, Postfach oder Ordner kopieren
s (seen)	'gelesen'-Markierung an E-Mails setzen
w (write)	Markierung von E-Mails z.B. als 'wichtig', 'Spam', 'kein Spam' (außer 'gelesen' und 'gelöscht')
i (insert)	Ablegen von E-Mails und Ordnern in diesem Ordner
p (post)	An Ordner senden (wird nicht von allen Clients unterstützt)
c (create)	Erstellen, löschen und umbenennen von Postfächern und Ordnern
d (delete)	Löschen von Nachrichten
a (administer)	Administrative Rechte zum Setzen von ACLs

2.2.2 Setzen von ACLs – sam

Das Setzen von ACLs erfolgt über den Befehl `sam`. Das Postfach oder der Ordner, welches verändert werden soll, die Benutzer, die Rechte bekommen oder denen Berechtigungen entzogen werden sollen sowie die Berechtigungen selbst müssen beim Aufruf von `sam` angegeben werden.

```
localhost> sam user/sauer/projektdoku@firma.de testuser@firma.de lrswipcda
```

In diesem Beispiel wird der Ordner 'projektdoku' innerhalb des Postfachs sauer@firma.de komplett für den Benutzer 'testuser@firma.de' freigegeben. Dieser kann nun nicht nur Nachrichten lesen, sondern auch Nachrichten in diesem Mail-Ordner ablegen, weiteren Benutzern Berechtigungen einräumen oder den Ordner löschen. Anstatt einzelner Berechtigungen können auch sprechende Schlüssel bei der Vergabe von ACLs verwendet werden:

none	(keine Berechtigung)
read	lrs
post	lrsp
append	lrsip
write	lrswipcd
all	lrswipcda

```
localhost> sam shared/messeberichte@firma.de koch@firma.de read
localhost> sam shared/messeberichte@firma.de sauer@firma.de all
localhost> lam shared/messeberichte@firma.de
koch@firma.de lrs
sauer@firma.de lrswipcda
```

2.2.3 Entfernen von ACLs – dam

Mit dem Befehl `dam` lassen sich ACLs von einem Postfach oder einem Ordner entfernen, falls ein Benutzer keinerlei Rechte mehr für diese besitzen soll.

```
localhost> dam shared/messeberichte@firma.de testuser@firma.de
localhost> sam shared@firma.de meyer@firma.de none
```

2.3 Mail-Quota

Quota sind Speicherplatzbeschränkungen, die pro Postfach gesetzt werden können. Die Angaben der Quota erfolgt jeweils in Kilobyte.

2.3.1 Setzen von Quota – sq

Das Beschränken der Größe von Postfächern erfolgt mit dem Befehl `sq`. Um die Größe des Postfachs des Benutzers Meyer auf 10 MB zu beschränken, ist folgender Befehl erforderlich:

```
localhost> sq user/meyer@firma.de 10000
quota:10000
```

In diesem Zusammenhang sollten auch die Univention Configuration Registry-Variablen `mail/cyrus/imap/quotawarnpercent` und `mail/cyrus/imap/quotawarnkb` beachtet werden, über die konfiguriert werden kann, dass ein Benutzer beim Erreichen der Quota durch seinen Mail-Client informiert wird.

2.3.2 Anzeigen von Quota – lq

Das Anzeigen der Quota erfolgt mit dem Befehl `lq` unter Angabe eines Postfachs.

```
localhost> lq user/meyer@firma.de
STORAGE 0/10000 (0%)
```

2.4 Übertragung von Postfächern und globalen Mail-Ordern auf andere Mail-Server

Mit dem Befehl `xfer` kann ein Postfach oder ein globaler Mail-Ordner vom aktuellen Cyrus-Server auf einen anderen übertragen werden.

```
localhost> xfer user/testuser@firma.de mailserver2.firma.de
```

3 Sicherung und Wiederherstellung von Postfächern

Im Cyrus Mail-Dienst werden Postfächer und Ordner als Verzeichnisse im Dateisystem angelegt. Auf einem UCS- oder UGS-System liegen diese Verzeichnisse im Mail-Spool-Bereich unterhalb von `/var/spool/cyrus/mail/`.

Die Eigenschaft von Cyrus, mehrere Mail-Domänen verwalten zu können, spiegelt sich in der weiteren Struktur des Mail-Spool-Bereiches wieder; für jede

Mail-Domäne wird ein eigenes Verzeichnis angelegt. Für die Mail-Domäne 'firma.de' hiesse das Verzeichnis `/var/spool/cyrus/mail/domain/f/firma.de/`. Unter dem Verzeichnis der Mail-Domäne liegen dann wieder in einer vorgegeben Struktur die Postfächer der Benutzer. Dabei werden alle Postfächer, deren zugehörige E-Mail-Adressen mit dem gleichen Zeichen beginnen, in entsprechenden Verzeichnissen angelegt. Das Verzeichnis des Postfachs 'testuser@firma.de' wäre daher `/var/spool/cyrus/mail/domain/f/firma.de/t/user/testuser/`.

In diesen Verzeichnissen sind E-Mails als einzelne Dateien abgelegt, in denen Inhalt (Mail Body) und Informationen für Auslieferung und Anzeige (Mail Header) enthalten sind. Weitere, vom Benutzer im Mail-Client gesetzte Attribute, wie z.B. die Markierung, dass eine E-Mail gelesen oder als wichtig eingestuft wurde, werden in internen Cyrus Seen-Datenbanken verwaltet. Die Liste der Ordner, die zu einem Postfach gehören, werden von Cyrus in der Sub-Datenbank gespeichert. Diese Datenbanken liegen unter `/var/lib/cyrus/`. Dieses Verzeichnis besitzt ähnlich dem Mail-Spool-Bereich eine Unterteilung in Domänen und Benutzer, die Seen- und Sub-Datenbank für die E-Mail-Adresse testuser@firma.de liegen entsprechend im Verzeichnis `/var/lib/cyrus/domain/f/firma/user/t/testuser` als testuser.seen und testuser.sub.

Es sollten im Rahmen der Datensicherung des Mail-Dienstes sowohl das Mail-Spool-Verzeichnis als auch das Cyrus-Datenbanken-Verzeichnis gesichert werden. Dadurch ergeben sich mehrere Ansätze bei der Wiederherstellung von E-Mails. Einerseits kann durch die Verfügbarkeit der Seen- und Sub-Datenbanken das komplette Postfach inklusive der zum Zeitpunkt der Sicherung gesetzten Markierungen an E-Mails wiederhergestellt werden. Andererseits können einzelne E-Mails (also einzelne Dateien) ohne die letzten Markierungen aus der Datensicherung wiederhergestellt werden. Bei der Wiederherstellung einzelner E-Mails gehen die Markierungen verloren, da weder einzelne Einträge aus der Seen-Datenbank extrahiert, noch zwei Versionen der Seen-Datenbanken zusammengeführt werden können.

Es ist zu beachten, dass alle Dateien unterhalb der Mail-Spool- und Datenbanken-Verzeichnisse dem Benutzer **cyrus** gehören müssen, da der Mail-Dienst ansonsten nicht auf diese Dateien zugreifen kann. Sollte sich bei der Datensicherung oder beim Wiederherstellen von E-Mails und Ordnern der Besitzer geändert haben, muss dies vor den folgenden Schritten mit dem Befehl `chown cyrus:mail <Dateiname>` berichtigt werden.

Bei der Wiederherstellung von E-Mails reicht es nicht aus, die Dateien aus der Datensicherung in die entsprechenden Verzeichnisse zu kopieren. Damit der Mail-Dienst die E-Mails dem Benutzer wieder zur Verfügung stellen kann, müssen die vorhandenen Ordner und Dateien im Postfach in den Seen- und Sub-Datenbanken des Benutzers erneut registriert werden. Dieser Abgleich wird mit dem Befehl `cyrreconstruct` als Benutzer **cyrus** vorgenommen. Schon vor dem Kopieren der gesicherten Dateien und Ordner sollte der Cyrus Mail-Dienst über den Befehl `/etc/init.d/cyrus22 stop` angehalten werden, um Inkonsistenzen im Postfach zu verhindern. Nach erfolgreicher Ausführung von `cyrreconstruct` kann der Mail-Dienst mit `/etc/init.d/cyrus22 start` erneut gestartet werden.

```
root@mailserver2:~# /etc/init.d/cyrus22 stop
root@mailserver2:~# cp /tmp/backup/testuser/223. \
/var/spool/cyrus/mail/domain/f/firma.de/t/user/testuser/
root@mailserver2:~# chown cyrus:mail \
/var/spool/cyrus/mail/domain/f/firma.de/t/user/testuser/223.
```

```
root@mailserver2:~# su cyrus
executing: /usr/sbin/univentionmounthomedir.
executing: /usr/bin/univentionskel.
executing: /usr/sbin/univentionuserquota.
cyrus@mailserver2:~\$
```

cyrreconstruct unterstützt eine Vielzahl an Parametern. Für die Wiederherstellung von Postfächern aus Sicherungskopien wird der Befehl folgendermaßen aufgerufen:

```
cyrus@mailserver2:~\$ /usr/sbin/cyrreconstruct -C /etc/imapd/imapd.conf \
> rf
user/testuser@firma.de
user/testuser@zwanzig.de
cyrus@mailserver2:~\$ exit
root@mailserver2:~#
root@mailserver2:~# /etc/init.d/cyrus22 start
```

Da cyrreconstruct einige Einstellungen aus der Cyrus-Konfiguration benötigt, wird über den Parameter `-C` die aktuelle Konfigurationsdatei angegeben. Mit den Parametern `-r -f` wird veranlasst, dass die Registrierung rekursiv, also alle Ordner einbeziehend erfolgt, und dass alle Ordner im Postfach, in denen eine Datei `cyrus.header` liegt, in die Sub-Datenbank aufgenommen werden. Der letzte Parameter ist der Name des Postfachs, das wiederhergestellt werden soll.

Nach dem erneuten Start des Mail-Dienstes können Benutzer wieder auf ihre Postfächer und die darin wiederhergestellten E-Mails zugreifen.

4 Erneute Zustellung von E-Mails

Mit dem Cyrus Mail-Dienst werden in UCS standardmäßig die Anti-Viren- und Anti-Spam-Programme Amavis und Spamassassin ausgeliefert. Bevor eine E-Mail an ein Postfach zugestellt wird, überprüfen beide Programme, ob die E-Mail Viren enthält oder es sich bei der E-Mail um Spam handelt. In diesem Fall wird die E-Mail nicht zugestellt, sondern in einem Verzeichnis im Dateisystem abgelegt und der Benutzer darüber informiert. Da beide Programme mit heuristischen Erkennungsverfahren arbeiten, kann es dazu kommen, dass erwünschte E-Mails nicht ausgeliefert werden. In diesem Fall muss der Systemadministrator die isolierten E-Mails erneut zustellen.

In Cyrus ist das Programm `cyrdeliver` enthalten, mit dem Dateien – also auch isoliert abgelegte E-Mails – an ein vom Cyrus Mail-Dienst verwaltetes Postfach ausgeliefert werden können. `cyrdeliver` übergibt E-Mails direkt an den lokalen Mail-Dienst, daher ist es im Gegensatz zur Wiederherstellung von Postfächern mit `cyrreconstruct` erforderlich, dass der Mail-Dienst erreichbar ist. Grundsätzlich muss `cyrdeliver` nicht als bestimmter Benutzer aufgerufen werden. Allerdings muss der aufrufende Benutzer Leserechte für die zuzustellende Datei besitzen. E-Mails, die beispielsweise von Amavis isoliert wurden, liegen im Verzeichnis `/var/lib/amavis/`. Für jede E-Mail existiert ein eigenes Verzeichnis, dessen Name aus **amavis**, dem Zeitstempel des Eingangs und einer fortlaufenden Nummer besteht. Die eigentliche E-Mail ist in der Datei `email.txt` abgelegt. Diese Datei gehört

dem Besitzer **amavis** und nur dieser hat Leserechte. Daher bietet es sich an, cyrdeliver als Benutzer **root** auszuführen. Beim Aufruf von cyrdeliver muss über den Parameter **-C** die Konfigurationsdatei des Cyrus Mail-Dienstes angegeben werden. Der letzte Parameter ist die E-Mail Adresse, an welche die E-Mail ausgeliefert werden soll:

```
root@mailserver2:~# cat /var/lib/amavis/amavis20060915T08360201395/email.txt | \  
cyrdeliver -C /etc/imapd/imapd.conf testuser@firma.de
```