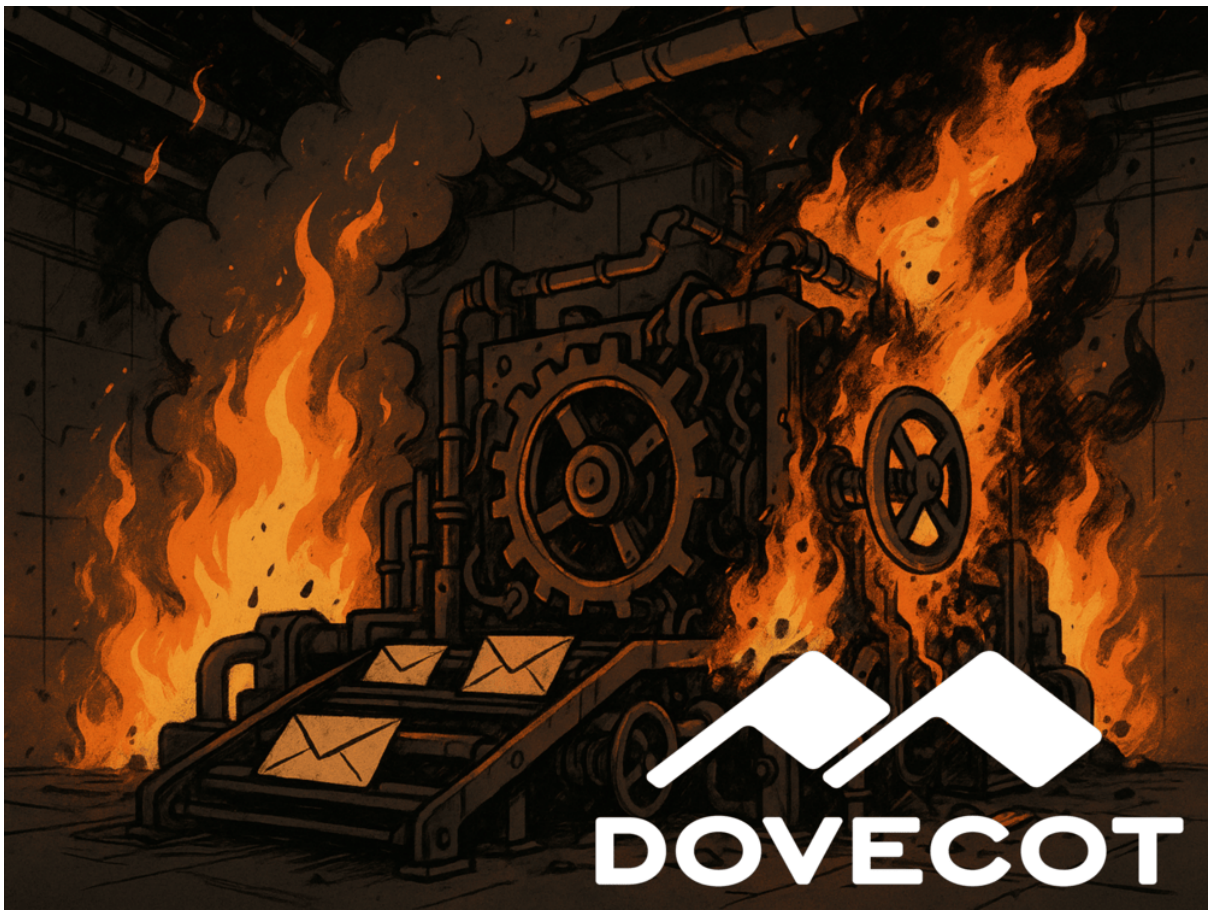
Änderungen mit Unterbrechungen

Dovecot 2.3 auf 2.4 in Debian Stable aktualisieren

Willem L. Middelkoop
June 4, 2025



Letzte Woche geriet ich während einer Routinewartung unserer E-Mail-Infrastruktur in unerwartete Schwierigkeiten. Wir verarbeiten täglich tausende von E-Mails und nutzen Dovecot, um unseren Kunden Zugriff auf ihre Nachrichten zu ermöglichen. Das alles kam zu einem jähen Stillstand, als ich auf Version 2.4 aktualisierte, die Breaking Changes enthält... oh je!

TL;DR: Upgrade von Dovecot 2.3 → 2.4 auf Debian

- **Dovecot 2.4 führt Breaking Changes ein**: Konfigurationsdateien von 2.3 sind inkompatibel. Die Software startet nicht, wenn Sie sie nicht umschreiben.
- **Neue Konfigurationssyntax und Variablensystem**: Parameter wie ‘ssl_cert‘, ‘mail_location‘ und ‘%d‘ haben Format und Bedeutung geändert.

- **Kein automatisierter Migrationspfad**: Manuelle Überprüfung und Umschreiben der Konfiguration ist erforderlich – insbesondere bei Verwendung von SQL-Backends, Sieve oder benutzerdefinierter Authentifizierung.
- **Empfehlung**: Lesen Sie die offizielle Upgrade-Anleitung sorgfältig durch, bevor Sie ein Upgrade durchführen, und testen Sie Konfigurationen isoliert.

Spaziergang im Park

Aufgrund einiger Sicherheitsupdates und zur Behebung einiger Kompatibilitätsprobleme habe ich beschlossen, einige Pakete auf einem Debian GNU/Linux-Server zu aktualisieren, der für die E-Mail-Dienste meines Unternehmens zuständig ist. Diese spezielle Distribution von GNU/Linux ist für ihre Stabilität und Zuverlässigkeit bekannt. Es gab keinen Grund, Probleme zu erwarten, und ich startete das Upgrade in der Erwartung, dass es in wenigen Minuten abgeschlossen sein würde. Nur "ein Spaziergang im Park", was könnte schon schiefgehen..?

'dovecot_config_version' erforderlich

Der größte Teil des Servers kam wie erwartet fast sofort wieder online, wodurch die Dienste so wenig unterbrochen wurden, dass selbst der Uptime Monitor Alarm keinen Ausfall feststellte - außer bei Dovecot. Diese spezielle Software ist für den IMAP- und POP3-Zugriff auf Postfächer zuständig. Sie fügt sich als fein abgestimmtes Zahnrad in ein größeres Setup ein, bei dem andere Programme wie Postfix auf ihre Funktion angewiesen sind, um eingehende E-Mails zu empfangen. Der Startfehler von Dovecot verursachte eine Reihe von Problemen.

Das erste, was man als Serveradministrator tut, ist, die Server-Daemons ('systemctl status dovecot') zu überprüfen, gefolgt von der Überprüfung der Logs, z. B. durch Ausführen von 'journalctl -u dovecot'. Das zeigte schnell, dass Dovecot sich weigerte zu starten, weil ein Konfigurationsparameter fehlte: 'dovecot_config_version'.

Einfach den Parameter zur Konfiguration unter '/etc/dovecot/dovecot.conf' hinzufügen, könnte man denken? Nun... NEIN. Es stellt sich heraus, dass die Entwickler von Dovecot den Fehler aus gutem Grund eingebaut haben: Die neue Version 2.4 von Dovecot ist nicht kompatibel mit früheren 2.3-Konfigurationsdateien; das bedeutet, dass Sie viele verschiedene Parameter umschreiben müssen. Es sind nicht nur die Namen der Konfigurationsvariablen, es wird auch eine völlig neue Syntax für die Erweiterung von Einstellungsvariablen eingeführt. Ein alter Variablenwert wie '%d' wird nun zu '%{user | domain}'. Die Liste der Änderungen ist lang und es gibt keine automatisierte Möglichkeit, Ihre Konfiguration zu migrieren. Stellen Sie sich mein Gesicht vor, als mir das Ausmaß meines Problems bewusst wurde.

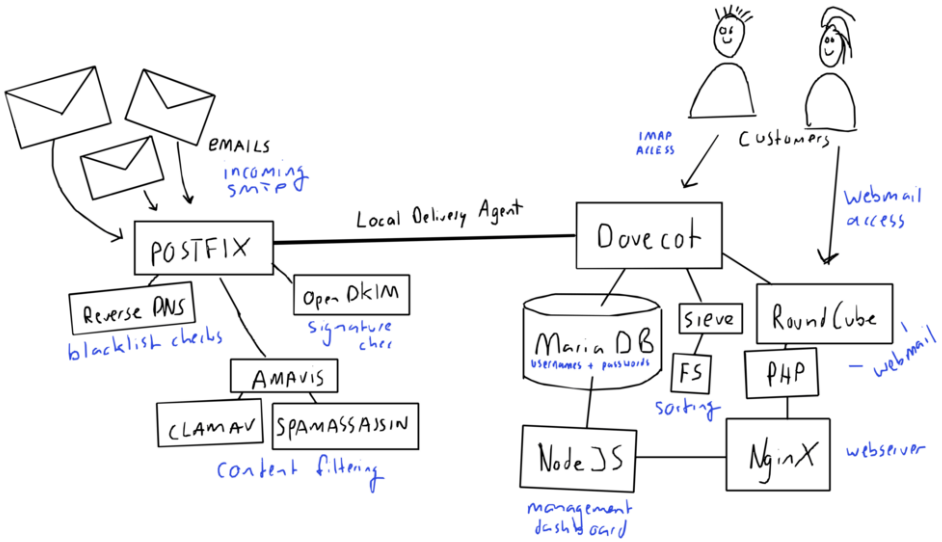
Integrierte Komplexität: Zahnräder in einer Maschine

Die Sache mit E-Mail-Diensten ist, dass es *schwierig* ist. Nicht, weil eine einzelne Komponente schwierig ist, sondern weil man zum Betrieb eines vollständigen E-Mail-Stacks viele verschiedene Teile benötigt, die nahtlos zusammenarbeiten. Hier sind einige der Teile, aus denen sich der E-Mail-Dienst meines Unternehmens zusammensetzt:

- **Postfix:** Der primäre SMTP Mail Transfer Agent (MTA), der mit anderen Mailservern kommuniziert, um E-Mails zu empfangen und zu senden. Er muss wissen, welche

E-Mail-Adressen für den Empfang von Mails gültig sind und wer berechtigt ist, neue Nachrichten zu senden.

- **Amavis-Filter:** Alle vom Server verarbeiteten Mails durchlaufen den Amavis-Filtermechanismus, der einzelne Nachrichten mit SpamAssissin und ClamAV überprüft.
- **SpamAssasin:** Anhand eines komplexen Regelsatzes und Bayes'scher Analysen werden Nachrichten automatisch auf die Wahrscheinlichkeit gescannt, Spam zu sein.
- **ClamAV:** Nachrichten werden auf Viren gescannt. Anhänge werden extrahiert und Datei für Datei analysiert.
- **Reverse DNS-Blacklists:** Zusätzlich zum Scannen der Nachrichten führt der Mailserver auch eine Hintergrundprüfung der externen Server durch, mit denen er kommuniziert. Mail-Header werden analysiert und einzelne Hops auf ihren Ruf überprüft.
- **OpenDKIM:** Einige Nachrichten enthalten eine 'Domain Key'-Signatur, die beweist, dass ihr Absender autorisiert ist. Nachrichten mit Headern werden überprüft, während andere mit einem in Postfix eingebundenen Milter-Dienst signiert werden.
- **Sieve:** Eingehende Nachrichten werden automatisch nach benutzerspezifischen Regeln sortiert, z. B. werden bestimmte Nachrichten in bestimmten Ordnern abgelegt. Sieve muss wissen, welche Regeln für welche Adressen gelten.
- **MariaDB / MySQL:** Die E-Mail-Adressen, gültige Logins, Benutzernamen, Passwort-Hashes und Aliase werden in einer zentralen Datenbank gespeichert. Spezifische SQL-Abfragen sind konfiguriert, um Dinge wie "Ist dies ein gültiges Passwort?" zu überprüfen.
- **Nginx:** Der E-Mail-Server verfügt auch über einen Webserver, der die Verwaltung von Konten und den Zugriff auf E-Mails per Webmail ermöglicht.
- **NodeJS:** Die Verwaltungskonsole verwendet ein NodeJS-Backend, um Serveradministratoren und Clients die Einrichtung ihrer Adressen und Passwörter zu ermöglichen.
- **Roundcube**: Der Server verwendet ein weit verbreitetes Webmail-Programm, um Clients den Zugriff auf ihre E-Mails über den Browser zu ermöglichen.
- **PHP:** Das Webmail benötigt PHP zum Ausführen, einschließlich einiger Abhängigkeiten, damit es mit Dovecot (mit IMAP) und MariaDB (mit SQL) kommunizieren kann.
- **Dovecot:** Dann gibt es noch Dovecot, die eigentliche Software, die es Endbenutzern ermöglicht, auf ihre E-Mails zuzugreifen. Sie ermöglicht authentifizierten Benutzern den Zugriff auf die E-Mails, die auf den Festplatten der Infrastruktur gespeichert sind, unter Verwendung von Protokollen wie IMAP oder POP3.



Ein vollständiger Mailserver-Stack besteht aus vielen kleineren Komponenten, die fein aufeinander abgestimmt sind

Diese Teile sind alle fein aufeinander abgestimmt, wie Zahnräder in einer komplexen Maschine passen sie präzise zusammen. Ihre Konfiguration ist auf ihre spezifische Rolle zugeschnitten und interagiert oft mit mehreren anderen Teilen. Sie können sich vorstellen, dass eine unerwartete Änderung an einem dieser Zahnräder (wie Dovecot) eine ziemliche Störung verursachen kann!

Es gab keine schnelle Lösung, kein automatisiertes Konfigurations-Upgrade. Da dieses Update relativ neu ist, hatten die meisten großen Sprachmodelle (KI) auch keine Antwort. ChatGPT generierte einfach Vorschläge basierend auf der alten 2.3-Dokumentation. Um das Problem zu lösen, musste ich *'Old-School-Linux-Server-Fähigkeiten'* anwenden: manuelle Erstellung einer neuen, maßgeschneiderten Konfiguration für Dovecot 2.4.

Stopp, um Datenverlust zu verhindern

Sobald ich die Natur des Problems erfasst hatte, stoppte ich sofort die meisten E-Mail-Dienste (z. B. brachte ich die Engine zum vollständigen Stillstand). Dies verhindert Datenverlust, da die Verarbeitung von E-Mails gestoppt wird. Dies führt dazu, dass andere Mailserver E-Mails in die Warteschlange stellen und manchmal 4xx SMTP-Fehler (wie 421, 451, 454 oder 455) ausgeben. Das Design des weltweiten E-Mail-Protokolls berücksichtigt temporäre Ausfälle und andere Server werden es einfach später erneut versuchen.

Umschreiben der Konfiguration durch RTFM

Die Fehlermeldung in den Logs verwies mich auf die offiziellen Dovecot Dokumente, und da war sie: eine gelblich hervorgehobene WARNUNG, die die Konfigurationsänderungen beschrieb. Es ist ein langes Dokument: als PDF zählt es 18 Seiten. An einem normalen Tag würde es einige Mühe kosten, dies durchzuarbeiten - stellen Sie sich vor, Sie müssten dies tun, während das sprichwörtliche Haus in Flammen steht!

Die Konfiguration von Dovecot besteht aus verschiedenen Dateien, die alle Teile des Verhaltens der Software einrichten. Wie z. B. die Authentifizierung durchgeführt wird, oder wie sie mit einem Sieve-Filter integriert wird, oder woher sie die Benutzernamen und Passwort-Hashes für die Anmeldung bezieht. Die in Dovecot 2.4 eingeführten Änderungen betreffen fast alle Parameter, da die Entwickler eine neue Syntax für Servervariablen eingeführt haben.

Syntax der Variablenschreibweise

Früher verwendete die Konfiguration die Variablenschreibweise wie '%u' als Platzhalter für einen Benutzernamen. Die neue Syntax erlaubt es, Variablen an einen Modifikator zu übergeben, was Normalisierung und Dinge wie die Auswahl von Teilstrings ermöglicht. Zum Beispiel: Um eine E-Mail-Domain aus einem Benutzernamen zu erhalten, verwendet man nicht mehr '%d', sondern die 'user'-Variable als Basis, um sie mit dieser Syntax an den Domain-Modifikator zu übergeben: '%{user | domain}'.

Sobald ich diese neue Sprache verstand, wusste ich das Kunstwerk, das sie darstellt, wirklich zu schätzen. Es ist eine Verbesserung gegenüber den älteren abgekürzten Variablennamen, da man nicht mehr in einem Wörterbuch nachschlagen muss: Statt etwas vagem wie '%r' liest man jetzt '%{remove_ip}'. Es ist von Natur aus lesbarer, was ich sehr schätze.

Verschlüsselung: 'ssl_cert' wird zu 'ssl_server_cert_file'

Weitere Änderungen betreffen die Art und Weise, wie die Konfiguration auf externe Dateien verweist, die für die Verschlüsselung verwendet werden. Früher hatte man eine Einstellung 'ssl_cert', die das eigentliche SSL/TLS-Zertifikat als String enthalten konnte. In Version 2.4 hat man die Variable 'ssl_server_cert_file', die stattdessen einen Pfad zur Zertifikatsdatei im Dateisystem enthält. **Es ist nicht nur eine Umbenennung, auch die Art des Werts ist neu!** Um die Konfiguration zu korrigieren, müssen Sie jeden dieser aktualisierten Parameter durchgehen und seine Auswirkungen auf Ihr spezielles Setup bestimmen. Das ist zeitaufwändig und fehleranfällig.

Aufteilen der Einstellung 'mail_location'

Neu in 2.4 ist die Art und Weise, wie die 'mail_location' in mehrere kleinere Variablen aufgeteilt wird. Früher definierte eine einzige Variable, wo E-Mails auf der Festplatte gespeichert wurden. Jetzt müssen Sie diese in die beiden Variablen 'mail_driver' und 'mail_path' aufteilen, **UND** die neue Servervariablensyntax verwenden. Wenn Sie eine davon falsch eingeben, verschwinden alle E-Mails (vertrauen Sie mir!). Abhängig von Ihrer spezifischen Speicherkonfiguration sollten Sie den Benutzernamenteil überprüfen (z. B. geben Sie die gesamte E-Mail-Adresse oder nur das Präfix ohne Domainnamen an?).

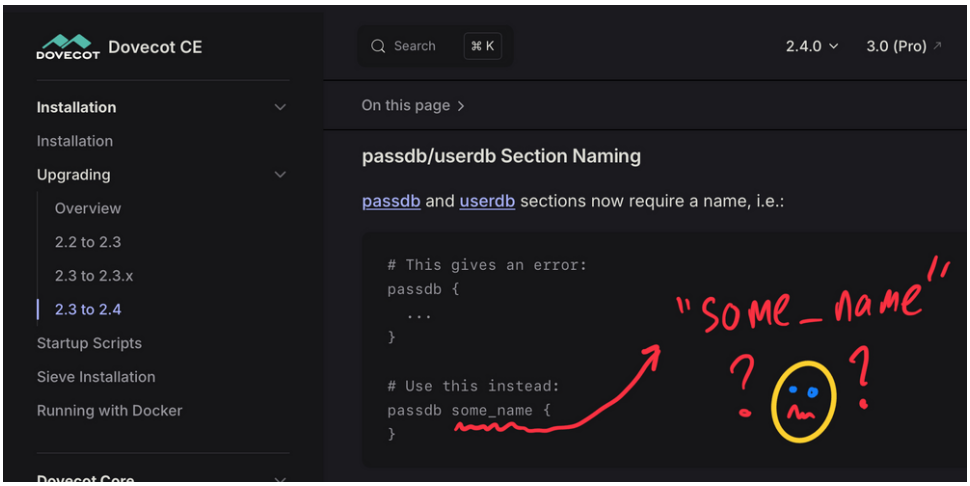
```
# Dovecot 2.3 config:
# mail_location = maildir:/var/vmail/%d/%u

# Corresponds to 2.4 syntax:
mail_driver = maildir
mail_path = /var/vmail/%{user | domain }/%{user | username}
```

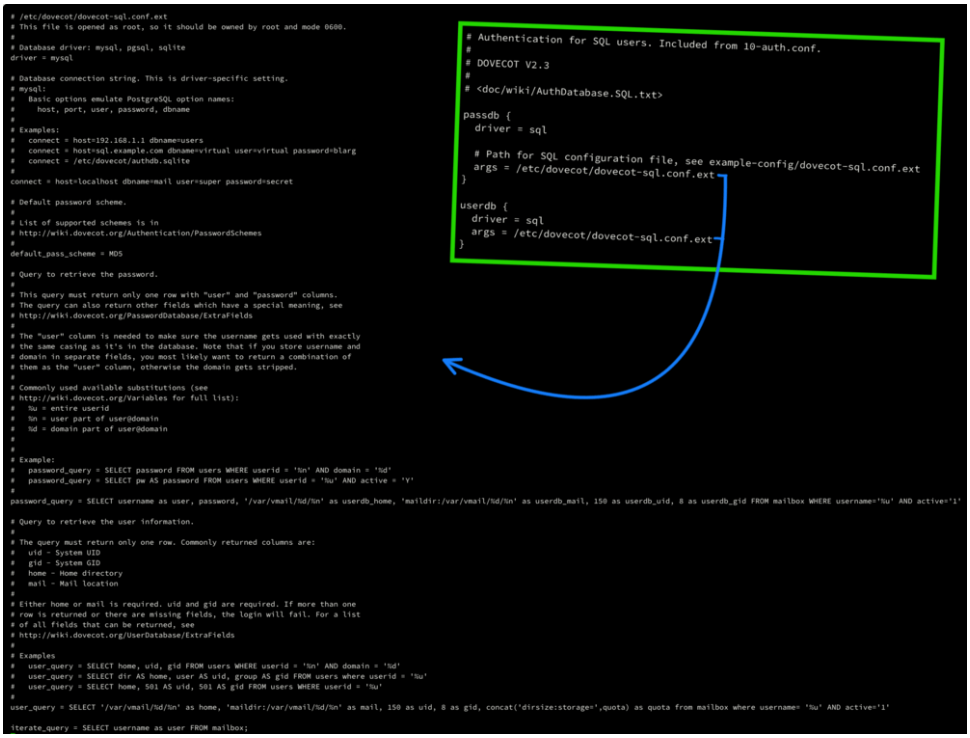
Migration von mail_location zu mail_driver und mail_path unter Verwendung der neuen Servervariablen-Syntax

Dovecot mit SQL-Backend: passdb und userdb

Wenn Ihre Dovecot-Installation mit einer externen Datenbank (oder einem Speicher) arbeitet, um Benutzernamen und Passwörter zu authentifizieren, müssen Sie die 'auth-sql.conf.ext' in '/etc/dovecot/conf.d/' umschreiben, die von der Datei 10-auth.conf aufgerufen/eingebunc wird. In Dovecot 2.4 gibt es eine neue Art der Segmentierung der passdb- und userdb-Einstellungen. Im Dovecot 2.3-Setup habe ich eine externe Datei verwendet, um die Datenbankabfragen und die Verbindungszeichenfolge bereitzustellen. Während der Authentifizierung werden die mehreren Abfragen verwendet, um 1) Benutzer zu authentifizieren und 2) benutzerspezifische Einstellungen wie den Pfad des E-Mail-Speichers zu laden.



Die Upgrade-Anleitungen für userdb und passdb sind auf den ersten Blick sehr hilfreich /s



Dovecot 2.3 SQL-Backend-Setup (auth-sql.conf.ext und dovecot-sql.conf.ext)

In der neuen Version 2.4 müssen Sie die Parameter so umstrukturieren, dass sie in Abschnitten eingeschlossen sind, die direkt hinter den Schlüsselwörtern 'userdb' und 'passdb' in der Konfiguration einen Backend-Typ-Indikator enthalten. Wenn Sie also eine MySQL-Datenbank als Backend verwenden, müssen Sie 'userdb' in 'userdb sql' ändern. Sie können die Parameter der Verbindungszeichenfolge direkt in die Datei 'auth-sql.conf.ext' einfügen, so dass sich alle relevanten Parameter in einer Konfigurationsdatei befinden. Um die Komplexität zu reduzieren, habe ich den userdb-Abschnitt so umgeschrieben, dass er den 'static'-Datenbanktreiber verwendet: Generierung von Konfigurationsvariablen wie dem Mail-Pfad des Benutzers basierend auf dem Benutzernamen des Benutzers. Siehe die entsprechenden Dokumente.

```
# Authentication for SQL users. Included from auth.conf.
#
# DOVECOT 2.4
#
# <https://doc.dovecot.org/latest/core/config/auth/databases/sql.html>

# Database driver: mysql, pgsql, sqlite
sql_driver = mysql

# Database connection string. This is driver-specific setting.
mysql localhost {
    user = super
    password = secret
    dbname=mail
}

passdb sql {
    default_password_scheme = MD5
    query = SELECT username as user, password FROM mailbox WHERE username='%{user}' AND active='1'
}

# If you don't have any user-specific settings, you can avoid the user_query
# by using userdb static instead of userdb sql, for example:
# <https://doc.dovecot.org/latest/core/config/auth/databases/static.html>
userdb static {
    fields {
        uid = 150
        gid = 8
        home = /var/vmail/%{user | domain}/%{user | username}
    }
}
```

Dovecot 2.4 SQL-Backend-Setup (auth-sql.conf.ext) - jetzt viel kompakter als sein Vorgänger. Es gibt jetzt nur noch eine SQL-Abfrage, da die userdb-Sektion jetzt das statische Backend verwendet

Sieve-Plugin

Wenn Ihr Setup Sieve zum Sortieren eingehender E-Mails verwendet, müssen Sie Ihr Setup in Bezug auf den Speicherort des Skripts, seine Standardeinstellungen und sein Verhalten anpassen. Die neue Dovecot 2.4-Version führt ein Konzept namens "Script Storage" ein, das es ermöglicht, dynamisch geladene Skripte für verschiedene Benutzer bei verschiedenen Ereignissen auszuführen. Unser Setup beinhaltet ein einfaches Standard-Sieve-Skript, das als Spam markierte E-Mails automatisch in einen Ordner namens Spam sortiert. Die neue Syntax ermöglicht eine kompaktere Konfiguration:

```
##
## Settings for the Sieve interpreter
##
## DOVECOT 2.3
##

# Do not forget to enable the Sieve plugin in 15-lda.conf and 20-lmtp.conf
# by adding it to the respective mail_plugins= settings.

plugin {
  # The path to the user's main active script. If ManageSieve is used, this the
  # location of the symbolic link controlled by ManageSieve.
  sieve = ~/.dovecot.sieve

  # The default Sieve script when the user has none. This is a path to a global
  # sieve script file, which gets executed ONLY if user's private Sieve script
  # doesn't exist. Be sure to pre-compile this script manually using the sievec
  # command line tool.
  # --> See sieve_before fore executing scripts before the user's personal
  #     script.
  sieve_default = /var/lib/dovecot/sieve/default.sieve

  # Directory for :personal include scripts for the include extension. This
  # is also where the ManageSieve service stores the user's scripts.
  sieve_dir = ~/sieve
}
```

Sieve-Konfiguration in Dovecot 2.3 (90-sieve.conf) mit den nun veralteten Variablen sieve_default und sieve_dir

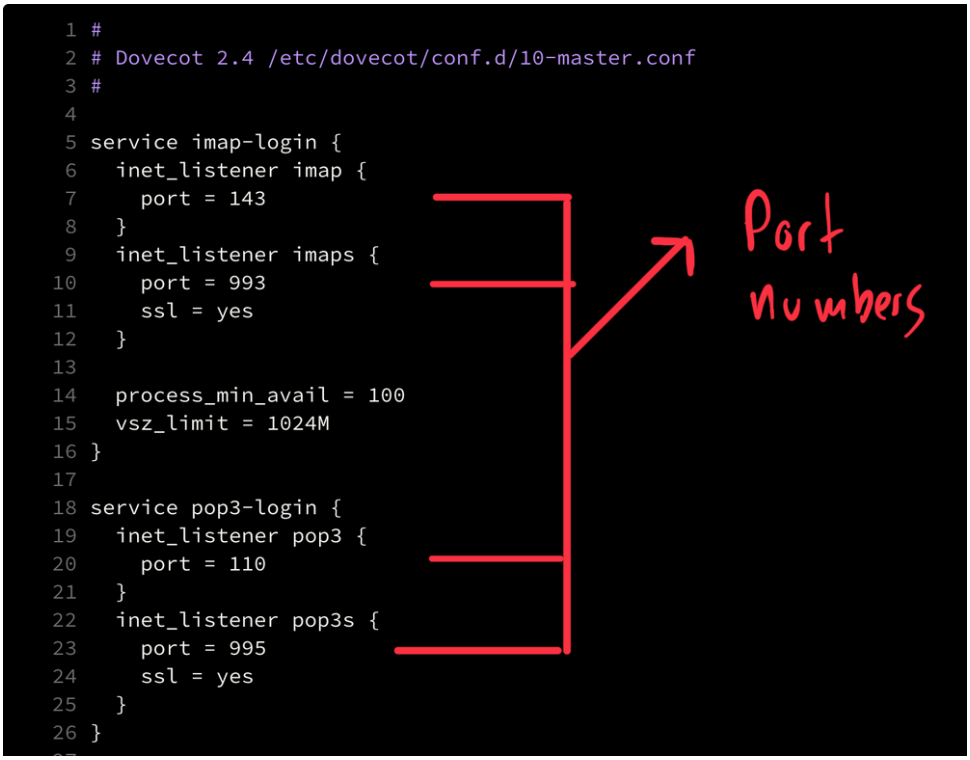
```
1  # /etc/dovecot/conf.d/90-sieve.conf
2  #
3  # DOVECOT 2.4
4  #
5  # Sieve default settings loading global script
6
7  sieve_script default {
8      type = default
9      name = default
10     driver = file
11     path = /var/lib/dovecot/sieve/default.sieve
12 }
```

Sieve-Konfiguration in Dovecot 2.4 (90-sieve.conf)

Testen der neuen Konfiguration

Sie könnten versucht sein, den Server einfach wieder zu starten, nachdem Sie die 2.4-Konfiguration neu definiert haben. Sie sollten jedoch sehr vorsichtig sein, da eine falsche Konfiguration dazu führen könnte, dass Clients den Zugriff auf alle E-Mails verlieren und/oder gezwungen sind, ihre gesamten Postfächer erneut herunterzuladen. Stattdessen habe ich mich für einen schrittweisen Ansatz entschieden, bei dem ich die IMAP- (und POP3-) Portnummern in beliebige Werte geändert habe. Auf diese Weise konnte ich das neue Setup selbst testen, während ich die tatsächlichen Kunden davon abhielt, sich mit dem Server zu verbinden. So konnte ich einige Tippfehler beheben, die neue Servervariablensyntax verfeinern und einige merkwürdige Log-Meldungen bearbeiten. Sie können

die Portnummern des Servers in der Datei '10-master.conf' steuern.



Einrichten der IMAP- und POP-Nummern des Servers, um privates/schrittweises Debuggen der neuen Konfiguration zu ermöglichen

Schlussfolgerung

Ausfälle wie dieser sind dank der Stabilität von Debian GNU/Linux selten, aber nicht unmöglich. Für den Lemmid Online E-Mail-Dienst meines Unternehmens sind tägliche Backups und ein getesteter Disaster-Recovery-Plan vorhanden. Obwohl diesmal kein vollständiges Failover erforderlich war, erwiesen sich frühere Übungen als entscheidend für die schnelle Anpassung der Konfiguration.

Dieser Vorfall hat uns daran erinnert, dass selbst mit Automatisierung und KI tiefes Systemwissen, Vorbereitung und manuelles Debugging unverzichtbare Werkzeuge bleiben, wenn sich kritische Infrastrukturkomponenten unerwartet und ohne automatisierte Migrationspfade ändern.

Dovecot 2.4 Beispielkonfiguration

Wenn Sie diesen Beitrag auf der Suche nach einer Lösung für Ihren eigenen defekten Mailserver finden, könnten diese Dovecot 2.4 Beispielkonfigurationsdateien nützlich sein. Ich habe sie während meiner eigenen Reparaturarbeiten gefunden und sie könnten Ihnen etwas Zeit sparen, um die neue Syntax herauszufinden: https://source.willem.com/dovecot-2.4-sample-config/