05/2011 Deutschland € 14,90 Österreich € 16,40 Schweiz SFR 29,80
www.TecChannel.de

IDG

TECCHANNEL COMPACT

IT Experts Inside

★ LAN ★ WLAN ★ Breitband ★

NETZWERK

Sicherheit

- Sichere WLAN-Konfiguration
- Netzwerkzugriffsschutz (NAP) mit Windows
- Netzwerkschutz mit Linux

Ratgeber

- Alles was Sie über IPv6 wissen müssen
- VDSL, Glasfaser, LTE und Co. im Vergleich

Praxis

- Windows 7 als Hotspot
- Tipps: WLAN einfacher und schneller
- RADIUS- & IMAP-Server einrichten

Netzwerk-Tools für Admins

2 Infrastruktur

Die wachsenden Ansprüche an Geschwindigkeit, Verfügbarkeit und Flexibilität von Netzwerken schlagen sich nieder in den immer höheren Anforderungen an die jeweilige Infrastruktur. Die sechs Praxisbeiträge in diesem Kapitel geben IT-Managern und Administratoren leicht nachvollziehbare Arbeitsanleitungen zur Einrichtung und Anpassung von Netzwerkressourcen an die Hand.

2.1 Workshop – IMAP-Server Dovecot installieren und konfigurieren

Wenn Benutzer ihren Mail-Client starten und Mails empfangen, kommen diese von einem sogenannten Mail-Transfer-Agent entweder über einen POP3- oder einen IMAP-Server. Dort meldet sich ein Mail-Client an, der Mail-Server bestätigt die Identität des Nutzers, die Liste der Nachrichten wird heruntergeladen, und der Benutzer kann sie lesen. POP3- und IMAP-Server haben demzufolge nichts mit dem Versand von E-Mails, sondern lediglich mit dem Empfang zu tun. Für den Versand ist der Mail-Transfer-Agent zuständig. Das bedeutet: Bevor Sie sich an die Installation und Konfiguration des IMAP-Servers machen, bringen Sie den Mail Transfer Agenten zum Laufen. In Debian und Ubuntu ist das üblicherweise Exim, in openSUSE wird meist Postfix verwendet. Erst danach kommt der IMAP-Server dran. Der Linux- und Unix-Server Dovecot (www.dovecot.org) unterstützt IMAP rev1 und POP3; IPv6, SSL und TLS werden ebenfalls genutzt.

Der Server wird hauptsächlich mit Linux, Solaris, FreeBSD, OpenBSD, NetBSD und Mac OS X eingesetzt. Laut seinem finnischen Entwickler Timo Sirainen hat Dovecot auch sonst gleich mehrere Vorteile: Er sei schnell, einfach aufzusetzen und benötige wenig Speicher. Dovecot unterstützt die Standard-Mailbox-Formate mbox und Maildir. Die Indexierung erfolgt relativ transparent, und der Server ist kompatibel zu vorhandenen Mailbox-Tools. Der Version 1.1.5 und darüber wird als einem von drei IMAP-Servern die volle Konformität bescheinigt, im Gegensatz zu weitaus bekannteren wie Cyrus, Courier und Microsoft Exchange. Die Indexdateien der Mailboxen optimieren sich während der Laufzeit selbst, und der Server behebt Probleme wie unterbrochene Indexdateien ebenso selbstständig. Auftretende Probleme loggt der Server in verständlichen Meldungen mit; sie erscheinen standardmäßig in der Datei */var/log/syslog*.

Auf die Mailboxen und Indexdateien kann man von vielen Computern gleichzeitig zugreifen und diese ändern. Postfix- und Exim-Nutzer können für den Mail-Versand und darüber hinaus für die SMTP-Authentifizierung direkt auf das Dovecot-Backend zugreifen, ohne dass eine separate Konfiguration erforderlich ist. Über Plugins kann der Server erweitert werden, um so neue Kommandos hinzuzufügen. Verschiedene Funktionen wie *Quota* und *ACL*-Unterstützung sind vollständig in

Plugins ausgelagert. Dovecot ist laut Sirainen speziell auf Sicherheit ausgelegt. Der Finne ist von seinem Produkt so überzeugt, dass er dem Ersten 1.000 Euro zahlen will, der eine Sicherheitslücke findet.

2.1.1 Dovecot installieren

In Ubuntu und Debian gibt es insgesamt sechs Pakete zu Dovecot, von denen aber nur eines für die Installation benötigt wird: für den POP3-Server das Paket *dovecot-pop3d* und für den IMAP-Server, dessen Installation im Folgenden erläutert wird, das Paket *dovecot-imapd*. Während der Installation werden drei Konfigurationsdateien angelegt:

- /etc/dovecot/dovecot-ldap.conf
- /etc/dovecot/dovecot-sql.conf
- /etc/dovecot/dovecot.conf

Die Datei */etc/dovecot/dovecot.conf* enthält eine Beispielkonfiguration; dafür fehlt in den Ubuntu- und Debian-Paketen die in der Dokumentation erwähnte und in anderen Distributionen vorhandene dovecot-example.conf. Ist die Datei im Verzeichnis */etc/dovecot* nicht vorhanden, kopieren Sie diese aus dem Verzeichnis */usr/share/dovecot*. Die Datei */etc/dovecot/dovecot.conf* ist auch die erste, die man anpassen muss. Öffnen Sie diese Datei daher in einem Editor. Die Datei enthält bereits alle Programmparameter. Diese sind zunächst allerdings größtenteils auskommentiert, weil es sich jeweils um die Standardvorgaben handelt. Damit Dovecot ordnungsgemäß startet, müsste der Benutzer lediglich in der Zeile mit dem Parameter „protocols“ das Kommentarzeichen löschen und anschließend das Kommando */etc/init.d/dovecot start* aufrufen. Doch eventuell wollen Sie noch verschiedene weitere Werte in der Konfiguration anpassen.

2.1.2 Protokoll festlegen

Ganz wichtig ist es, das vom Dovecot-Server verwendete Protokoll festzulegen. Für einen IMAP-Server schreiben Sie in die */etc/dovecot/dovecot.conf* die Zeile:

```
protocols = imap imaps
```

```
# Base directory where to store runtime data.
#base_dir = /var/run/dovecot/

# Protocols we want to be serving: imap imaps pop3 pop3s managesieve
# If you only want to use dovecot-auth, you can set this to "none".
#protocols = imap imaps
protocols = imap imaps
```

Editieren: Ziemlich am Anfang der Konfigurationsdatei /etc/dovecot/dovecot.conf steht die „protocols“-Zeile. Tragen Sie hier das Gewünschte ein.

Trennen Sie die Protokolle mit einem Leerzeichen, nicht mit Komma. Falls Sie auch POP3 nutzen wollen, fügen Sie das Protokoll einfach hinzu. Anschließend können Sie Dovecot mit */etc/init.d/dovecot start* starten und testen, ob der IMAP-Server am Port 143 auf Verbindungen horcht:

```
# telnet localhost 143
Trying 127.0.0.1...
Connected to localhost.localdomain
Escape character is '^]'.
* OK Dovecot ready.
```

Funktioniert das nicht, prüfen Sie die „protocols"-Einstellung und stellen sicher, dass *listen*=* in der Konfiguration steht, Dovecot also auf jedem Port horcht. Klappt alles, testen Sie die Verbindung von einem entfernten Rechner aus mit *telnet HOST 143*. Klappt das nicht, prüfen Sie, ob zwischengeschaltete Firewalls den Port sperren. Die sichere IMAPS-Verbindung testen Sie mit dem Befehl:

```
# openssl s_client -connect localhost:993
```

Von einem entfernten Rechner schreiben Sie anstelle von *localhost* den Host-Namen des IMAP-Servers. Der Befehl prüft darüber hinaus, ob Dovecot die SSL-Zertifikate korrekt erhält. Prüfen Sie danach, ob ein Login möglich ist.

```
# telnet localhost 143
a login username password
```

Anstelle von *username* und *password* setzen Sie einen vorhandenen Benutzernamen samt Passwort ein. Wenn Sie stattdessen ein *Authentication failed* erhalten, stellen Sie in der Konfigurationsdatei */etc/dovecot/dovecot.conf* die Parameter *auth_verbose = yes* und *auth_debug = yes* ein, starten Dovecot neu und versuchen es abermals. Jetzt sollte die Log-Datei genügend Informationen enthalten, um das Problem zu lösen.

Denken Sie daran, nach der Prüfung die Parameter wieder abzuschalten. Erhalten Sie stattdessen einen Alarm, dass das Passwort in Plaintext übertragen wird, schalten Sie in der Dovecot-Konfiguration um auf *disable_plaintext_auth = no*.

2.1.3 Wo sich die Mails befinden

Wenn das Protokoll geklärt ist, prüfen Sie im nächsten Schritt mit telnet, ob Dovecot die Inbox erkennt:

```
# telnet localhost 143

Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
* OK Dovecot ready.
```

```
a login username password
a OK Logged in.
b select inbox
* FLAGS (\Answered \Flagged \Deleted \Seen \Draft Old
➥ $Forwarded NonJunk Junk $MDNSent receipt-handled)
* OK [PERMANENTFLAGS (\Answered \Flagged \Deleted \Seen
➥ \Draft Old $Forwarded NonJunk Junk $MDNSent
➥ receipt-handled \*)] Flags permitted.
* 233 EXISTS
* 15 RECENT
* OK [UIDVALIDITY 1260711131] UIDs valid
* OK [UIDNEXT 87093] Predicted next UID
b OK [READ-WRITE] Select completed.
```

Erscheint nach *b select inbox* stattdessen die Meldung *NO Internal error [<date> <time>]*, kann das mehrere Gründe haben:

- Die Benutzerdatenbank enthält eine UID-Nummer für den Benutzer, die nicht dem Besitzer der Mail-Dateien entspricht.
- Wenn Sie LDAP nutzen, beachten Sie, dass die Datei */etc/dovecot/dovecot-ldap.conf* eine UID-Einstellung enthält, die nicht dem Besitzer der Dateien mit den Mails entspricht.
- Die Mail-Dateien des Benutzers sind nicht in dem Verzeichnis, das in der Dovecot-Konfiguration mit *mail_location* gesetzt wurde.

Die einfachste Methode, der Ursache auf den Grund zu kommen ist: Setzen Sie in der Konfiguration *mail_debug = yes* und versuchen es erneut. Anschließend sollte der Befehl *c list "" **** in telnet auch weitere bereits vorhandene Mailboxen anzeigen. Werden diese angezeigt und sind trotzdem im Mail-Client keine zu sehen, so liegt es am Mail-Client.

2.1.4 Mailboxen automatisch erkennen

Dovecot kann die Mailboxen automatisch erkennen. Das funktioniert aber nur, wenn ein Benutzer bereits Mails in der Inbox hat. Sollte das nicht der Fall sein oder wollen Sie weitere Optionen nutzen, konfigurieren Sie das mithilfe der Einstellung *mail_location*. Hier werden üblicherweise die folgenden Variablen verwendet:

- %u: vollständiger Benutzername
- %n: der Benutzername aus user@domain (identisch mit %u, wenn dort keine Domain angegeben ist)
- %d: Domain-Teil in user@domain (leer, wenn keine Domain vorhanden)

Für eine Maildir-Mailbox wird normalerweise folgende Einstellung benutzt:

```
mail_location = maildir:~/Maildir
```

Für das mbox-Format ist die folgende Einstellung typisch:

```
mail_location = mbox:~/mail:INBOX=/var/mail/%u
```

In beiden Beispielen werden das Mail-Format, der Ordner im Home-Verzeichnis und für *mbox* das Spool-Verzeichnis angegeben. Die Indexdateien werden üblicherweise im selben Verzeichnis gespeichert wie die Mails – für *maildir* in den aktuellen Mail-Verzeichnissen, für *mbox* im versteckten .imap-Verzeichnis. Das kann man ändern, indem man *:INDEX=location* hinzufügt, etwa so:

```
mail_location = mbox:~/mail:INBOX=/var/mail/%u
➥ :INDEX=~/imap-indexes
```

Nun sollte vonseiten Dovecots alles funktionieren. Wenn Sie sich mit einem Mail-Client nicht mit dem IMAP-Server verbinden können, liegt die Ursache vermutlich beim Mail-Client. Hier sollten Sie zunächst die SSL/TLS-Einstellungen prüfen. Stellen Sie sicher, dass der Client die Plaintext-Authentisierung nutzt, sofern Sie Dovecot nicht explizit anders konfiguriert haben. Falls der Client nur den Posteingang anzeigt, prüfen Sie, ob der Client vielleicht so eingestellt ist, dass er nur abonnierte Mailboxen anzeigt. In dem Fall sollten Sie die gewünschten noch abonnieren. Welche Mailboxen Sie abonniert haben, zeigt Ihnen telnet mit *d lsub "" **.

2.1.5 In Datei loggen

Standardmäßig loggt Dovecot seine Aktivitäten in die Datei */var/log/syslog*. Möchten Sie stattdessen eine eigene Datei benutzen, ändern Sie in der Datei */etc/dovecot/dovecot.conf* die Variablen *log_path* und *info_log_path*, etwa so:

```
log_path: /var/log/dovecot/error.log
info_log_path: /var/log/dovecot/info.log
```

Anschließend müssen Sie noch das Verzeichnis erzeugen und dessen Benutzerrechte festsetzen:

```
# mkdir /var/log/dovecot
# chown dovecot:adm /var/log/dovecot
# chmod 2755 /var/log/dovecot
```

Damit diese Verzeichnisse nicht überlaufen und eventuell den Festplattenplatz verschlingen, lassen Sie die Log-Dateien rotieren. Das erledigt das Programm *logrotate*. Im Verzeichnis */etc/logrotate.d* ist aufgeführt, welche Log-Dateien regelmäßig rotiert werden. Legen Sie dort die Datei */etc/logrotate.d/dovecot* an, um auch Dovecots Log-Dateien in die Rotation aufzunehmen. Die Datei kann zum Beispiel folgenden Inhalt haben:

```
/var/log/dovecot/error.log /var/log/dovecot/info.log {
daily
missingok
rotate 60
```

```
compress
delaycompress
notifempty
create 640 dovecot adm
sharedscripts
postrotate
if [ -f /var/run/dovecot/master.pid ]; then
/bin/kill -USR1 'cat /var/run/dovecot/master.pid'
fi
endscript
}
```

2.1.6 Authentifizierung des Benutzers testen

Wenn via Telnet der Login fehlschlägt und den Versuch mit der Meldung *NO Authentication failed* quittiert, gibt es dafür mehrere Gründe:

- Der Benutzer steht nicht in der Benutzerdatenbank.
- Der Benutzer steht in der Benutzerdatenbank, hat aber kein Passwort.
- Wenn Sie LDAP verwenden, ist in der pass_attrs-Einstellung in der Datei */etc/dovecot/dovecot-ldap.conf* kein Passwort spezifiziert.
- Sie haben den Benutzernamen und/oder das Passwort falsch geschrieben.

Mehr erfahren Sie, wenn Sie die Einstellung *auth_verbose = yes* in der Dovecot-Konfiguration einschalten. Erhalten Sie anstelle der oben genannten Meldung den Fehler *NO Login failed: Unsupported authentication mechanism*, sollten Sie die Einstellung *auth_mechanisms = plain* für jeden Authentifizierungsvorgang einschalten.

```
webserver:~# dovecot -n
# 1.0.15: /etc/dovecot/dovecot.conf
log_timestamp: %Y-%m-%d %H:%M:%S
login_dir: /var/run/dovecot/login
login_executable: /usr/lib/dovecot/imap-login
mail_privileged_group: mail
auth default:
  passdb:
    driver: pam
  userdb:
    driver: passwd
webserver:~#
```

Auflistung: Dovecot mit dem Parameter „-n“ aufgerufen, listet alle Variablen und Argumente, die nicht den Standardvorgaben entsprechen.

Die geläufigste Methode zur Authentifizierung für existierende Systemnutzer ist PAM (Pluggable Authentication Modules). Mit virtuellen Benutzern wird meist LDAP, eine SQL-Datenbank oder eine *passwd*-Datei benutzt. Auch für den Konfigurationstest kann man zunächst eine Passwortdatei *passwd.dovecot* anlegen mit nur der folgenden Zeile:

```
benutzer:passwort
```

Anstelle von *benutzer* und *passwort* geben Sie Ihren Nicht-Root-Benutzernamen ein sowie irgendein einfaches Passwort, das nur zum Testen verwendet wird. Bedenken Sie, dass das Passwort unverschlüsselt übertragen wird; wählen Sie daher nicht Ihr eigentliches Passwort. Danach ändern Sie die Konfigurationsdatei */etc/dovecot/dovecot.conf*. Fügen Sie im Bereich hinter *auth default* die drei Zeilen hinzu:

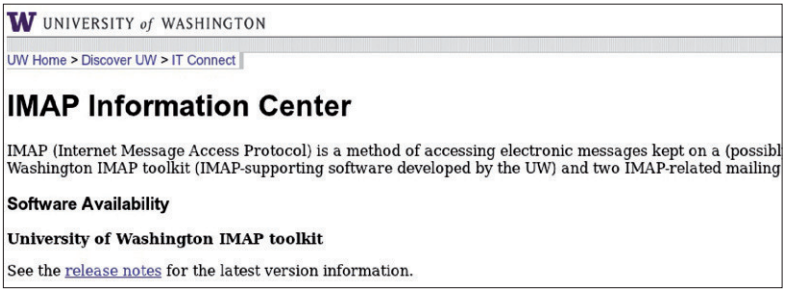
```
passdb passwd-file {
args = /etc/passwd.dovecot
}
```

Kommentieren Sie anschließend noch den Bereich *passdb pam* aus, damit die PAM-Authentifizierung nicht unnötigerweise versucht wird. Stellen Sie außerdem den Parameter *disable_plaintext_auth = no* ein, um die Plaintext-Authentifikation zu ermöglichen. Denken Sie aber daran, diese nach den Tests auf den Standardwert zurückzustellen. Nach dem Speichern der Konfiguration sollte *dovecot -n* nun unter anderem diese Ausgabe liefern:

```
auth default:
passdb:
driver: passwd-file
args: /etc/passwd.dovecot
userdb:
driver: passwd
```

2.1.7 Von anderen IMAP-Servern umsteigen

Wer von anderen IMAP-Servern zu Dovecot wechselt, muss ein paar Dinge berücksichtigen. So erlaubt etwa UW-IMAP (www.washington.edu/imap/) den Zugriff auf das gesamte Home-Verzeichnis. Viele Nutzer speichern daher ihre Mails im mail/-Verzeichnis und haben das auch als *mail/* im Client eingestellt. Dovecot hat damit Probleme, denn es interpretiert dies als *~/mail/mail/*. Das kann man abstellen, indem man die Vorgabe im Client entfernt.



Referenz: UW-IMAP, der IMAP-Server der Universität von Washington, gilt als Referenzserver.