

Einführung in die Serverdienste  
- Deutsche Ausgabe -

# Rinux Manual

Clemens Renner

Version 1.0 vom 13. April 2005





## Vorwort

Schön, dass du dir die Zeit nehmen willst, etwas über die Serverdienste auf Rlinux zu lesen. Das Rlinux Manual ist vor allem aus dem Grund entstanden, mir etwas Arbeit beim Support der Nutzeraccounts abzunehmen. Ich wollte einmal alle wichtigen Dinge aufschreiben, gegebenenfalls später Ergänzungen hinzufügen und letztlich bei konkreten Fragen, die hier abgedeckt werden, einfach auf das Rlinux Manual verweisen.

Falls deiner Meinung nach Punkte nicht klar genug sind oder einige zusätzliche Bemerkungen angebracht wären, so freue ich mich natürlich über jeden Hinweis in dieser Richtung. Schreib dazu bitte einfach eine E-Mail an [hosting@rlinux.net](mailto:hosting@rlinux.net).

*Clemens Renner*  
Dortmund, April 2005.

## Rechtliche Festlegungen

Das Rlinux Manual wurde erstellt, um Benutzern des Rlinux-Servers den Einstieg in die vielen verschiedenen Dienste zu erleichtern und bei einigen fortgeschrittenen Fragen Hilfestellung zu geben.

Es ist daher im Interesse des Autors, dass alle Benutzer Zugang zu diesem Handbuch haben - die uneingeschränkte Weitergabe dieses Dokuments (vornehmlich, aber nicht ausschließlich im Kreis der Nutzer) ist zulässig und erwünscht. Hingegen sind Veränderungen an diesem Dokument nicht erlaubt, ebensowenig wie die kommerzielle Verwertung als Ganzes oder von Teilen daraus.

Ferner sei erwähnt, dass die Zusammenstellung der im Rlinux Manual zu findenden Anleitungen mit großer Sorgfalt erfolgt ist. Letztlich ist aber nicht auszuschließen, dass die Darstellungen unvollständig oder fehlerhaft sind, zumal mit hoher Wahrscheinlichkeit nicht alle Aktualisierungen der jeweiligen Software berücksichtigt werden können.

Das Dokument befindet sich im Prozess stetiger Aktualisierung und wird bei Bedarf in neuerer Fassung zur Verfügung gestellt. Die jeweils jüngste Version kann von der Startseite des Servers (<http://rlinux.net>) bezogen werden.

**Copyright © 2005 Clemens Renner.**

This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/2.0/de> or send a letter to

Creative Commons  
559 Nathan Abbott Way  
Stanford, California 94305  
USA.



# Inhaltsverzeichnis

<b>1</b>	<b>Willkommen</b>	<b>1</b>
<b>2</b>	<b>Schnelleinstieg</b>	<b>3</b>
2.1	Das Passwort ändern . . . . .	3
2.2	SSL-Root-Zertifikat installieren (optional) . . . . .	5
2.3	E-Mail-Dienste einrichten . . . . .	10
<b>3</b>	<b>Das Konfigurationsmenü</b>	<b>11</b>
3.1	Speicherplatznutzung einsehen (Disk Quota) . . . . .	11
<b>4</b>	<b>E-Mail</b>	<b>13</b>
4.1	Vorbemerkungen zu E-Mail via SSL . . . . .	13
4.2	Eingehende Post . . . . .	13
4.3	Ausgehende Post . . . . .	14
4.4	E-Mail-Empfang und -Versand absichern . . . . .	15
4.5	Der Webmailer . . . . .	16
4.6	Spam- und Virenschutz . . . . .	17
4.7	Verschlüsselte E-Mails mit GnuPG . . . . .	19
4.8	Weiterleitung . . . . .	20
4.9	Mailinglisten . . . . .	20
4.10	Post von anderen Servern abholen ( <code>fetchmail</code> ) . . . . .	21
4.11	Sortieren und Filtern ( <code>procmail</code> ) . . . . .	24
<b>5</b>	<b>Webspace</b>	<b>27</b>
5.1	Dateien hochladen ( <code>ftp</code> ) . . . . .	27
5.2	Dynamische Webseiten mit PHP . . . . .	28
5.3	MySQL-Datenbanken benutzen und verwalten . . . . .	28
5.4	Skripte mit CGI und SSI . . . . .	29
5.5	Teilbereiche mit einem Passwort schützen ( <code>.htaccess</code> ) . . . . .	30
5.6	Nutzungsstatistiken (AWStats) . . . . .	31
5.7	Bildergalerie . . . . .	32

## *Inhaltsverzeichnis*

# 1 Willkommen

Willkommen auf Rinux! Dein Account auf Rinux soll eine Bereicherung für dein Online-Dasein darstellen. Er soll dir dabei helfen, schnell und unkompliziert mit den alltäglichen Aufgaben fertigzuwerden und darüber hinaus etwas dazu beitragen, dass du dich um die für dich wichtigen Dinge kümmern kannst, ohne über technische Kleinigkeiten nachdenken zu müssen.

Das Rinux Manual soll dir den Einstieg in die Dienste, die auf Rinux angeboten werden, erleichtern. Das fängt bei einfachen Fragen an, wie:

- Wie kann ich E-Mails empfangen und versenden?
- Wo kann ich die Dateien für meine Homepage hochladen?
- Wieviel Platz habe ich noch auf dem Server?

Daneben sollen aber auch schwierigere Fragen berührt werden, etwa:

- Was muss ich beachten, wenn ich CGI-Skripte benutzen möchte?
- Wie kann ich schon auf der Server-Seite unerwünschte E-Mails entsorgen, sodass diese gar nicht mehr den Weg in mein Postfach finden?
- Was tun, wenn's brennt? Welches Programm löscht Feuer in meinem Home-Verzeichnis?

Ich hoffe, dass dir diese ausführliche Anleitung hilft, schon bald möglichst produktiv all das zu nutzen, was für dich wichtig ist. Und wenn du einen interessanten Dienst durch das Rinux Manual neu entdeckst: Nur keine Angst, probier ihn ruhig aus!

Letzten Endes steht dir immer die Möglichkeit offen, technische Unterstützung zu bekommen, indem du eine E-Mail an `hosting@rinux.net` schickst.<sup>1</sup>

---

<sup>1</sup>Bitte benutze ausschließlich diese E-Mail-Adresse für Supportanfragen.



## 2 Schnelleinstieg

Bevor es richtig losgeht, musst du einige wenige Dinge unbedingt erledigen. Um den optimalen Start hinzulegen, musst du als erstes:

1. Das Passwort ändern.
2. Das SSL-Root-Zertifikat installieren (optional, aber *empfohlen*).
3. Den E-Mail-Dienst startklar machen.

Sowohl die Änderung des Passworts als auch die grundlegende Einrichtung des E-Mail-Diensts sind zwingend erforderlich.

### 2.1 Das Passwort ändern

Es ist wichtig, dass du ein gutes Passwort wählst. Unter <http://makeashorterlink.com/?S561126CA><sup>1</sup> findest du einige Hinweise, die du besser berücksichtigst. In den meisten Fällen bist du selbst derjenige, dem es am meisten Leid tut, hier nicht den nötigen Aufwand betrieben zu haben.

#### 2.1.1 Mit dem Konfigurationsmenü

Jetzt ist der geeignete Zeitpunkt, einen Web-Browser zu öffnen und eine Webseite anzuspringen: <http://config.rinux.net>.



Falls du auf das Konfigurationsmenü nicht zugreifen kannst, ist vermutlich durch eine Firewall auf dem Rechner, an dem du sitzt, der Port 20000 auf Zielrechnern gesperrt. In diesem Fall musst du das Passwort ändern, wie in Kapitel 2.1.2 beschrieben.

Auf der Seite angekommen, loggst du dich dort mit dem Benutzernamen, den du gewählt hast und dem Passwort, dass du erhalten (oder anfänglich gewählt) hast, ein. Danach wird ein

<sup>1</sup><http://www.uni-regensburg.de/Einrichtungen/Rechenzentrum/Benutzer/Accounts/passwords.html>

## 2 Schnelleinstieg

Menü angezeigt, in dem du am oberen Rand (wie in Abb. 2.1 gezeigt) eine Kategorie auswählen kannst. Du entscheidest dich hier für *Password, Themes & Quota*. Danach wählst du die Option *Change Password*. Jetzt gibst du zuerst dein aktuelles und danach zwei mal dein neues Passwort ein. Mit *Change Now* bestätigst du die Änderung.



Abbildung 2.1: Kategorieauswahl im Konfigurationsmenü



Bitte logge dich aus dem Konfigurationsmenü jetzt aus und versuche sofort danach, dich mit dem geänderten Passwort wieder einzuloggen. Sollte das nicht funktionieren, ist etwas schiefgegangen und du solltest dich umgehend mit mir in Verbindung setzen, da du sonst deinen Account nicht benutzen kannst.

### 2.1.2 Mit dem Webmailer

Eine alternative Möglichkeit, dein Passwort zu ändern, ist über den Webmailer. Du findest den Webmailer unter <http://smaill.rinux.net> (Details zur Bedienung des Webmailers sind in Kapitel 4.5, S. 16 beschrieben).

Auch hier loggst du dich mit deinem Benutzernamen und deinem anfänglichen Passwort ein. Danach siehst du am oberen Rand im rechten Teil des Fensters das Menü ähnlich wie in Abb. 2.2.

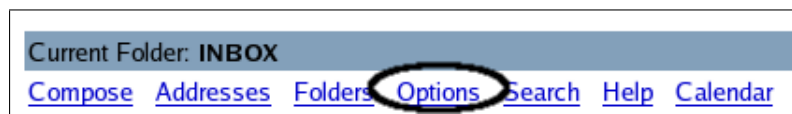


Abbildung 2.2: Wähle *Options* im Menü des Webmailers

Dort gibt es eine Option mit dem wohlklingenden Namen *Change Password*, die du auswählst. Du siehst drei Eingabefelder, in die du zunächst dein altes Passwort und dann zwei mal dein neues Passwort einträgst. Nach einem Klick auf *Submit* ist das Passwort geändert - oder du erhältst eine Fehlermeldung, zum Beispiel, wenn du dich bei der Wiederholung des neuen Passworts vertippt hast. Versuch es dann einfach noch einmal.



Bitte logge dich aus dem Webmailer jetzt aus und versuche sofort danach, dich mit dem geänderten Passwort wieder einzuloggen. Sollte das nicht funktionieren, ist etwas schiefgegangen und du solltest dich umgehend mit mir in Verbindung setzen, da du sonst deinen Account nicht benutzen kannst.

## 2.2 SSL-Root-Zertifikat installieren (optional)

Für viele Dienste, die auf Rinux angeboten werden, gibt es die Möglichkeit, Verschlüsselung über SSL zu verwenden. Das bedeutet, dass beim Verbindungsaufbau zu dem jeweiligen Dienst zunächst ein Verschlüsselungsmodus ausgehandelt wird. Danach wird der Dienst wie gewöhnlich angesprochen. Für den Benutzer entsteht nahezu kein Unterschied in der Bedienung.

Der entscheidende Vorteil besteht aber darin, dass die Daten, die von deinem Computer aus gesendet werden (ebenso wie die vom Rinux-Server erhaltenen Daten) nicht im Klartext, sondern chiffriert übertragen werden. Das erschwert unter anderem natürlich das „Mithören“ von Passwörtern, ist also ein Gewinn in Sachen Sicherheit.

Ein Risiko, dem man dabei entgegen muss, ist der sogenannte Mittelsmann-Angriff. Im eher unwahrscheinlichen, aber nicht unmöglichen Fall, dass es jemandem gelingt, bei einem Zugriff auf Rinux die Kommunikation abzufangen und auf einen dritten Rechner umzuleiten, kann der Angreifer beispielsweise dein Passwort ausspionieren. Besonders populär sind diese Angriffe derzeit im Rahmen von Phishing-Versuchen, bei denen Bankkunden etwa das bekannte Portal ihres Online-Bankings angezeigt wird, sich dahinter aber eine Webseite verbirgt, die die eingegebenen Daten abhört, speichert und an den richtigen Bankrechner weiterleitet. Anschließend wird der Kunde automatisch auf die tatsächliche Bank-Webseite geschickt und merkt von all dem Spuk nichts, da sich das System wie gewöhnlich verhält. Der Angreifer jedoch ist nun im Besitz der Login-Daten für das Online-Banking des Opfers.

Gerade bei verschlüsselten Verbindungen gibt es jedoch ein Mittel dagegen. Dort präsentiert der angesteuerte Dienst zunächst ein Zertifikat, mit dem er beteuert, tatsächlich der zu sein, für den er sich ausgibt. Diese Zertifikate werden unterschrieben von einer vertrauenswürdigen Instanz - in unserem Fall der Rinux-Zertifikats-Autorität. Da diese jedoch nicht standardmäßig z.B. in Browsern oder E-Mail-Programmen registriert ist, muss das nachgeholt werden (siehe Abbildungen 2.3, 2.4, 2.5 und 2.6).

Der erste Schritt ist das Herunterladen des Zertifikats von <http://rinux.net/rinux-root.crt>. Falls dir das nicht sicher genug ist, kannst du das Zertifikat auch per E-Mail an [hosting@rinux.net](mailto:hosting@rinux.net) anfordern.

Dann rufst du (Abb. 2.3) den Zertifikat-Manager in Thunderbird auf. Gemäß Abb. 2.4 wird danach die Kategorie *Authorities* ausgewählt und dort die *Import*-Funktion aufgerufen. Es erscheint ein Fenster, in dem das (gerade gespeicherte) Root-Zertifikat als Datei ausgewählt wird.

Ist das geschehen, musst du angeben, dass dieses Zertifikat für die Identität von Webseiten (im

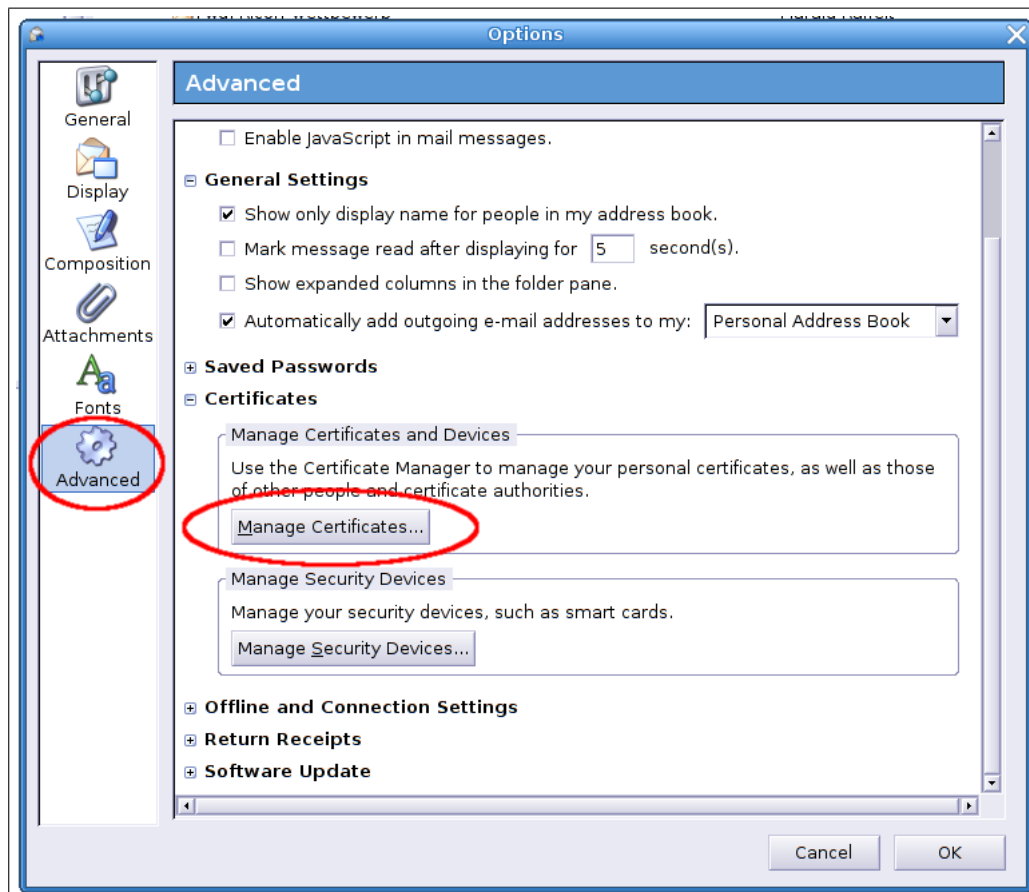


Abbildung 2.3: Thunderbird: Zertifikate verwalten

weiteren Sinne: Internet-Diensten) bürden soll (Abb. 2.5). Solltest du noch Zweifel am Zertifikat haben, kannst du mit einem Klick auf *View* die Zertifikats-Details einsehen.

Am Ende solltest du noch sicherstellen, dass Rinux erfolgreich in die Liste der Zertifikats-Autoritäten aufgenommen wurde (Abb. 2.6).

## 2.2 SSL-Root-Zertifikat installieren (optional)

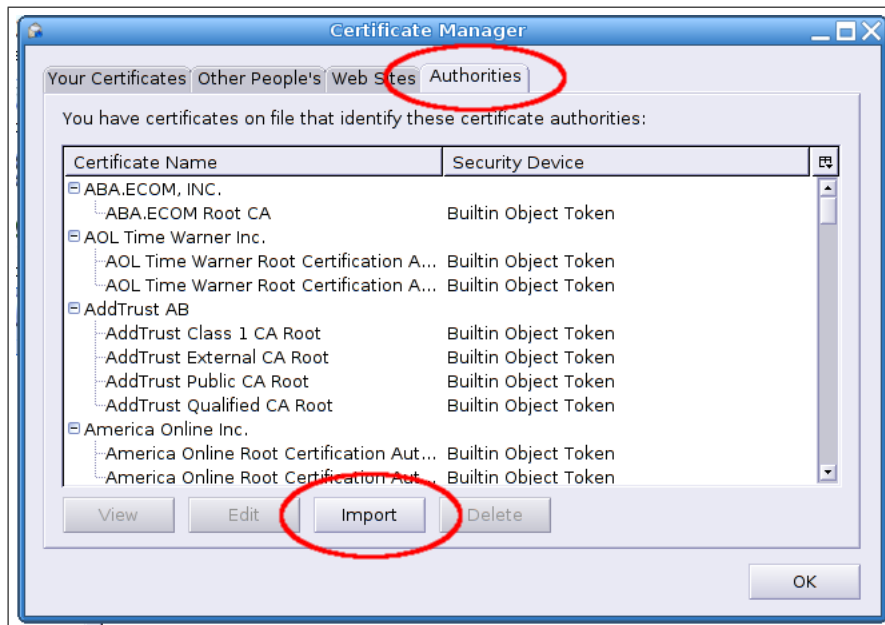


Abbildung 2.4: Thunderbird: Ein Zertifikat importieren

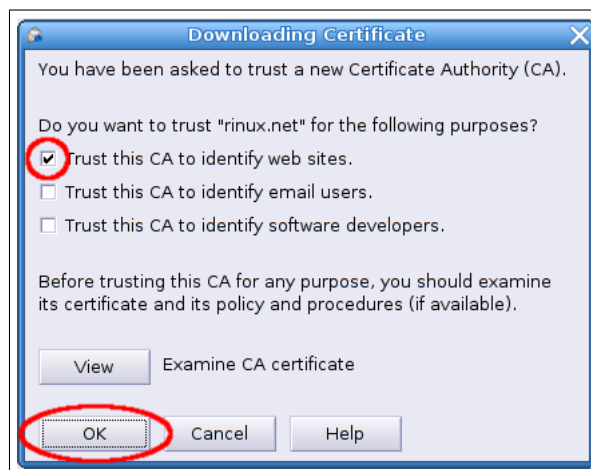


Abbildung 2.5: Thunderbird: Zertifikatimport abschließen

## 2 Schnelleinstieg

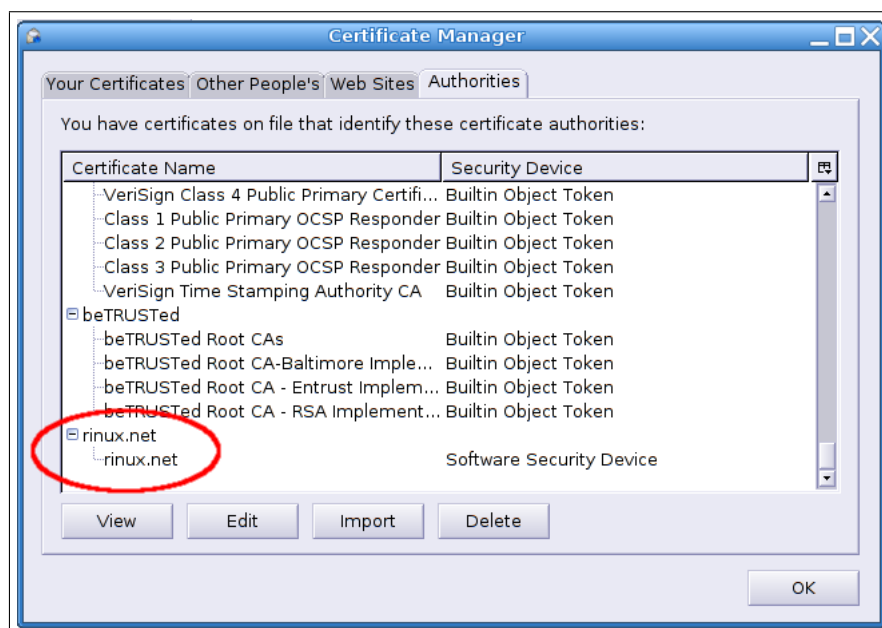


Abbildung 2.6: Thunderbird: Das importierte Zertifikat überprüfen

Der Import des Rinux-Root-Zertifikats (also eines Zertifikats, das für die Identität aller über SSL aufgerufenen Rinux-Dienste bürgt), hat mehrere Vorteile:

- Dienst-Zertifikate müssen nicht einzeln bestätigt werden. Diese werden vielmehr implizit angenommen, weil sie vom Root-Zertifikat abstammen, das als vertrauenswürdig eingestuft wurde.
- Die Einzel-Zertifikate tragen ein Ablaufdatum und müssen bei Erreichen des Ablauftags gegen neue Zertifikate ausgetauscht werden. Auch hier werden die erneuerten Zertifikate automatisch akzeptiert (durch das in das Root-Zertifikat ausgesprochene Vertrauen).
- Der Import des „großen“ Zertifikats schützt vor oben beschriebenem Angriff, da Dienste, die sich mit einem nicht von Rinux erstellten Zertifikat ausweisen, kein implizites Vertrauen erhalten. Hat man das Root-Zertifikat also installiert und verlangt ein Dienst *zusätzlich*, dass *sein* vorgeblich von Rinux stammendes Zertifikat akzeptiert werden muss, ist hier Vorsicht geboten!

Letzten Endes musst du die angebotenen SSL-Varianten, bei denen eben dieser Zertifikatsabgleich erfolgt, natürlich auch *nutzen*, um von der zusätzlichen Sicherheit profitieren zu können. Beispiele für SSL-Angebote findest du im Kapitel 4 über E-Mail und im Kapitel 5 zu den Webhosting-Diensten.

## 2.3 E-Mail-Dienste einrichten

Die zweite Aufgabe am Anfang ist, sicherzustellen, dass du die E-Mails empfangst, die an deine E-Mail-Adresse auf Rinux geschickt werden. Das ist die einzige Möglichkeit für mich, dich zu erreichen.

Details zur E-Mail-Einrichtung findest du in den ersten Abschnitten von Kapitel 4.

## 2 Schnelleinstieg

## 3 Das Konfigurationsmenü

Über das Konfigurationsmenü (*Usermin*) kannst du eine ganze Reihe allgemeiner Einstellungen für deinen Account vornehmen. Die meisten Funktionen dieses Werkzeugs werden in anderen Kapiteln näher beschrieben, da sie dort thematisch besser passen.



### Konfigurationsmenü (*Usermin*)

Werkzeuge und accountweite Einstellungen.

Server: <http://config.rinux.net>

*Um das Konfigurationsmenü benutzen zu können, musst du auf Zielrechnern den Port 20000 ansprechen können. In Firmen- oder Hochschulnetzwerken ist das unter Umständen nicht gestattet und durch eine Firewall technisch unterbunden.*

### 3.1 Speicherplatznutzung einsehen (Disk Quota)

Logge dich in das Konfigurationsmenü ein und wähle die Kategorie *Password, Themes & Quota*; klicke danach auf *Disk Quotas*.

In der Tabellenspalte *Blocks, Hard Limit* findest du den für dich vorgesehenen Speicherplatz auf dem Server. Die Spalte *Blocks, Used* gibt Auskunft darüber, wieviel Platz du momentan belegt hast. Der belegte Platz wird dabei in Kilobytes (KB) angegeben - um diese Zahl in Megabytes (MB) umzurechnen, teilst du diese durch 1024.

In der Regel haben User auf Rinux einen Platz von 80 MB zur Verfügung. Solltest du mehr Platz benötigen, können wir gerne darüber verhandeln.

### 3 *Das Konfigurationsmenü*

## 4 E-Mail

In diesem Kapitel wird beschrieben, wie du Herr über dein elektronisches Postfach wirst. Neben grundlegenden Konfigurationshinweisen findest du hier auch Anleitungen, mit denen du deinen E-Mail-Account auf Rinux zu deiner elektronischen Nachrichtenzentrale machst.

### 4.1 Vorbemerkungen zu E-Mail via SSL

Sowohl der Empfang als auch der Versand von E-Mails über Rinux kann verschlüsselt erfolgen. Dazu sind in der Regel jedoch zusätzliche Einstellungen in deinem E-Mail-Programm nötig. Am Beispiel Thunderbird ist das in Kapitel 4.4 erklärt.

In der Einleitung dieses Handbuchs (Kap. 2.2) wird darauf eingegangen, warum dieses Vorgehen überhaupt interessant ist. Auch wenn das anfangs kompliziert klingt, solltest du die Verschlüsselung in Betracht ziehen.

### 4.2 Eingehende Post

Wenn du ein klassisches E-Mail-Programm (*E-Mail-Client*) benutzt, hast du die Wahl zwischen zwei Möglichkeiten. Beide haben ihre Vorteile - entscheide selbst, was dir angemessener erscheint.

#### 4.2.1 POP3

Das etwas betagte Post Office Protocol (*POP3*) trägt seine Abkürzung nicht zu Unrecht. Man bezeichnet das Herunternehmen von Elementen aus einem Stapel auch als *pop*. Dieser Name ist bezeichnend, denn bei POP3 holst du mit deinem E-Mail-Programm die E-Mails vom Server ab und lagerst sie ausschließlich auf deiner Festplatte.<sup>1</sup>

Der Vorteil dabei ist, dass du keine Verbindung zum E-Mail-Server aufrechterhalten musst, um deine E-Mails zu lesen. Du kannst also alle E-Mails abholen, die Verbindung trennen und offline deine Post lesen. Der Nachteil wiederum liegt auf der Hand: Nur an dem Rechner, an dem du die E-Mails abgeholt hast, kannst du diese auch lesen.

---

<sup>1</sup>Das stimmt nicht so ganz. Du kannst auch festlegen, dass die E-Mails nach dem Abholen noch auf dem Server bleiben sollen. Das ist aber nicht der eigentliche Sinn des Verfahrens.



### **POP3-Server**

E-Mails abholen und zu Hause lesen.

Servername: **rinux.net**

Port: 110 (unverschlüsselt), 995 (verschlüsselt)

Wenn du dich für POP3 entscheidest, kannst du deine E-Mails nicht in verschiedenen Ordnern auf dem Server verwalten, und im Webmailer siehst du deine E-Mails ebenfalls nur so lange, wie du sie noch nicht mit deinem E-Mail-Programm abgeholt hast.

### **4.2.2 IMAP4**

Mit dem Internet Message Access Protocol (*IMAP*) kannst du anders als bei POP3 von jedem Computer mit Internetzugang auf deine E-Mails zugreifen. Du kannst deine E-Mails in Ordnern auf dem Server verwalten und dort sortieren. Auch hier deutet sich der Nachteil an: Ohne eine Internetverbindung macht IMAP keinen Spaß.

Mit der zunehmenden Verfügbarkeit breitbandiger Internetzugänge, die nicht nach Online-Zeit, sondern nach übertragenem Volumen abrechnen, überwiegen hier jedoch in der Regel die Vorteile.



### **IMAP4-Server**

E-Mails serverseitig organisieren und weltweit lesen.

Servername: **rinux.net**

Port: 143 (unverschlüsselt), 993 (verschlüsselt)

Gerade, wer viele E-Mails verwalten muss, wird sich an IMAP erfreuen können. IMAP funktioniert hervorragend sowohl mit deinem E-Mail-Client als auch mit dem Webmailer (siehe Kapitel 4.5).

## **4.3 Ausgehende Post**

Das Versenden von E-Mails erfolgt über einen SMTP-Server. Da es hier keine großartigen Alternativen gibt, seien hier lediglich die Serverdaten genannt.



### **SMTP-Server**

Zum Versenden von E-Mails.

Servername: **rinux.net**

Port: 25 (unverschlüsselt), 465 (verschlüsselt)

## 4.4 E-Mail-Empfang und -Versand absichern

Bei den jeweiligen Server-Details findest du fast immer zwei Port- oder Adressenangaben. Der Vermerk *unverschlüsselt* bedeutet dabei, dass die Verbindung zum Server ungesichert stattfindet. Sollte es jemandem gelingen, die Kommunikation zwischen deinem Computer und Rinux mitzuhören, so kann dieser Dritte unter Umständen dein Passwort herausfinden. Um dem zu entgegnen, kannst du die Verbindung absichern.

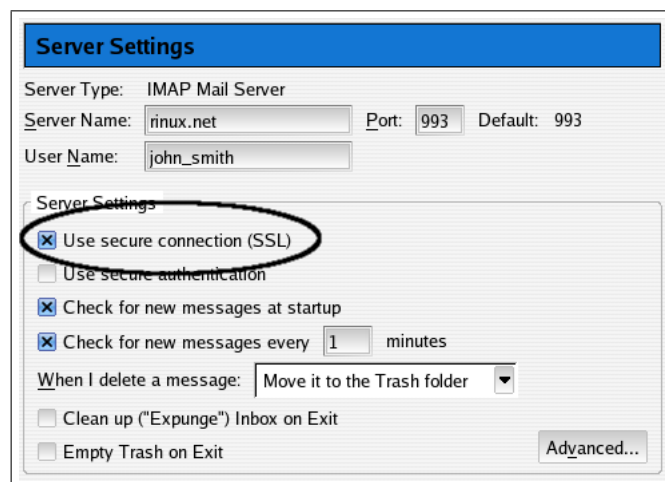


Abbildung 4.1: Servereinstellungen in Thunderbird: Verbindung zum *E-Mail-Empfang* absichern

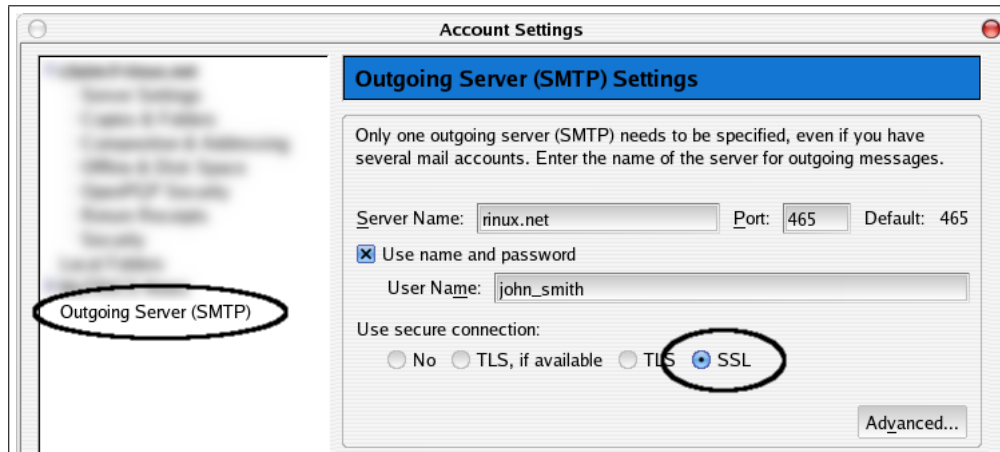


Abbildung 4.2: Servereinstellungen in Thunderbird: Verbindung zum *E-Mail-Versand* absichern

Die meisten E-Mail-Programme bieten dazu eine Funktion an, die (wie in Abb. 4.1 am Beispiel Thunderbird) entsprechendes veranlasst.

Zu beachten: Für die Absicherung des Mailversands sind oft zusätzliche Einstellungen nötig (in Thunderbird gemäß Abb. 4.2).



Das Absichern der Verbindung zum Server bewirkt lediglich, dass dein Passwort sehr viel schwerer abzuhören ist. Während deine E-Mail im Internet unterwegs ist, ist sie weiterhin für Dritte offen lesbar. Wenn dir das nicht behagt, ist E-Mail-Verschlüsselung mit GPG das Richtige für dich (mehr dazu in Kapitel 4.7).

## 4.5 Der Webmailer

Oft verfügt man unterwegs zwar über einen Internetzugang - etwa in Internet-Cafés oder an Internet-Terminals in Hochschulen - möchte oder kann aber keinen E-Mail-Client einrichten bzw. benutzen. In diesem Fall bietet es sich an, den Webmailer zu benutzen, da hierfür lediglich ein Web-Browser benötigt wird.



### Webmailer

Über einen Browser E-Mails lesen und verschicken.

Servername: `http://smail.rinux.net` (verschlüsselt),  
`http://mail.rinux.net` (unverschlüsselt)

### 4.5.1 Sprache einstellen

Vielleicht solltest du als erstes die Sprache des Webmailers ändern, falls du große Schwierigkeiten mit der englischen Sprache hast. Beachte aber bitte, dass der Rest der Anleitung für den Webmailer sich auf die englischen Menübeschriftungen bezieht.

Die Sprache kannst du nach einem Klick auf *Options* (oberer Rand des Webmailer-Fensters) unter *Display Preferences* einstellen. Dort gibt es eine Aufklappbox mit den verfügbaren Sprachen.

### 4.5.2 Identitäten verwalten

Der auf Rinux verwendete Webmailer unterstützt mehrere Identitäten pro Benutzer. Das ist beispielsweise interessant für diejenigen, die mehr als eine E-Mail-Adresse auf Rinux haben und mit diesen verschiedenen Absenderadressen Mails versenden möchten. Doch auch, wer nur eine Adresse hat, sollte hier kurz vorbeischaun, um zumindest seinen Namen (und eventuell eine Signatur) zu hinterlassen.

Logge dich unter der in Kapitel 4.5 genannten Adresse ein und rufe das Optionenmenü auf (siehe auch Abb. 2.2). Dort wählst du den Punkt *Personal Information*. Hier sollten zumindest die Felder *Full Name* und *EMail Address* ausgefüllt werden. Wenn du möchtest, kannst du

natürlich auch eine Signatur eintragen, die dann gemäß der *Signature Options* (weiter unten auf der Seite) unter von dir verfasste E-Mails gesetzt wird.



Die Signaturen, die du im Webmailer verwendest, haben keinen Einfluss auf E-Mails, die du in deinem E-Mail-Programm schreibst. Sie gelten nur für Mails, die du im Webmailer verfasst.

Für diejenigen nun, die mehr als eine Absenderadresse verwalten möchten, sollte *Edit Advanced Identities* interessant klingen. Nach einem Klick auf diesen Link erscheint eine Seite, in der man zusätzlich zu der eben sichtbaren Identität weitere Identitäten hinzufügen kann. Dazu trägt man in das Formular am unteren Ende der Seite die Daten für eine neue Absenderadresse ein und klickt auf *Save / Update*. Die gleichnamigen Buttons unter den schon eingetragenen Identitäten beziehen sich im Übrigen immer nur auf die direkt darüber stehende Identität. Bearbeite also immer nur eine Identität und speichere die Änderungen, bevor du eine andere modifizierst.

### 4.5.3 Ordner verwalten

Wie bereits erwähnt, kann man mit IMAP (und auch im Webmailer) mehrere Ordner für die Verwaltung von E-Mails benutzen. In der Navigationsleiste am oberen Rand des Webmailers wählst du dazu den Eintrag *Folders*.

Es baut sich eine Seite auf, die es dir erlaubt, neue Ordner anzulegen, bestehende Ordner umbenennen oder zu löschen oder die Liste mit den abonnierten Ordnern (*Subscribed folders*) zu bearbeiten. Bei der Erstellung eines Ordners musst du dich entscheiden: Soll der neue Ordner E-Mails oder weitere Unterordner aufnehmen können? Beides zur selben Zeit ist nicht möglich.

## 4.6 Spam- und Virenschutz

Spam ist E-Mail-Alltag - kaum ein elektronisches Postfach bleibt von unerwünschter Werbung verschont. Um dem zu entgegnen, setzt der Rlinux-Mailserver auf SpamAssassin<sup>2</sup>, eine Filter-Software, die anhand eines ausgefeilten Kriteriensatzes versucht, Spam-typische E-Mails zu markieren. Anhand dieser Markierung kann man später leichter gute von schlechten E-Mails unterscheiden.

Um dich und andere vor den immer häufiger auftretenden E-Mail-Plagen wie Würmern oder Trojanischen Pferden<sup>3</sup> zu schützen, begutachtet ein Virens Scanner alle eingehenden und abgehenden E-Mails.

E-Mails nicht zuzustellen (nach welchen Kriterien auch immer) bedeutet immer auch, dass möglicherweise harmlose E-Mails nicht das Zielpostfach erreichen. Daher wird in der Grundeinstellung

<sup>2</sup>Homepage: <http://spamassassin.apache.org>

<sup>3</sup>vgl. <http://de.wikipedia.org/wiki/Computervirus>

alles - bis auf durch den Virenschanner als infiziert eingestufte Mails - in dein Postfach durchgelassen. Dort sollst du selbst entscheiden, wie hart du gegen unerwünschte Post vorgehst.

### 4.6.1 Spam-Einstufung anpassen

In den meisten Fällen wird die Standardeinstellung von SpamAssassin ausreichenden Schutz bieten. Falls du jedoch unter der Last von zu viel Spam zu ersticken drohst, findest du hier ein paar Tipps.

Zunächst solltest du beobachten, welcher Art die Spam-Mails sind, die du bekommst. Damit ist gemeint, dass du dir in deinem E-Mail-Programm alle Kopfzeilen dieser Mails ansehen und nach einer Zeile, die mit `X-Spam-Status` beginnt, Ausschau halten solltest. Solch eine Zeile sieht in etwa so aus:

```
X-Spam-Status: Yes, score=5.3 required=5.0 tests=BAYES_99, RCVD_HELO_IP_MISMATCH,
RCVD_NUMERIC_HELO autolearn=no version=3.0.2
```

Was man daraus lesen kann:

**Yes, score=5.3 required=5.0** - Das bedeutet, dass die E-Mail als Spam eingestuft wurde, weil sie den *required*-Wert von 5.0 mit einer Trefferzahl von *score*=5.3 um 0.3 Punkte überschritten hat.

**test=...** - Es folgt eine Liste mit Namen von Kriterien, die auf diese E-Mail zutreffen.<sup>4</sup>

**autolearn=no** - Gemäß der bisher verarbeiteten E-Mails kann es sein, dass SpamAssassin versucht, auch aus dieser Mail für zukünftige Mails zu lernen. In diesem Fall passiert das nicht. Steht dort *ham* statt *no* (wie im obigen Beispiel), so lernt SpamAssassin von dieser Mail Dinge über gute Mails, steht dort *spam*, so lernt das Programm über schlechte Mails.

**version=3.0.2** - Das ist die Version der SpamAssassin-Software, die die Überprüfung der Mail durchgeführt hat.

Im Webmailer kannst du dir bei jeder E-Mail, die du liest, beliebige Kopfzeilen anzeigen lassen, so auch `X-Spam-Status`. Dazu musst du lediglich unter *Options* im Untermenü *Display Preferences* in das Textfeld ganz unten (*Show Headers (One Per Line)*) `X-Spam-Status` eintragen, wie in Abb. 4.3 gezeigt.

Ein erster Ansatzpunkt ist, die Gewichtung für häufig auftretende Kriterien hochzusetzen. Tritt beispielsweise in jeder E-Mail das Kriterium `TO_EMPTY` (keine Empfängerangabe) auf, so könnte man die Gewichtung für dieses Kriterium etwa auf 4.0 heraufsetzen.

---

<sup>4</sup>Die komplette Liste der Kriterien mit kurzer Beschreibung und Standard-Punktezahl findet sich unter [http://spamassassin.apache.org/tests\\_3.0.x.html](http://spamassassin.apache.org/tests_3.0.x.html)

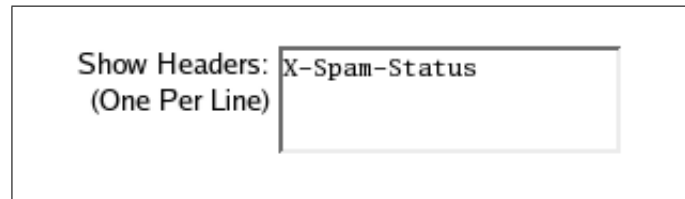


Abbildung 4.3: Im Webmailer: Zusätzliche Kopfzeilen anzeigen lassen

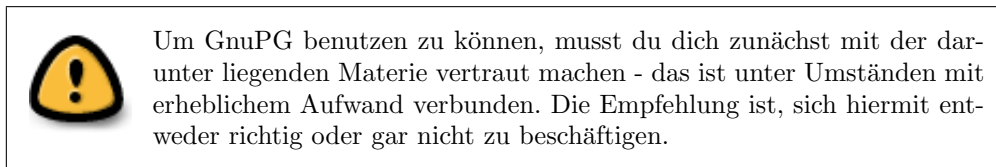
Das kann man im Konfigurationsmenü (siehe auch Kapitel 3) tun. Einloggen, die Kategorie *Settings & Tools* auswählen, dort auf *Custom Commands* klicken und danach *Edit SpamAssassin configuration* wählen. Es erscheint ein Editor-Fenster mit der bestehenden SpamAssassin-Konfiguration für deinen Account. Dort fügst du am Ende der Datei die folgende Zeile ein:

```
score TO_EMPTY 4.0
```

Ab der nächsten ankommenden E-Mail wird dieses Kriterium höher bewertet.

Um automatisch schon auf der Serverseite E-Mails wegzusortieren oder gar wegzuworfen, musst du entsprechende Filterregeln erstellen. Das wird in Kapitel 4.11 erklärt.

## 4.7 Verschlüsselte E-Mails mit GnuPG



E-Mails, die du verschickst, sendest du von deinem Computer an den Rinux-Mailserver (oder du übergibst sie fast direkt an den Mailserver, wenn du den Webmailer verwendest). Da die E-Mail dann aber erst noch den Weg zum eigentlichen Adressaten finden muss, wird sie noch einige andere Mailserver besuchen, bevor sie im Postfach des Empfängers landet.

Auf diesem Weg wird die E-Mail im Klartext weitergereicht und ist somit für Angreifer ohne Probleme lesbar. Wenn du sichergehen willst, dass der Inhalt der Mail ein Geheimnis zwischen dir und dem Empfänger bleibt, müsst ihr beide GnuPG benutzen.

GnuPG erschöpfend zu beschreiben, sprengt den Rahmen des Rinux Manual. Statt dessen sei an dieser Stelle auf das *GNU Handbuch zum Schutze der Privatsphäre*<sup>5</sup> verwiesen.

Im Webmailer (unter *Options, GPG Plugin Options*) gibt es die Möglichkeit, entsprechende Einstellungen vorzunehmen, um von den Verschlüsselungs- und Signaturoptionen zu profitieren.

<sup>5</sup><http://www.gnupg.org/gph/de/manual>

Um auf deinem Rechner (und damit auch mit deinem E-Mail-Programm) GnuPG zu verwenden, musst du zunächst GnuPG selbst installieren<sup>6</sup>. Danach musst du deinem E-Mail-Programm beibringen, mit verschlüsselten oder signierten E-Mails umzugehen. Für Thunderbird bietet sich das Plugin *Enigmail*<sup>7</sup> an.

### 4.8 Weiterleitung

Obwohl Rinux eigentlich alles bietet, um problemlos mit E-Mails zu hantieren, kannst du natürlich die auf Rinux für dich ankommenden E-Mails an eine andere Adresse weiterleiten lassen.

Das geht am einfachsten über das Konfigurationsmenü. Dort findest du in der Kategorie *E-Mail* die Option *Mail Forwarding* - dort fügst du eine neue Weiterleitungsregel hinzu (*Add a mail forwarding rule*).

In der Auswahlbox entscheidest du dich für *Email address* und trägst in das Feld daneben die Ziel-Adresse ein (etwa Abb. 4.4). Das Ganze bestätigst du dann mit einem Klick auf *Save*.

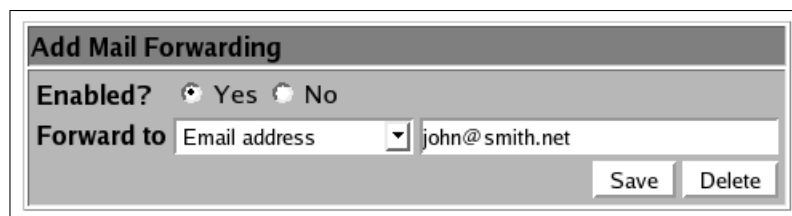


Abbildung 4.4: Option zum Weiterleiten von E-Mails im Konfigurationsmenü (2. Schritt)

### 4.9 Mailinglisten

Mailinglisten sind eine nützliche Sache, falls per E-Mail innerhalb einer Gruppe diskutiert werden soll. Der Weg ohne Mailinglisten sieht dabei so aus, dass jeder, der an dieser Diskussion teilnimmt, alle Adressen der anderen Empfänger in seinem E-Mail-Adressbuch verwalten muss. Beim Versand der Mail müssen dann alle diese Empfänger angegeben werden.

Hier können Mailinglisten helfen und die Kommunikation vereinfachen. Auf Rinux wird eine Liste angelegt, in die alle Adressaten eingetragen werden. Wer nun an alle schreiben möchte, schreibt statt dessen an die Adresse der Mailingliste. Die Software, die die Mailinglisten verwaltet, verteilt dann diese eingehende Mail automatisch an alle eingetragenen Adressaten.

Es gibt öffentliche Listen, auf die sich jeder eintragen kann und fortan ebenfalls Mails erhält, die an diese Liste gehen. Auf der anderen Seite gibt es auch geschlossene Listen, die die möglichen Adressaten einschränken oder nur bestimmte Absender erlauben.

<sup>6</sup>Weitere Informationen und Downloads unter <http://www.gnupg.org>.

<sup>7</sup>Informationen und Download auf <http://enigmail.mozdev.org>.



### Mailinglisten

E-Mails in Gruppen austauschen

Server: <http://whiletrue.de/mailman>

Mailinglisten werden von whiletrue.de verarbeitet, einem virtuellen Server, der ebenfalls zu Rlinux gehört. Die Adressen bleiben also sozusagen in der Familie.

Mailinglisten kannst du nicht selbst einrichten, sie müssen vielmehr von mir angelegt werden. Falls du interessiert bist, selbst eine Mailingliste zu betreuen (keine Angst, das ist in der Regel kaum Arbeit), schreibe eine E-Mail an [hosting@rlinux.net](mailto:hosting@rlinux.net) und beschreibe kurz, wofür du die Liste benutzen möchtest.

## 4.10 Post von anderen Servern abholen (*fetchmail*)

Manche FreeMail-Anbieter haben diese Funktion auch POP3-Sammeldienst genannt. Du kannst Post von anderen Servern abholen, auf denen du auch einen E-Mail-Account hast.

### 4.10.1 Serverprofile erstellen

Dazu gehst du in das Konfigurationsmenü und wählst in der Kategorie *E-Mail* die Funktion *Fetchmail Mail Retrieval* aus. Dort kannst du eine ganze Reihe von Serverprofilen anlegen (*Add a new server*), von denen du E-Mails abholen möchtest. Abbildung 4.5 zeigt ein Beispielprofil.

Im Feld *Server name* kann ein beliebiger Name eingetragen werden, oder direkt der tatsächliche Name des Mailserver. Falls man diesen dort nicht direkt vergeben will, muss wie abgebildet in der Zeile darunter (*Mail server to contact*) die Option neben dem Textfeld gesetzt und in das Feld der eigentliche Servername eingetragen werden.

Die Option *Polling enabled* entscheidet, ob das Abrufen für dieses Profil aktiviert sein soll. Darüber kannst du für ein bestimmtes Profil die Abholung unterbrechen.

Als nächstes sind Login-Informationen für den gerade eingegebenen Mailserver einzutragen. Dazu muss im Feld *Protocol* (in der Regel) POP3 oder IMAP ausgewählt werden. Als *Authentication method* wird in den meisten Fällen „PASSWORD“ richtig sein. Im Zweifelsfall hilft eine Nachfrage nach den angebotenen Authentisierungsmechanismen beim Anbieter des anderen Servers. *Check condition* muss in jedem Fall auf „Always Check“ stehen.

Jetzt geht es an die eigentlichen Login-Daten. Im Feld *Remote user* und *Remote password* trägst du den Usernamen und das Passwort für den anderen Mailserver ein. In das Feld *Local user(s)* gehört nun noch deine E-Mail-Adresse auf Rlinux, an die die eingesammelten Mails zugestellt werden sollen.

Add Server

**Mail server options**

<b>Server name</b>	<input type="text" value="oldserver.com"/>	<b>Polling enabled?</b>	<input checked="" type="radio"/> Yes <input type="radio"/> No
<b>Mail server to contact</b>	<input type="radio"/> Same as server name <input checked="" type="radio"/> <input type="text" value="pop.oldserver.com"/>		
<b>Protocol</b>	<input type="text" value="POP3"/>	<b>Server port</b>	<input checked="" type="radio"/> Default <input type="radio"/> <input type="text"/>
<b>Authentication method</b>	<input type="text" value="PASSWORD"/>		
<b>Check condition</b>	<input checked="" type="radio"/> Always check		
	<input type="radio"/> Only if interface is up <input type="text"/> with address / netmask <input type="text"/> / <input type="text"/>		

**Mail server user details**

<b>Remote user</b>	<input type="text" value="john_smith1882"/>	<b>Remote password</b>	<input type="text" value="*****"/>
<b>Local user(s)</b>	<input type="text" value="john_smith@rinux.net"/>		
<b>Leave messages on server?</b>	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Default (Usually no)		
<b>Always fetch all messages?</b>	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Default (Usually no)		
<b>Connect in SSL mode?</b>	<input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> Default (Usually no)		
<b>Command to run before connecting</b>	<input type="text"/>		
<b>Command to run after disconnecting</b>	<input type="text"/>		

Abbildung 4.5: Fetchmail: Ein neues Serverprofil anlegen



Obwohl bei *Local user(s)* eigentlich nach einem Benutzernamen gefragt wird, genügt es nicht, hier nur deinen Accountnamen einzutragen. Du musst hier unbedingt deine vollständige E-Mail-Adresse auf Rinux angeben.

Schließlich kannst du einstellen, ob eingesammelte Mails auf dem Server bleiben sollen (speziell für POP3 interessant, siehe auch Kap. 4.2.1), ob du jedes mal alle Nachrichten einsammeln möchtest und ob du die Verbindung zum anderen Mailserver verschlüsseln lassen willst (*Connect in SSL mode?*).

Nachdem die entsprechenden Felder befüllt wurden, bestätigst du das neue Serverprofil mit einem Klick auf *Create*.

Im Beispiel aus Abb. 4.5 werden vom Mailserver `pop.oldserver.com` über das POP3-Protokoll alle neuen E-Mails für den User `john_smith1882` eingesammelt und an die Rinux-Adresse `john_smith@rinux.net` zugestellt. Das Profil ist aktiv, die Mails werden nach der Abholung gelöscht, und die Verbindung zum anderen Mailserver erfolgt unverschlüsselt.

### 4.10.2 Bearbeiten und Löschen von Serverprofilen

Im Menü *Fetchmail Mail Retrieval* kannst du ein bereits angelegtes Profil auswählen (auf den entsprechenden Servernamen unter *Server to poll* klicken) und bearbeiten oder mit dem Button *Delete* wieder löschen.

### 4.10.3 Automatisches Abholen veranlassen

Falls du nur sehr selten E-Mails auf den zum Einsammeln eingetragenen Servern erhältst, genügt es, wenn du hin und wieder im Menü *Fetchmail Mail Retrieval* auf *Check all servers* klickst.

Meist wird es aber zweckmäßiger sein, automatisch die neuen Mails einzusammeln. Dazu musst du im *Fetchmail*-Menü auf *Scheduled Checking* klicken, um einen sogenannten *Cron-Job* zu erstellen - das ist eine Aufgabe, die zu bestimmten Zeiten regelmäßig ausgeführt wird.

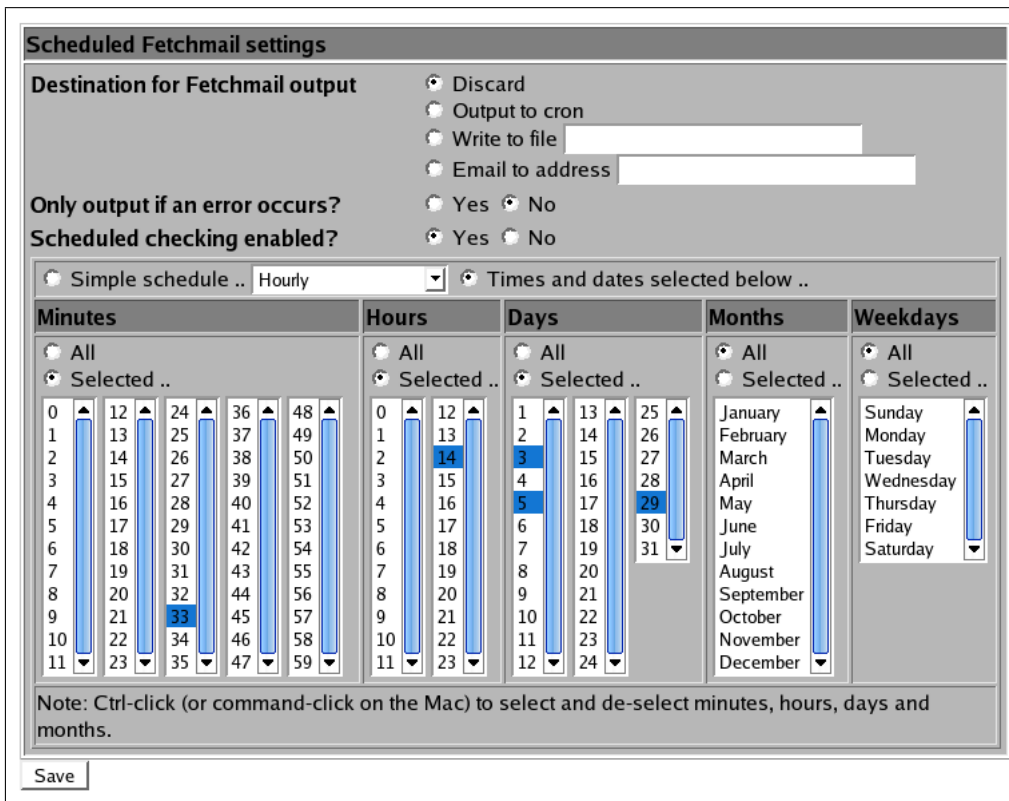


Abbildung 4.6: Fetchmail: Automatische Abholung mit Cron-Job

In Abb. 4.6 wird ein Cron-Job erstellt, der jeweils am 3., 5. und 29. eines Monats um 14:33 Uhr E-Mails von den eingetragenen Servern abholt. Monate und Wochentage sollen nicht berücksichtigt werden, deswegen stehen diese Optionen auf „All“<sup>8</sup>.

<sup>8</sup>Die merkwürdige Reihenfolge in diesen Feldern ist halb technisch, halb historisch bedingt.

*Destination for Fetchmail output* sollte auf „Discard“ stehen, *Only output if an error occurs* sollte deaktiviert sein. Damit dieser Cron-Job tatsächlich ausgeführt wird, muss *Scheduled checking enabled?* eingeschaltet sein.

Für einfachere Ausführungsintervalle könnte die Aufklappbox neben *Simple schedule* schon passende Optionen anbieten. Soll die genaue Spezifizierung der Termine im unteren Teil benutzt werden, muss die Option *Times and dates selected below ..* benutzt werden. Gespeichert wird der Eintrag wie üblich mit *Save*.

### 4.11 Sortieren und Filtern (procmail)

In vielen Fällen ist es sicher hilfreich, wenn die E-Mails auf dem Server sortiert werden. Paradebeispiele für diese Anwendung sind zum Einen das Wegwerfen unerwünschter E-Mails oder zum Anderen das Verschieben von E-Mails in Unterordner, die einer Einteilung nach Kategorien entsprechen. So könnte man zum Beispiel alle Mails von einem bestimmten Absender in den Ordner „Chef“ legen.



Bei der automatischen Filterung von E-Mails solltest du äußerst behutsam vorgehen! Wenn du hier zu eilig „Wegwerf-Regeln“ erstellst, ist beinahe garantiert, dass du E-Mails aussortierst, die du eigentlich bekommen möchtest. Teste jede neue Regel erst, bevor du weitere erstellst.

Das Programm, das uns bei dieser Aufgabe hilft, ist Procmail. Alle ankommenden Mails werden auch an Procmail weitergereicht - selbst, wenn du gar keine Filterregeln erstellt hast. In diesem Fall erfolgt keine Filterung oder Sortierung.

Wie bei den anderen Verwaltungsoptionen für E-Mails gibt es auch hierfür eine Funktion im Konfigurationsmenü: *Procmail Mail Filter* in der Kategorie *E-Mail*.

Dort fügst du nun eine neue Filterregel hinzu. Es erscheint ein Formular wie in Abb. 4.7 (die irrelevanten Teile des Formulars sind weggeschnitten).

Die wichtigen Felder sind hier markiert. Oben bei *Delivery mode* musst du auswählen, was mit einer Mail geschehen soll, die von der weiter unten angegebenen Bedingung erfasst wird. Du könntest beispielsweise alle E-Mails von einer bestimmten Absenderadresse an eine andere Adresse automatisch weiterleiten lassen. Wir entscheiden uns hier jedoch für die Option „Append to file“. Damit hängen wir die entsprechende E-Mail an eine bestehende Datei an. Da alle deine Ordner (bis auf die, die weitere Ordner aufnehmen können) Dateien sind, musst du dich jetzt nur noch entscheiden, in welchen Ordner du die Mail ablegen willst.

Das Beispiel in Abb. 4.7 legt alle eintreffenden E-Mails, die von SpamAssassin als Spam markiert wurden (siehe auch Kap. 4.6), in den Ordner „Spam“. Alle E-Mail-Ordner liegen direkt in deinem Home-Verzeichnis (bis auf die verschachtelten natürlich). Daher ergibt sich hier der Dateiname „/home/john.smith/Spam“.

Abbildung 4.7: Procmail: Eine Filterregel anlegen bzw. bearbeiten

Als Bedingung (*Action conditions*) wählst du nun „Matches regular expression“ und trägst in das Textfeld die zunächst mystisch anmutende Zeichenfolge `^X-Spam-Flag: YES$` ein. Die Formulierung entspricht einem sogenannten *regulären Ausdruck*<sup>9</sup>. Das Zeichen `^` steht dabei für den Zeilenanfang. Der Text `X-Spam-Flag: YES` danach beschreibt den eigentlichen Inhalt der Zeile. Da die Zeile, nach der wir suchen, danach zu Ende ist, steht schließlich noch das Dollarzeichen dort - für das Zeilenende.

Ist die Regel erstellt, wird sie in der Liste der Procmail-Regeln angezeigt. Dort finden wir in Abb. 4.8 noch eine weitere Regel.

Action to take	Conditions	Move	Add
<a href="#">Append to file /dev/null</a>	Match regexp ^X-Spam-Level:  \* \* \* \* \* \*.*	↓	↑ ↓
<a href="#">Append to file /home/john_smith/Spam</a>	Match regexp ^X-Spam-Flag: YES\$	↓ ↑	↑ ↓

Abbildung 4.8: Procmail: Liste der schon erstellten Filterregeln

Zusammen ergeben die beiden Regeln folgenden Sinn: Zunächst werden alle E-Mails, die bei der Spam-Prüfung sechs oder mehr Punkte bekommen haben, weggeworfen. Das Anhängen an die Datei `/dev/null` - den Mülleimer auf dem Server - bewirkt, dass die E-Mail verworfen wird. Alle anderen E-Mails, die zwar nicht mehr als sechs Punkte bekommen haben, aber dennoch Spam sind, sollen zur Begutachtung in den Spam-Ordner verschoben werden.

Weitere Tipps zu ausgefuchster Procmail-Konfiguration finden sich zum Beispiel unter <http://www2.uibk.ac.at/zid/systeme/mail/procmail>.

<sup>9</sup>Diese Ausdrücke spielen unter Unix-Betriebssystemen an vielen Stellen eine wichtige Rolle. Als Einstiegslektüre sei <http://www.lrz-muenchen.de/services/schulung/unterlagen/regul> empfohlen.




## 5 Webservice

Dieses Kapitel soll dir zeigen, welche Möglichkeiten du nutzen kannst, um deine Ideen ins Web zu bringen und welche unterstützenden Technologien auf Rinux angeboten werden.

### 5.1 Dateien hochladen (ftp)

Zunächst ist es sicher interessant zu wissen, wie du die Dateien deiner Homepage auf den Rinux-Webserver hochladen kannst. Die bekannteste und einfachste Möglichkeit, dies zu erledigen, ist mittels FTP.




**FTP-Server**  
Dateien in dein Home-Verzeichnis auf Rinux übertragen.

Server: `rinux.net`  
Port: 21 (nur unverschlüsselt)

Du brauchst dazu lediglich einen FTP-Client. Leider gibt es zumindest für Windows-Systeme nur ein sehr eingeschränktes Angebot an Programmen dieser Art. LeechFTP ist kostenlos<sup>1</sup>, CuteFTP Home<sup>2</sup> (USD 39,99) und WS\_FTP Home<sup>3</sup> (USD 34,95) dagegen nicht.

Für Linux-Systeme hingegen empfehlen sich einige, komfortable Konsolenprogramme, so etwa der Midnight Commander, der einiges an FTP-Funktionalität bereits beinhaltet, daneben `ncftp` als komfortable Alternative zum eher spröden und umständlichen Standard-`ftp`. Letztlich gibt es auch noch `gftp`, das in der Bedienung stark an WS\_FTP erinnert (für GNOME).



Beim FTP-Zugriff auf deinen Rinux-Account startest du nicht in deinem eigentlichen Home-Verzeichnis, sondern im Unterverzeichnis `public_html`.

<sup>1</sup>Homepage: <http://stud.fh-heilbronn.de/~jdebis/leechftp>

<sup>2</sup>Homepage: <http://www.globalscape.com/cuteftp>

<sup>3</sup>Homepage [http://www.wsftp.com/products/WS\\_FTP/home](http://www.wsftp.com/products/WS_FTP/home)

## 5.2 Dynamische Webseiten mit PHP

Bei PHP handelt es sich um eine Skript-Sprache, mit der du dynamische Webseiten erstellen kannst. Das eröffnet zum einen die Möglichkeit, eigene Seiten zu entwickeln, die selbstgeschriebene PHP-Skripte benutzen, zum anderen kannst du damit auch fertige Lösungen für deine Homepage verwenden. Beispiele für solche bereits verfügbaren Skriptsammlungen sind Wiki-Systeme<sup>4</sup> oder Content-Management-Systeme<sup>5</sup>.

Letztere vereinfachen die Wartung einer Webseite, sodass nach einer anfänglichen Einrichtung des Systems der Schwerpunkt auf die Erstellung und Bearbeitung von Inhalten gelegt werden kann. Das ermöglicht unter anderem auch Autoren, die keinerlei HTML- oder PHP-Kenntnisse haben, an einer Webseite mitzuwirken, da sich deren Arbeit im Wesentlichen auf das Ausfüllen von Web-Formularen beschränkt.



Rinux verwendet ausschließlich PHP in der Version 5. Viele Skripte und Skriptsammlungen, die auf frühere PHP-Versionen ausgelegt sind, funktionieren wegen grundlegender Änderungen in Version 5 nicht mehr. In vielen Fällen haben die Entwickler dieser Skripte schon die entsprechenden Anpassungen vorgenommen oder bieten Hilfe an.

Das Rinux-Webhosting wird keinesfalls für „problematische“ Skripte abweichende Regelungen treffen. Entweder die Skripte arbeiten korrekt unter PHP5 oder sie werden nicht auf Rinux laufen.

## 5.3 MySQL-Datenbanken benutzen und verwalten

Mit dem MySQL-Server auf Rinux steht dir ein Datenbanksystem zur Verfügung, das zu den beliebtesten SQL-Varianten gehört. Viele PHP-Lösungen setzen auf eine MySQL-Anbindung zur Verwaltung der anfallenden Daten.



### MySQL-Server

SQL-basiertes Datenbanksystem.

Server: localhost


Username/Passwort sind separat vom Systemaccount.

Auf den MySQL-Server kann nicht von außerhalb zugegriffen werden. Alle Anwendungen, die MySQL benutzen, müssen auf Rinux laufen.

<sup>4</sup> u.a. PHPWiki: <http://phpwiki.sourceforge.net>

<sup>5</sup> u.a. phpCMS: <http://www.phpcms.de>

Die Verwaltung deiner MySQL-Datenbank kannst du per PHPmyAdmin vornehmen. Auf PHPmyAdmin kannst du mit einem Browser zugreifen.




**PHPmyAdmin**  
MySQL-Datenbank und -Tabellen verwalten.

Server: <http://sdb.rinux.net>  
Für Username und Passwort die MySQL-Zugangsdaten verwenden.

Du musst auf den Port 444 auf fremden Rechnern zugreifen können, um PHPmyAdmin zu verwenden.

Solltest du PHPmyAdmin nicht benutzen können, kannst du auf das Konfigurationsmenü ausweichen. Dort findest du in der Kategorie *Settings & Tools* die Option *MySQL Database Server*, wo du zunächst deine Zugangsdaten eintragen musst. Diese Konfigurationmöglichkeit ist jedoch eher als Notlösung einzustufen.



Deine Zugangsdaten zum Datenbank-Server (und zu PHPmyAdmin) sind vollkommen unabhängig von den Zugangsdaten, die du sonst verwendest. Falls du diese Zugangsdaten nicht weißt oder vergessen hast, hilft nur eine E-Mail an [hosting@rinux.net](mailto:hosting@rinux.net).

## 5.4 Skripte mit CGI und SSI

Neben PHP gibt es noch andere Möglichkeiten, dynamische Webseiten zu bauen oder Webanwendungen zu entwickeln.

### 5.4.1 Common Gateway Interface (CGI)

Manche Webseiten-Software wird mit anderen Skriptsprachen als PHP entwickelt. Typischerweise handelt es sich dabei um Perl-, Python- oder Ruby-Skripte, die als CGI<sup>6</sup> ausgeführt werden. Auch diese Lösungen kannst du auf Rinux nutzen - oder selbst entwickeln.

Movable Type<sup>7</sup> ist beispielsweise ein Content-Management-System ähnlich phpCMS, das aber in Perl entwickelt wurde und daher als CGI läuft.

<sup>6</sup>CGI: Beschreibung z.B. unter <http://www-user.tu-chemnitz.de/~fischer/cgi/intro.html>

<sup>7</sup>Homepage: <http://www.movabletype.com>



### CGI-Skripte

Dynamische Webseiten über Skript-Sprachen.

Auf manchen Webservern musst du CGI-Skripte in einem bestimmtem Verzeichnis unter deinem Home-Verzeichnis ablegen, um sie benutzen zu können. Für deine Homepage auf Linux ist es egal, wo du diese Dateien ablegst, wichtig ist jedoch, dass sie die Dateiendung `.cgi` tragen.

## 5.4.2 Server Side Includes (SSI)

Eine weitere Möglichkeit, deinen statischen HTML-Webseiten eine dynamische Note zu verleihen, ist, an bestimmten Stellen in diesen Dateien Befehle auszuführen.



### SSI in SHTML-Dateien

Statische Seiten um dynamische Elemente erweitern.

Damit der Server mit den in deine Seite eingebauten Befehlen umgehen kann, müssen HTML-Dateien, die SSI benutzen, die Endung `.shtml` tragen und als *ausführbar* markiert sein.

Weiterhin müssen die externen Befehle, die du ausführst, im selben Verzeichnis wie die `.shtml`-Datei liegen. Du kommst also in dem Fall nicht umhin, selbst Skripte zu schreiben.

Neben der Ausführung von nahezu beliebigen Befehlen bieten Server Side Includes noch weitere interessante Möglichkeiten, etwa das Einbinden des Inhalts einer anderen Datei, Anzeige des aktuellen Datums oder des Zeitpunkts der letzten Änderung an der aktuellen Datei<sup>8</sup>.

## 5.5 Teilbereiche mit einem Passwort schützen (.htaccess)

Obwohl deine Homepage im Prinzip für die ganze Welt erreichbar sein soll, möchtest du vielleicht einzelne Verzeichnisse oder Teilbereiche vor unbefugtem Zugriff schützen - zum Beispiel die neueste Kurzgeschichte oder deine geheime Tastenbelegung für den aktuellen Ego-Shooter.

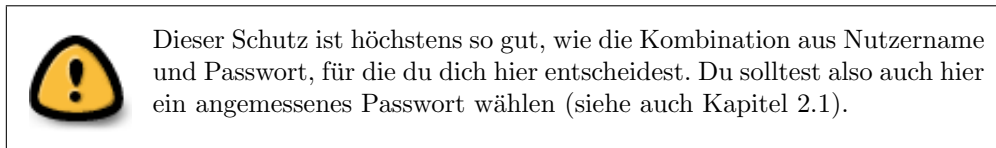
Am einfachsten kannst du einen derartigen Schutz über das Konfigurationsmenü einrichten. Dazu wählst du in der Kategorie *Settings & Tools* die Option *Protected Web Directories*. Dort klickst du zunächst auf den Button *Find existing directories...*, wobei in dem Textfeld daneben `/usr/home/DEIN_USERNAME` stehen sollte. Damit erfasst du in diesem Menü bereits bestehende Zugriffsbeschränkungen.

<sup>8</sup>Dokumentation (Englisch): <http://httpd.apache.org/docs-2.0/howto/ssi.html>

Als nächstes fügst du ein neues Verzeichnis zur Zugriffsverwaltung hinzu. Klick dazu auf *Add protection for a new directory*. In dem Menü, was danach erscheint, kannst du neben *Directory path* auf die drei Punkte klicken und das zu schützende Verzeichnis auswählen. Wähle dabei dein Homeverzeichnis unter `/usr/home/` aus. Danach vergibst du noch einen Namen für den Bereich (*Realm*) - ähnlich Abb. 5.1.

Abbildung 5.1: Einen neuen geschützten Bereich anlegen

Nach einem Klick auf *Create* landest du wieder in der Liste der eingerichteten Bereiche. Dort klickst du nun für das entsprechende Verzeichnis auf *Add a new user for this directory* und trägst in der darauf folgenden Seite einen Usernamen und ein Passwort ein; *Enabled* setzt du auf *Yes* (mit dieser Option kannst du zeitweilig einige User wieder aussperren, falls du sie nicht gänzlich entfernen möchtest).



## 5.6 Nutzungsstatistiken (AWStats)

Für deine Subdomains auf Rinix werden die Zugriffsprotokolle ausgewertet und daraus grafisch aufbereitete Statistiken generiert und zweimal täglich aktualisiert.

Beim Anlegen deiner Subdomains wurden auch die Statistiken eingerichtet. Du kannst sie ansehen unter

`http://rinix.net/awstats/awstats.pl?config=DEINE_SUBDOMAIN`

wobei du für *DEINE\_SUBDOMAIN* deine komplette Subdomain einsetzt, also zum Beispiel `johnsmith.rinix.net`.

## 5.7 Bildergalerie

Wenn du Bilder online stellen möchtest, musst du das nicht über deinen eigenen Account tun. Du kannst dazu das Rlinux-Galeriesystem benutzen, das du unter <http://gallery.rlinux.net> findest. Das hat unter anderem den Vorzug, dass die dort eingestellten Bilder nicht zum von dir verbrauchten Plattenplatz zählen.

Im Galeriesystem musst du dir als erstes einen Account anlegen, der nichts mit deinem sonstigen Rlinux-Account zu tun hat.



Verwende für deinen Account im Galeriesystem keinesfalls die gleichen Daten wie zum Login auf den anderen Diensten!

Danach schreibst du eine E-Mail an [hosting@rlinux.net](mailto:hosting@rlinux.net) mit dem Accountnamen, den du für das Galeriesystem gewählt hast. Ein Album wird dann für dich angelegt.

Details zur Benutzung des Systems findest du (auf Englisch) unter <http://makeashorterlink.com/?J271120DA><sup>9</sup>.

---

<sup>9</sup><http://gallery.menalto.com/modules.php?op=modload&name=GalleryDocs&file=index>