Avira AntiVir MailGate / Avira MailGate Suite

Handbuch für Anwender

AVIRA

Inhalt

1 Über dieses Handbuch

In diesem Kapitel finden Sie einen Überblick über den Aufbau und den Inhalt dieses Handbuchs.

Auf eine kurze Einleitung folgen Informationen zu den folgenden Themen:

1.1 Einleitung

In diesem Handbuch haben wir für Sie alle nötigen Informationen über Avira AntiVir MailGate zusammengestellt und führen Sie Schritt für Schritt durch die Installation, Konfiguration und Bedienung der Software.

Im Anhang finden Sie ein Glossar, in dem grundlegende Begriffe erläutert werden.

Weitere Informationen und Hilfestellungen bieten Ihnen darüber hinaus unsere Webseite, die Hotline unseres Technischen Supports und unser regelmäßiger Newsletter (Service – Seite 120).

Ihr Avira-Team

1.2 Aufbau des Handbuchs

Das Handbuch zu Ihrer Avira AntiVir MailGate-Software besteht aus mehreren Kapiteln, in denen Sie folgende Informationen finden:

Kapitel	Inhalt
1 Über dieses Handbuch	Aufbau des Handbuchs, Zeichen und Symbole
2 Produktinformationen	Allgemeine Hinweise zu Avira AntiVir MailGate, seinen Modulen, Leistungsmerkmalen und Systemanforderungen sowie zur Lizenzierung
3 Milter-Modus	Einführung des Milter-Modus in Avira AntiVir MailGate
4 Installation	Anweisungen zur Installation von Avira AntiVir MailGate auf Ihrem System
5 Konfiguration	Hinweise zur optimalen Anpassung der Avira AntiVir MailGate-Komponenten an Ihr System
6 Bedienung	Befehle und Parameter zum Ausführen des Scanners und des Warteschlangen-Managers; Vorgehen beim Erkennen von Viren und unerwünschten Programmen
7 Aktualisierungen	Aktualisierung per Internet und Intranet
8 Service	Avira GmbH Support und Service
9 Anhang	Glossar mit Erläuterungen von Fachbegriffen und Abkürzungen Goldene Regeln zum Schutz vor Viren

1.3 Zeichen und Symbole

Im Handbuch werden die folgenden Zeichen und Symbole verwendet:

Symbol	Bedeutung
✓	steht vor einer Voraussetzung, die vor dem Durchführen einer Maßnahme erfüllt sein muss.
▶	steht vor einem Schritt, der auszuführen ist.
↳	steht vor einem Ergebnis, das sich direkt aus der vorangegangenen Handlung ergibt.
	steht vor einem Alarm, wenn kritische Datenverluste oder Schäden an der Hardware drohen.

Symbol	Bedeutung
	steht vor einem Hinweis mit besonders wichtigen Informationen, die sich beispielsweise auf durchzuführende Schritte beziehen.
	kennzeichnet einen Tipp, der das Verständnis und die Bedienung von Avira AntiVir MailGate erleichtert.

Zur besseren Lesbarkeit und eindeutigen Kennzeichnung werden im Text außerdem folgende Hervorhebungen verwendet:

Hervorhebung im Text	Erläuterung
Strg+Alt	Tasten oder Tastenkombinationen
/usr/lib/AntiVir/mailgate	Pfadangaben und Dateinamen
`ls /usr/lib/AntiVir`	Benutzereingaben
Komponente auswählen Alles auswählen	Bestandteile der Software-Oberfläche, z. B. Menüoptionen, Fenstertitel oder Schaltflächen in Dialogfenstern
http://www.avira.com	URLs
Zeichen und Symbole – Seite 5	Querverweise innerhalb des Dokuments

1.4 Abkürzungen

In diesem Handbuch werden die folgenden Abkürzungen verwendet:

Abkürzung	Bedeutung
ACL	Access Control List
FAQ	Frequently Asked Question
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
MIME	Multipurpose Internet Mail Extensions
MTA	Mail Transport Agent
RFC	Request For Comment
SMTP	Simple Mail Transfer Protocol
VDF	Virus Definition File

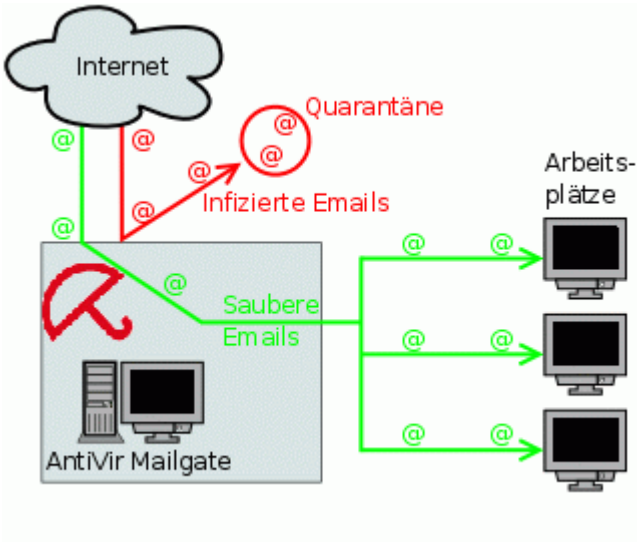
2 Produktinformationen

Die Dateiübertragung per Email ist zu einem festen Bestandteil der modernen Kommunikation geworden, und wir können uns ein Leben ohne diese Errungenschaft kaum noch vorstellen. Doch Emails übertragen häufig auch Viren oder unerwünschte Programme.

Viele dieser Viren und Programme wurden speziell für Angriffe auf Windows-Betriebssysteme entwickelt. UNIX-Systeme sind jedoch der gleichen Gefahr ausgesetzt, da Malware auch von UNIX-Mailservern übertragen wird. Cyber-Angreifer machen nutzen solche Gelegenheit gern, um in fremde Netzwerke einzudringen. Wenn Windows-Clients infiziert werden können, gilt dies auch für die Rechner der Kommunikationspartner.

Eine zunehmende Anzahl von Unternehmen und öffentlichen Einrichtungen baut inzwischen auf UNIX. Da hier auch freie Software eingesetzt wird, können die Betriebssysteme leicht zum Ziel von Virenprogrammierern werden. Virenschutz unter UNIX bleibt also auch in Zukunft ein Thema. Aus diesem Grund haben wir Avira AntiVir MailGate entwickelt.

Avira AntiVir MailGate prüft alle ein- und ausgehenden Emails (inklusive Anhang) auf Ihrem UNIX-Mailserver. Die Software arbeitet mit einer Vielzahl von Mail Transport Agents (MTAs) zusammen, z. B. mit Sendmail, Postfix, Exim, Qmail und ähnlichen Programmen. Viele bekannte Distributionen werden effektiv unterstützt – Red Hat, SuSE, Debian usw. (laut 2.4 Systemanforderungen).



Zwei besonders wichtige Hinweise gleich zu Beginn:

***Warnung**: Der Verlust wertvoller Daten hat meist dramatische Folgen. Auch die beste Virenschutzsoftware kann Sie jedoch nicht hundertprozentig vor Datenverlusten schützen.*

▶ *Legen Sie deshalb regelmäßig Backups Ihrer Dateien an.*

Ein Virenschutzprogramm ist nur dann zuverlässig und wirksam, wenn es aktuell ist.

▶ *Stellen Sie durch automatische Aktualisierungen sicher, dass Ihr Avira AntiVir MailGate stets auf dem neuesten Stand ist. In diesem Handbuch erfahren Sie, wie Sie dabei vorgehen.*

2.1 Leistungsmerkmale

Avira AntiVir MailGate unterstützt eine Vielzahl von Konfigurationseinstellungen, mit denen Sie den Email-Verkehr auf Ihrem System lückenlos überwachen können.

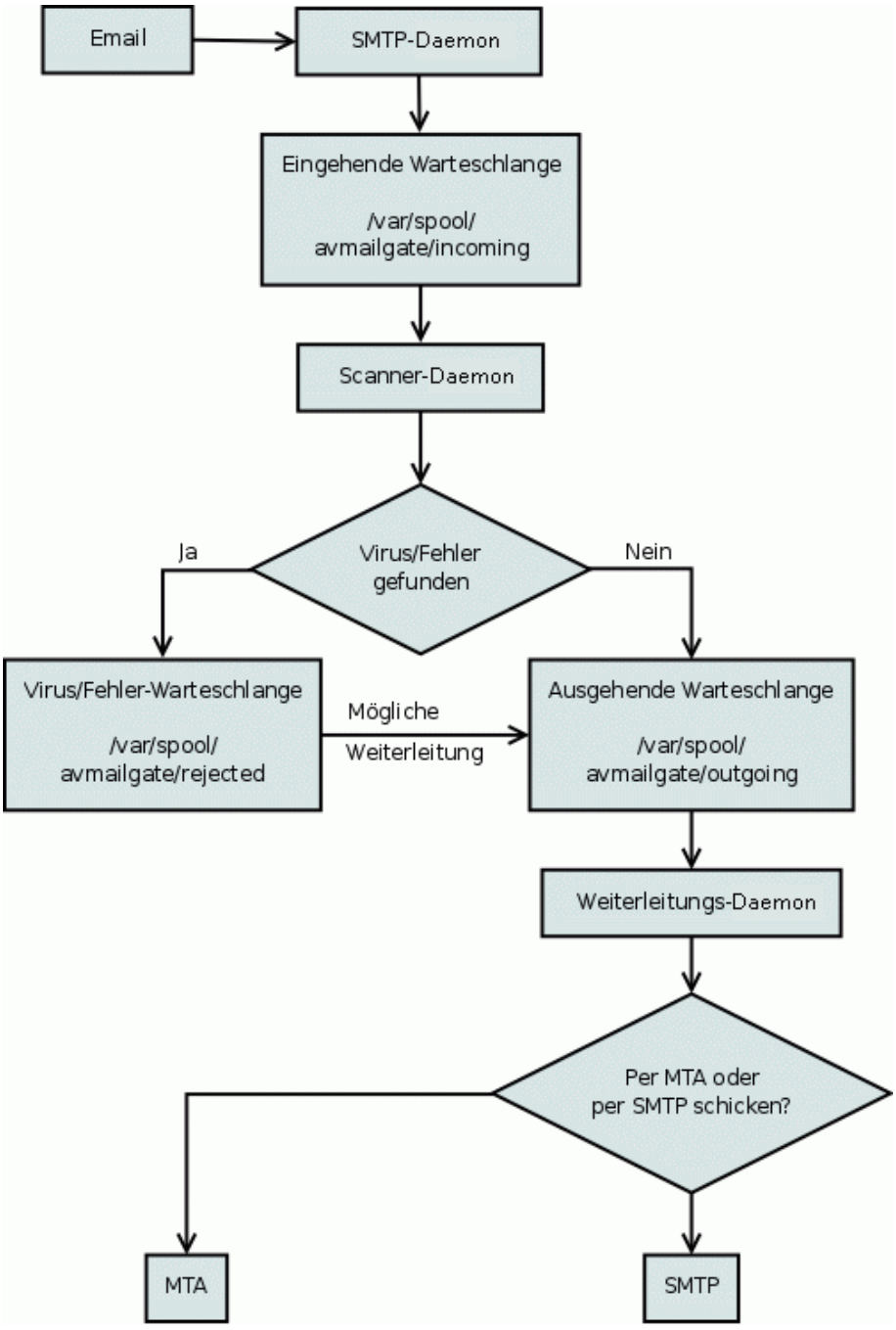
Die wichtigsten Leistungsmerkmale von Avira AntiVir MailGate:

- Echtzeitprüfung ein- und ausgehender Emails
- Prüfung auf Viren und unerwünschte Programme
- Konfigurierbarer Spam-Filter (in der **Avira MailGate Suite** enthalten)
- Prüfung von Mailboxen
- Isolierung verdächtiger und infizierter Dateien
- Konfigurierbare Benachrichtigungsfunktionen für den Administrator, den Absender und den Empfänger der Email
- Externes Reporting über Avira AntiVir MailGate Aktivitäten in einer Datenbank
- Automatische Internet-Aktualisierung von MailGate, Scanner, VDF und Engine
- Heuristische Erkennung von Makroviren
- Erkennung aller gebräuchlichen Archivtypen (mit konfigurierbarer Rekursionstiefe für verschachtelte Archive)
- Optional: GUI-Unterstützung für die Integration in Avira Security Management Center

2.2 Module und Funktionsweise von Avira AntiVir MailGate

Avira AntiVir MailGate ist ein SMTP-Scanner, der auf Ihrem UNIX-Mailserver alle ein- und ausgehenden Emails (inklusive Anhang) auf Viren und unerwünschte Programme prüft. Die Prüfung läuft extrem schnell ab und ist leicht zu konfigurieren.

Neben SMTP unterstützt Avira AntiVir MailGate auch die Sendmail Milter-Schnittstelle.



Dieser Agent, dessen Aufgabe es ist, Emails zu speichern und weiterzuleiten, teilt die Arbeit zwischen zwei Programmen auf:

SMTP-Daemon

Der SMTP-Daemon empfängt die Emails und speichert sie im Spool-Verzeichnis. Das Programm läuft als eigenständiger Server, der Port 25 verwendet (SMTP).

Scanner und Weiterleitungs-Daemon

Der Weiterleitungs-Daemon liest die Emails im Spool-Verzeichnis, decodiert die Anhänge und beginnt mit der Prüfung auf Viren und unerwünschte Programme.

Je nach Ergebnis der Prüfung werden saubere Emails weitergeleitet, während infizierte Emails im Spool-Verzeichnis gesperrt werden (rejected).

Entsprechend der Konfiguration in avmailgate.conf sperrt das Programm im selben Verzeichnis auch verdächtige Emails, z. B. passwortgeschützte Archive und fragmentierte Emails. In derselben Konfigurationsdatei werden auch die Regeln für den Spam-Filter festgelegt.

Die Warteschlange kann bei Bedarf mit dem Warteschlangen-Manager avq geprüft werden. Wie das Spool-Verzeichnis geprüft wird, erfahren Sie unter Warteschlangen-Manager avq – Seite 106.

Warnungen:
Der Postmaster erhält eine Email mit detaillierten Alarmen, wenn Viren, unerwünschte Programme oder verdächtige Dateien entdeckt werden. Die Alarme können auch an den Absender und den Empfänger der Email gesendet werden. Das Programm stellt Alarmvorlagen bereit, die Sie anpassen und verwenden können.

Updater:
Der Avira Updater lädt in regelmäßigen Zeitabständen die neuesten Aktualisierungen von den Avira AntiVir MailGate-Webservern herunter und installiert sie (manuell oder automatisch). Das Modul kann auch Benachrichtigungen per Email versenden.

Sie können Avira AntiVir MailGate insgesamt aktualisieren oder nur den Scanner.

2.3 Lizenzierungskonzept

Um Avira AntiVir MailGate verwenden zu können, müssen Sie eine Lizenz für das Programm erwerben und die Lizenzbedingungen anerkennen (siehe http://www.avira.com/de/license-agreement)

Für Avira AntiVir MailGate stehen 2 Lizenzmodelle zur Verfügung:
- Testversion
- Vollversion

Die Lizenzierung hängt von der Anzahl der Benutzer im Netzwerk ab, die durch Avira AntiVir MailGate geschützt werden sollen.

Die Lizenz wird über die Lizenzdatei hbedv.key vergeben. Sie erhalten diese Datei per Email von der Avira GmbH. Die Datei enthält genaue Angaben darüber, welche Programme für welchen Zeitraum lizenziert werden. Ein und dieselbe Lizenzdatei

kann für mehrere Produkte der Avira GmbH gelten.

Testversion

30-Tage-Testlizenz für Avira AntiVir MailGate.

Weitere Informationen zur Evaluation Version finden Sie auf unserer Website http://www.avira.com.

Vollversion

Zum Lizenzumfang der Vollversion gehören:

- Avira AntiVir MailGate-Versionen zum Herunterladen aus dem Internet
- Lizenzdatei per Email zur Freischaltung der Testversion zur Vollversion
- Ausführliche Installationsanleitung (digital)
- Vierwöchiger Installationssupport ab Kaufdatum
- Newsletter-Dienst (per Email)
- Internet-Aktualisierungsdienst für Programmdateien und VDF

Nach der Installation eines Avira AntiVir MailGate-Produkts können Sie sich mit dem folgenden Befehl Informationen über die aktuelle Lizenz anzeigen lassen:

```
/usr/lib/AntiVir/mailgate/avlinfo
```

▶ Wechseln Sie in das Verzeichnis /usr/lib/AntiVir/mailgate und rufen Sie `./avlinfo`

Weitere Informationen erhalten Sie mit dem folgenden Befehl: `avlinfo -h`

2.4 Systemanforderungen

Damit Avira AntiVir MailGate auf Ihrem Server wunschgemäß funktioniert, müssen die folgenden Mindestanforderungen erfüllt sein (abhängig von Faktoren wie dem Umfang des Email-Verkehrs, der Anzahl und Größe der Anhänge usw. kann zusätzlicher Speicher erforderlich sein):

Die Versionen für Linux und Solaris verwenden ähnliche Installations- und Nutzungsverfahren (im Normalfall unterscheiden sich je nach Zielsystem nur einige Dateinamen).

- Rechner: x86, SPARC
- Betriebssystem: Linux (mit GLIBC 2.2 oder höher) oder Solaris
- 32-Bit oder 64-Bit Prozessor
  Einsatz unter 64 Bit UNIX: Bitte verwenden Sie dazu die notwendigen 32 Bit Bibliotheken. Mehr Details finden Sie in der Dokumentation Ihres UNIX-Systems.
- RAM: 512MB
- HDD: 1GB Speicherplatz für das Entpacken der Archive.
- Verwaltung über die SMC: libstdc++so.5 für den SMC-Agent.

Die folgenden Distributionen werden von Avira AntiVir MailGate offiziell unterstützt:

- Red Hat Enterprise Linux 4 Server
- Red Hat Enterprise Linux 5 Server

- Red Hat Enterprise linux 6 Server
- Novell Open Enterprise Server (10.2)
- Novell SUSE Linux Enterprise Server 9 (SLES 9)
- Novell SUSE Linux Enterprise Server 10 - 10.2 (SLES 10)
- Novell SUSE Linux Enterprise Server 11 (SLES 11)
- Debian GNU/Linux 4
- Debian GNU/Linux 5
- Debian GNU/Linux 6
- Ubuntu Server Edition 8
- Ubuntu Server Edition 9
- Ubuntu Server Edition 10
- Ubuntu Server Edition 11
- Sun Solaris 9 (SPARC)
- Sun Solaris 10 (SPARC)

Für die Verwendung von Avira AntiVir MailGate auf einem x86_64 Debian-System wird eine vorherige Installation von lib32nss-mdns empfohlen.

2.4.1 Active Directory

Avira AntiVir MailGate unterstützt die Verwendung von Active Directory auf folgenden Plattformen:

- Windows Server 2003 SP2
- Windows Server 2003 R2 SP2
- Windows Server 2008
- Windows Server 2008 R2

3 Milter-Modus

3.1 Übersicht

Damit Avira AntiVir MailGate im Milter-Modus gestartet wird, ist für die Option `ListenAddress` in avmailgate.conf die folgende Syntax erforderlich (nach der Installation von Avira AntiVir MailGate):

```
inet:port@{hostname|ip-address}
Example: inet:3333@localhost
```

– oder –

```
{unix|local}:/path/to/file
```

Beispiel:

```
unix:/path/to/file
local:/path/to/file
```

Bei Bedarf muss dem Eintrag ForwardTo die Sendmail-Binärdatei zugewiesen werden. Wenn dies bereits der Fall ist, bleibt die Option unverändert:

```
ForwardTo /usr/lib/sendmail -oem -oi
```

3.2 Funktionen von Avira AntiVir MailGate (Milter-Modus)

Avira AntiVir MailGate (Milter-Modus) ist ein Plugin für Sendmail ab Version 8.11, das über die libmilter-Schnittstelle von Sendmail kommuniziert.

Das Modul prüft alle ein- und ausgehenden Emails. Infizierte Emails werden nicht weitergeleitet. In syslog wird eine Statusbenachrichtigung angezeigt. Der Absender, der Empfänger und der Administrator können über eine Infektion benachrichtigt werden.

Funktionen

Die meisten der folgenden Funktionen gelten auch für Avira AntiVir MailGate, wenn es nicht im Milter-Modus läuft.

- Alle Sendmail-Funktionen bleiben verfügbar (z. B. SMTP-Authentifizierung, Anti-Relaying und Anti-Spam)
- Einfache Installation und Integration in Sendmail
- Stündliche oder tägliche Internet-Aktualisierung von MailGate, Scanner, VDF und Engine
- Prüfung ein- und ausgehender Emails
- Verlässliche Echtzeiterkennung von Viren und Malware
- Konfigurierbare Reaktion auf erkannte Viren oder Malware
- Isolierung infizierter oder verdächtiger Dateien in einem Quarantäneverzeichnis
- Logdatei als Log für Email-Verkehr
- Sofortige Aktivierung einer neuen VDF
- Heuristische Erkennung von Makroviren
- Konfigurierbare Alarmvorlagen
- Archivprüfung

3.3 Integration von Avira AntiVir MailGate (Milter-Modus) in Sendmail

3.3.1 Anforderungen

Sendmail in der Version 8.11 oder höher mit libmilter-Schnittstelle wird benötigt.

Andernfalls:

▶ Lesen Sie die Datei README im Verzeichnis libmilter des Sendmail-Kits (http://www.sendmail.org).

▶ Kompilieren Sie die neue Version von Sendmail mit der libmilter-Schnittstelle.

So überprüfen Sie, ob Sendmail mit der libmilter-Schnittstelle kompiliert wurde:

```
sendmail -d0.10 < /dev/null | grep MILTER
```

3.3.2 Integration

Es gibt zwei Möglichkeiten, Avira AntiVir MailGate (Milter-Modus) zur Sendmail-

Konfigurationsdatei sendmail.cf hinzuzufügen:
- Direktes Ändern von sendmail.cf

– ODER –

- Generieren von sendmail.cf

Direktes Ändern von sendmail.cf

▶ Fügen Sie der Konfigurationsdatei sendmail.cf die beiden folgenden Zeilen hinzu:

```
Xavmilter, S=inet:3333@localhost, F=R,
T=S:2m;R:2m;E:10m
O InputMailFilters=avmilter
```

Bedeutung der Werte

- F: legt fest, was geschehen soll, wenn der Filter nicht verfügbar ist:
  - T: Emails werden vorübergehend nicht angenommen (Fehler 4XX)
  - R: Emails werden zurückgewiesen (Fehler 5XX)
- T: legt die folgenden Timeouts fest:
  - C: Timeout für die Herstellung der Verbindung zum Filter
  - S: Timeout für das Senden von Informationen zum Filter
  - R: Timeout für das Lesen einer Antwort vom Filter
  - E: Timeout zwischen dem Senden von „End of Message“ und der Antwort des Filters

Ändern Sie diese Werte, wenn das Log die folgende Benachrichtigung anzeigt:
„Milter (avmilter): timeout before data read“

Generieren von sendmail.cf

▶ Fügen Sie der Datei sendmail.mc die entsprechenden Zeilen hinzu (Befehle, die mit `INPUT` beginnen, müssen in einer Zeile stehen):

Für Sendmail 8.11.x:

```
define('_FFR_MILTER', `true')
INPUT_MAIL_FILTER(`avmilter',`S=inet:3333@localhost,
F=R, T=S:2m;R:2m;E:10m')
```

Für Sendmail 8.12.x:

```
INPUT_MAIL_FILTER(`avmilter',`S=inet:3333@localhost,
F=R, T=S:2m;R:2m;E:10m')
```

▶ Generieren Sie die Datei sendmail.cf
Beispiel:

```
m4 sendmail.mc > /etc/mail/sendmail.cf
```

4 Installation

Die aktuelle Version von Avira AntiVir MailGate finden Sie auf der Avira-Webseite. Avira AntiVir MailGate steht als komprimiertes Archiv zur Verfügung. Sie können das Programm mit dem Skript install auf Ihrem System installieren.

Anforderungen

Um Avira AntiVir MailGate installieren zu können, müssen Sie als **root** angemeldet sein. Außerdem muss auf Ihrem System ein MTA (Sendmail, Postfix, Exim, Qmail usw.) zur Verfügung stehen. Unser Support beschränkt sich jedoch ausschließlich auf Probleme, die direkt mit Avira AntiVir MailGate zu tun haben.

Dieser Abschnitt beschreibt eine Sendmail-Standardinstallation auf einer SuSE-Distribution. Wenn Sie das Programm in einen anderen MTA oder z. B. in Lotus Domino integrieren möchten, finden Sie weitere Informationen in den entsprechenden Dateien (INSTALL.sendmail, INSTALL.exim, INSTALL.qmail, INSTALL.postfix usw.).

Dieses Kapitel enthält die folgenden Abschnitte:

Wenn Sie auch Avira AntiVir Server (UNIX) oder Avira AntiVir Professional (UNIX) installiert haben und diese Produkte mithilfe der GUI konfigurieren und nutzen, beachten Sie, dass die GUI mit den aktuellen Versionen (beginnend mit Version 3) von Avira AntiVir MailGate und Avira AntiVir WebGate nicht kompatibel ist.

4.1 Installationsdateien vorbereiten

Programmdateien aus dem Internet herunterladen

- Laden Sie die aktuellen Dateien von unserer Website http://www.avira.com auf Ihren lokalen Rechner herunter. Der Dateiname lautet antivir-mailgate-prof.tgz.
- Kopieren Sie die Datei auf den Rechner, auf dem Avira AntiVir MailGate installiert werden soll, in ein Verzeichnis Ihrer Wahl (z. B. /tmp).

Programmdateien entpacken

- Wechseln Sie in das temporäre Verzeichnis:

  ```
  cd /tmp
  ```

- Entpacken Sie das Archiv für das Avira AntiVir-MailGate-Kit:
  ```
  tar -xzvf antivir-mailgate-prof.tgz
  ```

  ↳ Im temporären Verzeichnis wird der Ordner antivir-mailgate-prof-<Version> erstellt.

4.2 Lizenzierung

Um Avira AntiVir MailGate ausführen zu können, benötigen Sie eine Lizenz (siehe Lizenzierungskonzept – Seite 10). Die Lizenzdatei hbedv.key erhalten Sie per Email. Sie enthält Informationen über den Umfang und den Gültigkeitszeitraum der Lizenz.

Lizenz erwerben

- Sie dürfen Avira AntiVir MailGate 30 Tage lang testen, wenn Sie das Testlizenzformular auf unserer Website ausfüllen.
- Wenn Sie sich telefonisch oder über sales@avira.com an uns wenden, erhalten Sie eine gültige Lizenzdatei per Email.
- Sie können Avira AntiVir MailGate auch in unserem Online-Shop erwerben.

Lizenzdatei kopieren

- Kopieren Sie die Lizenzdatei hbedv.key in Ihr Installationsverzeichnis. Ein Beispiel:
  /tmp/antivir-mailgate-prof-<Version>.

Sie können die Lizenzdatei später in das Programmverzeichnis /usr/lib/AntiVir/mailgate *kopieren.*

4.3 Installation mit dem Installationsskript „install“

Das Skript install führt eine automatische Installation von Avira AntiVir MailGate durch.

Dazu führt das Skript install folgende Schritte aus:

- Prüfen der Integrität der Installationsdateien.
- Prüfen der zur Installation erforderlichen Berechtigungen.
- Suchen auf dem Rechner nach einer bereits installierten Version von Avira AntiVir MailGate.
- Kopieren der Programmdateien (und Überschreiben vorhandener Dateien, die nicht mehr benötigt werden).
- Kopieren der Konfigurationsdateien (vorhandene Konfigurationsdateien bleiben erhalten).
- Installation des Internet Updaters.
- Optional: Installation der GUI-Unterstützung für Avira SMC (Security Management Center).

Installation vorbereiten

✓ Die Programmdateien wurden aus dem Internet heruntergeladen und entpackt.

▶ Melden Sie sich als **root** an. Andernfalls reicht Ihre Berechtigung nicht aus, um die Installation durchzuführen, und das Skript gibt eine Fehlermeldung aus.

▶ Wechseln Sie in das Verzeichnis, in dem Sie das Avira AntiVir MailGate-Kit entpackt haben. Ein Beispiel:

```
cd /tmp/antivir-mailgate-prof-<Version>
```

Avira AntiVir MailGate installieren

▶ Geben Sie Folgendes ein:

```
./install
```

↳ Das Installationsskript wird gestartet.

▶ Sie müssen die Lizenzvereinbarung lesen und akzeptieren, bevor die Installation fortgesetzt werden kann.

▶ Schließen Sie die Datei mit der Lizenzvereinbarung mit q.

↳ Die folgende Frage wird angezeigt:

```
Do you agree to the license terms? [n]
```

▶ Geben Sie y ein und drücken Sie **Enter**.

↳ Die Avira AntiVir MailGate Core Komponenten sind installiert. Das Skript fragt nun nach dem Pfad der Lizenzdatei:

```
copying install_list_mailgate to  /usr/lib/AntiVir/mailgate ... done
copying LICENSE to /usr/lib/AntiVir/mailgate/LICENSE-mailgate ... done
1) installing AntiVir Core Components (Engine, Savapi and Avupdate)
copying ...

Enter the path to your key file []
```

▶ Geben Sie den Pfad der Lizenzdatei ein und drücken Sie **Enter**.

```
copying license key  to  /usr/lib/AntiVir/mailgate/ license-mailgate.key... done


installation of AntiVir Core Components (Engine, Savapi and Avupdate)
complete
```

– ODER –
Wenn Sie die Lizenzdatei später kopieren möchten, drücken Sie nur **Enter**.

↳ Im nächsten Schritt wird der automatische Internet Updater installiert. Danach werden Sie gefragt, ob in /usr/sbin ein Link für das Startskript erstellt werden soll:

```
2) Configuring updates
An internet updater is available with AVIRA MailGate (UNIX). It will ensure
that you always have the latest malware detection patterns and engine
updates.

In order to trigger an update you will need to run the command:
   /usr/lib/AntiVir/mailgate/avupdate-mailgate

Would you like to create a link in  /usr/sbin for avupdate-mailgate? [y]
```

▶ Bestätigen Sie mit **Enter** oder drücken Sie n.

↳ Nun werden Sie gefragt, ob Sie Cron-Jobs für die Aktualisierung des Scanners und des Produkts erstellen möchten:

```
Would you like to setup Scanner update as cron task? [y]
Please specify the interval to check.
Recommended values are daily or 2 hours.

available options: d [2]
creating Scanner update cronjob ... done

Would you like to check for MailGate updates once a week ? [n] y
creating MailGate update cronjob ... done

setup internet updater complete
```

Sie können diese Optionen auch später einstellen.

↳ Das Skript fährt mit der Installation des Hauptprogramms fort:

```
3) installing main program
copying doc/antivir_mailgate_de.pdf to /usr/lib/AntiVir/mailgate ... done
copying ...
```

↳ Die nächsten Fragen beziehen sich auf die Hosts, die als lokal behandelt werden, sowie jene Hosts, die über Avira AntiVir MailGate Emails weiterleiten dürfen:

```
Enter the hosts and/or domains that are local:
[<hostname>]:
```

▶ Ändern Sie bei Bedarf den Hostnamen und drücken Sie **Enter**.:

```
Please enter the hosts and networks that are allowed to relay. When running
MailGate in content filter mode (SMTP), the address suggested below will be
sufficient. You can change these settings by editing the file
 /etc/avira/avmailgate.acl
afterwards

 [127.0.0.1/8]:
```

↳ Nun werden Sie gefragt, ob in /usr/sbin ein Link für das Startskript erstellt werden soll:

```
Would you like to create a link in /usr/sbin for avmailgate? [y]
```

▶ Bestätigen Sie mit **Enter** oder drücken Sie n.

↳ Nun werden Sie gefragt, ob Avira AntiVir MailGate beim Systemstart automatisch gestartet werden soll:

```
Please specify if boot scripts should be set up.
Set up boot scripts [y]:
```

▶ Geben Sie n ein und drücken Sie **Enter**. Sie können diese Option später ändern.

– ODER –

Bestätigen Sie die Standardeinstellung mit **Enter**.

↳ Im nächsten Schritt wird das SMC-Plugin für Avira Security Management Center installiert:

```
installation of main program complete

4) activate SMC support
If you are going to use AVIRA Security Management Center (SMC)
to manage this software remotely you need this

 Would you like to activate SMC support? [y]
```

▶Drücken Sie **Enter**, um das SMC-Plugin zu installieren, oder n und **Enter**, um die Installation zu überspringen.

↳ Wenn das Skript beendet ist, wird die folgende Meldung angezeigt:

```
Installation of the following features complete:
    AntiVir Core Components (Engine , Savapi and Avupdate)
    AVIRA Internet Updater
    AVIRA MailGate
    AntiVir SMC plugin
```

- Setzen Sie die Installation abhängig von Ihrem MTA so fort, wie es unter Weitere Installationsschritte in Abhängigkeit vom MTA – Seite 24 beschrieben ist.
- Avira AntiVir MailGate wird unter

  `/usr/lib/AntiVir/mailgate`

  installiert.
- Nun können Sie Avira AntiVir MailGate starten:

  `/usr/lib/AntiVir/mailgate/avmailgate start`

Modifizierte Binärdateien können nicht starten.

Zum Beispiel, mit prelink: Entweder deaktivieren Sie prelink, oder tragen Sie /usr/lib/AntiVir/mailgate als Ausnahme in der Konfigurationsdatei /etc/prelink.conf ein.

Seit der Version 3.0.0 wird ein neues Scanner-Backend verwendet. Falls Sie bisher eine Avira AntiVir MailGate-Version eingesetzt haben, die älter als 3.0.0 ist, beachten Sie bitte, dass in der aktuellen MailGate-Version einige Scanner-spezifische Konfigurationsoptionen nicht mehr in avmailgate.conf, sondern in avmailgate-scanner.conf angegeben werden.

Es empfiehlt sich dringend, nach der Installation eine Aktualisierung durchzuführen, damit alle Schutzmechanismen auf dem neuesten Stand sind. Führen Sie dazu den folgenden Befehl aus:

```
/usr/lib/AntiVir/mailgate/avupdate-mailgate
```

Weitere Informationen über Aktualisierungen finden Sie unter *Aktualisierungen – Seite 118.*

4.4 Avira AntiVir MailGate erneut installieren oder deinstallieren

Sie können das Installationsskript jederzeit neu aufrufen. Hiermit sind folgende Vorgänge möglich:

- Installation einer neuen Version (Upgrade). Das Installationsskript prüft zunächst die Vorgängerversion und installiert die erforderlichen neuen Komponenten.
  Die vorhandenen Konfigurationseinstellungen werden dabei nicht überschrieben, sondern per Vererbung weitergegeben (siehe Konfiguration – Seite 29).
- Nachinstallation einzelner Komponenten.
- Aktivierung oder Deaktivierung des automatischen Starts des Avira Updaters und von Avira AntiVir MailGate.

Avira AntiVir MailGate erneut installieren

Das Vorgehen ist für alle Fälle gleich:

▶ Wechseln Sie in das temporäre Verzeichnis, in das Sie Avira AntiVir MailGate entpackt haben, also etwa:
`cd /tmp/antivir-mailgate-prof-<version>/`

▶ Geben Sie ein:
`./install`

↳ Das Installationsskript läuft weitgehend ab wie in der Erstinstallation beschrieben (siehe Avira AntiVir MailGate installieren – Seite 19).

▶ Ändern Sie die entsprechenden Einstellungen während der Installation.

↳ Avira AntiVir MailGate ist mit den neuen Einstellungen installiert.

Avira AntiVir MailGate deinstallieren

Wenn Sie Avira AntiVir MailGate deinstallieren wollen, können Sie das *uninstall* Skript benutzen. Es liegt im Installationsverzeichnis.

▶ Wechseln Sie in das Verzeichnis, in das Sie Avira AntiVir MailGate installiert haben
`cd /usr/lib/AntiVir/mailgate`

▶ Geben Sie ein:

`./uninstall --product=Mailgate`

↳ Das Skript deinstalliert das Produkt. Es fragt, ob Sie eine Kopie der Lizenz-Datei behalten möchten; ob Sie die Konfigurationsdateien und Logdateien sichern möchten. Es kann auch die cron-Jobs für die Aktualisierung von MailGate oder Scanner löschen.

▶ Antworten Sie mit ***y*** oder ***n*** und bestätigen Sie mit ***Enter***.

↳ Avira AntiVir MailGate ist deinstalliert.

4.5 Weitere Installationsschritte in Abhängigkeit vom MTA

Nach der oben beschriebenen Installation von Avira AntiVir MailGate müssen Sie je nachdem, welchen MTA Sie verwenden, einige Einstellungen manuell vornehmen.

Der folgende Abschnitt beschreibt die Besonderheiten von Sendmail, Exim, Qmail und Postfix.

Sendmail konfigurieren

Wenn Sie mit Sendmail arbeiten, empfiehlt sich die Verwendung von Avira AntiVir MailGate im Milter-Modus (siehe Kapitel Milter-Modus – Seite 13). Dieser Modus gewährleistet die volle SMTP-Funktionalität in Sendmail (z. B. SMTP-Authentifizierung).

Exim konfigurieren

Avira AntiVir MailGate läuft mit Exim Version 3.0 oder höher.

▶ Mit dem folgenden Befehl können Sie Ihre Exim-Version herausfinden:
`exim -bV`

Es gibt zwei Möglichkeiten, Avira AntiVir MailGate in Exim zu integrieren:
- Integration von Avira AntiVir MailGate als Inhaltsfilter in Exim (empfohlen)
- Proxy-Modus

Inhaltsfilter

Konfiguration von Avira AntiVir MailGate:

▶ Ändern Sie die folgenden Einträge in avmailgate.conf (oder fügen Sie sie hinzu):

```
ListenAddress 127.0.0.1 port 10024
ForwardTo SMTP: 127.0.0.1 port 10025
```

▶ Starten Sie Avira AntiVir MailGate neu.

Konfiguration von Exim:

▶ Ändern Sie die folgenden Einträge in exim.conf (oder fügen Sie sie hinzu):

```
# Listen on all interfaces on port 25
# and on 127.0.0.1 port 10025
local_interfaces = 0.0.0.0.25 : 127.0.0.1.10025
```

Fügen Sie einen Eintrag für den Router hinzu:

▶ Suchen Sie in exim.conf nach `begin router` und fügen Sie die folgenden Einträge hinzu:

```
# Router for AntiVir MailGate
  antivir_mailgate:
    debug_print = "R: AntiVir MailGate for
```

```
        $local_part@$domain"
    driver = manualroute
    transport = antivir_mailgate_transport
    route_list = "* localhost byname"
    self = send
    # do not call this router in the second instance of Exim
    condition = ${if !eq {$interface_port}{10025}{1}{0}}
```

Fügen Sie einen Eintrag für den Transport hinzu:

▶ Suchen Sie in exim.conf nach `begin transports` und fügen Sie die folgenden Zeilen hinzu:

```
# Transport for AntiVir MailGate
  antivir_mailgate_transport:
        driver = smtp
        # connect to port 10024
        port = 10024
        allow_localhost
```

▶ Starten Sie Exim neu.

Proxy-Modus

Konfiguration von Avira AntiVir MailGate:

▶ Ändern Sie die folgenden Einträge in avmailgate.conf (oder fügen Sie sie hinzu):

```
ListenAddress 0.0.0.0 port 25
ForwardTo SMTP: 127.0.0.1 port 825
```

▶ Starten Sie Avira AntiVir MailGate neu.

Konfiguration von Exim:

▶ Ändern Sie die folgenden Einträge in exim.conf (oder fügen Sie sie hinzu):

```
daemon_smtp_port = 825
```

▶ Starten Sie Exim neu.

Qmail konfigurieren

Zur besseren Integration von Avira AntiVir MailGate in Qmail ist ein Plugin verfügbar. Einzelheiten erfahren Sie bei support@avira.com.

Es gibt zwei Möglichkeiten, Avira AntiVir MailGate in Qmail zu integrieren:

- Sendmail-Wrapper
- Backdoor-Verfahren

Ersetzen Sie SMTP nur in der Datei `run` *durch* `825`*. Alle anderen Parameter sind nur*

Beispiele.

Sendmail-Wrapper

Sie können den Sendmail-Wrapper, der mit Qmail ausgeliefert wird, für die Zustellung von Emails verwenden (Standard). Wechseln Sie zuerst in den Qmail-Installationsordner und aktivieren Sie den Wrapper.

▶ Aktivieren Sie den Sendmail-Wrapper in Qmail:

```
ln -s /var/qmail/bin/sendmail /usr/lib/sendmail
ln -s /var/qmail/bin/sendmail /usr/sbin/sendmail
```

▶ Richten Sie den Email-Weiterleitungsmodus ein. In der Datei /etc/avira/avmailgate.conf finden Sie die folgende Zeile:

```
# Select how mail should be forwarded.
```

▶ Ändern Sie die dazugehörigen Einträge auf folgende Weise:

```
# Send mail by piping it through sendmail (this is the default)
  ForwardTo /usr/sbin/sendmail -oem -oi
# Or if you want the mail to be sent by SMTP
# ForwardTo SMTP: localhost port smtp
```

Backdoor-Verfahren

Bei der zweiten Möglichkeit wird die Email-Zustellung über Port 825 eingerichtet, auf dem Qmail aktiv sein sollte. Dies lässt sich z. B. mithilfe der Datei inetd.conf erreichen (siehe Qmail-Installationspaket).

▶ Richten Sie den Email-Weiterleitungsmodus ein. Suchen Sie in /etc/avira/avmailgate.conf nach der folgenden Zeile:

```
# Select how mail should be forwarded.
```

▶ Ändern Sie die dazugehörigen Einträge auf folgende Weise:

```
# ForwardTo /usr/sbin/sendmail -oem -oi
# Or if you want the mail to be sent by SMTP
  ForwardTo SMTP: localhost 825
```

Wenn Sie inetd mit Qmail verwenden:

▶ Fügen Sie in inetd.conf die folgende Zeile ein (1 Zeile!):

```
825 tcp nowait qmaild /var/qmail/bin/tcp-env tcp-env
/var/qmail/bin/qmail-smtpd
```

Wenn Sie tcpwrapper mit Qmail verwenden:

▶ Ändern Sie den Qmail-Port in /var/qmail/supervise/qmail-smtpd/run. Suchen Sie z. B. nach den folgenden Zeilen:

```
/usr/bin/tcpserver -D -R -v -p -x /etc/tcprules.d/qmail-smtp.cdb \
-u $QMAILDUID -g $NOFILESGID 0 smtp /var/qmail/bin/qmail-smtpd
2>&1
```

▶ Ändern Sie die Zeilen folgendermaßen:

```
/usr/bin/tcpserver -D -R -v -p -x /etc/tcprules.d/qmail-smtp.cdb \
-u $QMAILDUID -g $NOFILESGID 0 825 /var/qmail/bin/qmail-smtpd 2>&1
```

Postfix konfigurieren

Es gibt zwei Möglichkeiten, Avira AntiVir MailGate in Postfix zu integrieren:

- Integration von Avira AntiVir MailGate als Inhaltsfilter in Postfix (empfohlen)
- Avira AntiVir MailGate hört Port 25 ab und leitet Emails an Postfix weiter

Inhaltsfilter

Gehen Sie folgendermaßen vor:

▶ Suchen Sie in /etc/avira/avmailgate.conf nach der folgenden Zeile:

```
# Select how mail should be forwarded.
```

▶ Ändern Sie die dazugehörigen Einträge auf folgende Weise:

```
# Select how mail should be forwarded.
# Send mail by piping it through sendmail (this is the default)
# ForwardTo /usr/sbin/sendmail -oem -oi
# Or if you want the mail to be sent by SMTP
  ForwardTo SMTP: localhost port 10025
# Set the network interface the SMTP daemon will listen on.
  ListenAddress 127.0.0.1 port 10024
```

Wenn Sie SuSE Mail Server II verwenden:

▶ Ersetzen Sie den Eintrag `#AllowSourceRouting NO` durch den folgenden:

```
AllowSourceRouting YES
```

▶ Beenden Sie Avira AntiVir MailGate und starten Sie es neu:

```
/etc/init.d/avmailgate restart
```

▶ Fügen Sie in /etc/postfix/master.cf den folgenden Eintrag hinzu:

```
# For AntiVir maildaemon
  localhost:10025 inet n - n - - smtpd -o content_filter=
```

▶ Achten Sie darauf, dass das erste Zeichen in der Tabelle kein Leerzeichen und kein Tabulatorzeichen ist.

Der Parameter `-o content_filter` verhindert, dass Emails wiederholt zwischen Avira AntiVir MailGate und Postfix hin und her geschickt werden.

▶ Fügen Sie in /etc/postfix/main.cf die folgenden Einträge hinzu:

```
# AntiVir integration
  content_filter = smtp:[127.0.0.1]:10024
```

Diese Einstellung verhindert unnötige MX-Lookups.

▶ Starten Sie Postfix neu:

```
/etc/init.d/postfix restart
```

oder

```
/etc/init.d/postfix reload
```

Wenn Postfix für Emails den Status **deferred** *setzt, führen Sie nach der Installation von Avira AntiVir MailGate die folgenden Schritte durch:*

▶ Suchen Sie in main.cf nach der folgenden Zeile:

```
defer_transports = local
```

▶ Kommentieren Sie die Zeile aus:

```
# defer_transports = local
```

Port 25 abhören

▶ Suchen Sie in master.cf nach der folgenden Zeile:

```
smtp inet n - n - - smtpd
```

▶ Kommentieren Sie die Zeile aus:

```
# smtp inet n - n - - smtpd
```

↳ Dadurch wird verhindert, dass Postfix den SMTP-Port (25) abhört, denn der SMTP-Daemon von Avira AntiVir MailGate soll den SMTP-Port (25) abhören.

▶ Starten Sie Postfix neu:

```
/etc/init.d/postfix restart
```

oder

```
/etc/init.d/postfix reload
```

4.6 Avira AntiVir MailGate nach der Installation testen

Nachdem Sie Avira AntiVir MailGate installiert haben, sollten Sie seine Funktionsfähigkeit überprüfen. Zu diesem Zweck können Sie einen Testvirus namens Eicar verwenden, der von allen Virenscannern erkannt wird. Der Virus richtet keinerlei Schaden an, löst aber bei der Prüfung der Email eine Reaktion des Programms aus, sofern dieses richtig installiert und konfiguriert wurde.

▶ Kopieren Sie die folgende Zeichenkette in eine leere Datei:
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

– ODER –
Laden Sie die Eicar-Datei von der Website http://www.eicar.com herunter.

▶ Senden Sie diese Datei als Anhang einer Test-Email für Avira AntiVir MailGate.

▶ Überprüfen Sie die Reaktion im Verzeichnis /var/spool/avmailgate/rejected.

▶ Überprüfen Sie die Meldungen, die Avira AntiVir MailGate an die Logdatei oder an syslog gesendet hat.

5 Konfiguration

Sie können Avira AntiVir MailGate so anpassen, dass auf Ihrem System die bestmögliche Leistung erreicht wird. Während der Installation mit dem install-Skript werden einige der Einstellungen vorgeschlagen. Sie können diese Einstellungen jederzeit ändern.

In diesem Abschnitt werden Sie Schritt für Schritt durch den Konfigurationsvorgang geführt. Dazu gehören die folgenden Themenbereiche:

Die Konfigurationsdateien werden beim Programmstart gelesen. Dabei werden Leerzeilen und Zeilen, die mit „#“ beginnen, ignoriert.

Die Dateien enthalten Standardeinstellungen, die sich für die meisten Konfigurationen eignen. Einige Einträge sind deaktiviert oder durch ein „#“-Zeichen auskommentiert. Diese Einträge können durch Löschen des „#“-Zeichens aktiviert werden.

Beginnend mit Avira AntiVir MailGate 3.0.0 werden ungültige Konfigurationsoptionen eine Fehler-Meldung auslösen:
"Error at line ... in /etc/avira/mailgate.conf".

Am Ende der Installation wird die Liste der Konfigurationsdateien angezeigt:

/etc/avira/avmailgate.conf	(MailGate-Hauptkonfiguration)
/etc/avira/avmailgate-scanner.conf	(Scanner-Konfiguration)
/etc/avira/avmailgate.acl	(MailGate-Zugriffsliste)
/etc/avira/avmailgate.ignore	(MailGate-Ignore-Liste)
/etc/avira/avmailgate.scan	(MailGate-Scan-Liste)
/etc/avira/avmailgate.warn	(MailGate-Warnliste)
/etc/avira/asmailgate.except	(MailGate-Spamfilter-Konfiguration)
/etc/avira/avupdate-mailgate.conf	(Optionen für Avira avupdate)

5.1 Avira AntiVir MailGate-Spool-Verzeichnisse

Avira AntiVir MailGate nimmt infizierte Emails in „Quarantäne“. Je nach Konfiguration werden der Postmaster und/oder der Absender und/oder der Empfänger der Email über die Entdeckung eines Virus oder unerwünschten Programms benachrichtigt. Diese Parameter werden in der Datei avmailgate.conf festgelegt (siehe Avira AntiVir MailGate-Konfiguration in avmailgate.conf – Seite 31).

Spool-Verzeichnisse

Spool-Verzeichnisse

Das Spool-Verzeichnis (Standard: /var/spool/avmailgate/) enthält drei Unterverzeichnisse:

- incoming: eingehende Emails, die geprüft werden müssen.
- outgoing: geprüfte Emails, die weitergeleitet werden können.
- rejected: Emails, die einen Virus oder ein unerwünschtes Programm enthalten oder die (beispielsweise wegen eines MIME-Fehlers) als problematisch eingestuft wurden.

Spool-Dateien

Spool-Dateien

In diesen Verzeichnissen ist jede Email durch zwei Dateien vertreten:

- Datendatei
- Steuerdatei

Der Name der Datendatei beginnt mit df- und enthält eine ID (z. B. 32557-0BE692EB).

Die Steuerdatei hat dieselbe ID. Ihr Name beginnt jedoch abhängig vom Status mit:

- xf-: die Steuerdatei wurde soeben bearbeitet.
- qf-: die Email muss einer Virenprüfung unterzogen werden.
- Qf-: die Email kann ohne Prüfung weitergeleitet werden.
- vf-: die Email enthält einen Virus oder ein unerwünschtes Programm.
- mf-: in der Email gibt es ein MIME-Problem.

Beispiel

Beispiel

- Datendatei: df-32557-0BE692EB
- Entsprechende Steuerdatei: qf-32557-0BE692EB

Spool-Dateien bearbeiten

Spool-Dateien bearbeiten

Wurde ein Virus oder ein unerwünschtes Programm entdeckt, enthält das Verzeichnis
/var/spool/avmailgate/rejected/ die folgenden Dateien:

- df-Datei
- vf- oder mf-Datei

Diese Dateien können durch externe Programme oder Skripts bearbeitet werden (z. B. diejenigen im Parameter `ExternalProgram`, siehe Avira AntiVir MailGate-Konfiguration in avmailgate.conf – Seite 31).

Wurde kein Virus und kein unerwünschtes Programm entdeckt, werden die Daten- und Steuerdateien gelöscht, nachdem die Email geprüft und gesendet wurde.

5.2 Avira AntiVir MailGate-Konfiguration in avmailgate.conf

Die Konfigurationsdatei avmailgate.conf enthält zahlreiche Parameter für die Arbeit mit Avira AntiVir MailGate.

Parameter

Parameter

- Zeichenfolge (characters): Eine Zeichenkette, bestehend aus mindestens einem Zeichen. Wenn Sie den Wert mit Leerstellen beginnen oder beenden möchten, müssen Sie den Wert in „Anführungszeichen“ setzen.
- Pfadangabe: Pfadangabe zu einer Datei, wie z.B. `/usr/lib/AntiVir/mailgate/avmailgate`.
- Option: Vorgegebene Optionen, wie z.B. `RECIPIENT | SENDER | BOTH`.
- Zahl (number): eine Dezimalzahl.
  Erlaubter Minimalwert: -2147483648
  Erlaubter Maximalwert: 2147483647
- Nicht-negative Zahlen (non-negative number): Eine nicht-negative Dezimalzahl, 0 oder größer.
  Erlaubter Minimalwert: 0
  Erlaubter Maximalwert: 4294967295
- Logischer Ausdruck (boolean): Ein Boole’scher Wert, entweder JA (YES) oder NEIN (NO).
- Größe (size): Eine Dezimalzahl, optional gefolgt von einem Suffix wie B (Bytes) K (Kilobytes), M (Megabytes) oder G (Gigabytes). Ist kein Suffix vorgegeben, wird der Wert als Bytes interpretiert.
  Erlaubter Minimalwert: 0
  Erlaubter Maximalwert: 4294967295

  Erlaubter Maximalwert, wenn das Suffix G verwendet wird: 3
  Erlaubter Maximalwert, wenn das Suffix M verwendet wird: 4095
  Erlaubter Maximalwert, wenn das Suffix K verwendet wird: 4194303

- Zeitspanne (timespan): Eine Dezimalzahl, optional gefolgt von einem Suffix wie s (Sekunden), m (Minuten), h (Stunden) oder d (Tage). Ist kein Suffix vorgegeben, wird der Wert als Sekunden interpretiert.

Konfigurationsverfahren

Konfigurationsverfahren

- Passen Sie avmailgate.conf an Ihre Erfordernisse an.
- Starten Sie Avira AntiVir MailGate neu, damit die geänderten Einstellungen wirksam werden:

```
/usr/lib/AntiVir/mailgate/avmailgate restart
```

Die Einträge in avmailgate.conf werden im Folgenden beschrieben. Thematisch verwandte Einträge sind zu Gruppen zusammengefasst. Die Einträge betreffen nur Avira AntiVir MailGate und wirken sich auf keine andere AntiVir-Software aus.

Wenn Sie User, Group, PidDir oder ListenAddress ändern, müssen Sie zuvor Avira AntiVir MailGate beenden.

Mit folgendem Befehl

```
./avmailgate.bin --dump-config
```

können Sie sich die momentan gültigen Konfigurationswerte unter Ausschluss aller in der Konfigurationsdatei vorhandenen Kommentare und deaktivierter Konfigurationseinstellungen anzeigen lassen.

User, Group

Benutzer/Gruppe

Die Benutzer und die Gruppe für Avira AntiVir MailGate-Prozesse (sollten nicht **root** sein).

Wenn Sie diesen Parameter ändern, müssen Sie auch den Wert für `User` *und* `Group` *in* /etc/avira/avmailgate-scanner.conf *ändern (siehe* *Scanner-Konfiguration in avmailgate-scanner.conf – Seite 93**).*

Syntax:

```
User "Zeichenfolge"
Group "Zeichenfolge"
```

Voreingestellt:

```
User uucp
Group antivir
```

Beispiel:

```
User FooBarBaz
Group FooBar
```

Wenn Sie diese Einstellungen ändern, müssen Sie auch die Zugriffsrechte für das Spool-Verzeichnis (Konfigurationsoption `SpoolDir`) und für

```
/usr/lib/AntiVir/mailgate/gui
```

anpassen.

Postmaster

Postmaster

Dieser Parameter bestimmt die Email-Adresse, an die Alarme über Viren/ unerwünschte Programme und andere Benachrichtigungen gesendet werden.

Syntax:

```
Postmaster   "Zeichenfolge"
```

Voreingestellt:

```
Postmaster    postmaster.
```

Z. B.:

```
Postmaster virusmaster@admins.department.example.com
```

MyHostName

Hostname

FQDN (Fully Qualified Domain Name) des lokalen Hosts.

Syntax:

```
MyHostName "Zeichenfolge"
```

Beispiel:

```
MyHostName FooBarBaz
```

Ist diese Option nicht belegt, wird die Standardeinstellung durch `gethostname(2)` ermittelt. Andernfalls ist die Standardeinstellung:

```
MyHostName localhost
```

SpoolDir

Spool-Verzeichnis

Während ihrer Verarbeitung werden Emails in den Unterverzeichnissen incoming, rejected und outgoing abgelegt. Das Standardverzeichnis wird durch das Skript install erstellt. Wenn Sie die Option SpoolDir ändern, müssen Sie selbst die Unterverzeichnisse incoming, outgoing und rejected erstellen.

Das Spool-Verzeichnis und die Unterverzeichnisse incoming, outgoing und rejected müssen zu dem Benutzer und der Gruppe gehören, die unter User, Group festgelegt wurden. Der Zugriff darf nur diesen Benutzern erlaubt sein (mode=700).

Syntax:

```
SpoolDir "Pfadangabe"
```

Beispiel:

```
SpoolDir  /var/spool/FooBarBaz
```

Voreingestellt:

```
SpoolDir /var/spool/avmailgate
```

AntiVirDir

AntiVir-Verzeichnis

Das Bibliotheksverzeichnis von Avira AntiVir MailGate, das u. a. die Virendefinitionsdateien (*.vdf) und die Lizenzdatei enthält.

Syntax:

```
AntiVirDir "Pfadangabe"
```

Beispiel:

```
AntiVirDir /usr/lib/AntiVir/FooBarBaz
```

Wenn Sie AntiSpam verwenden, sollten Sie das AntiVir-Standardverzeichnis nicht ändern:

```
AntiVirDir /usr/lib/AntiVir/mailgate
```

TemporaryDir

Temporäres Verzeichnis

Dieses Verzeichnis enthält temporäre Dateien (z. B. Anhänge, die gerade auf Viren oder unerwünschte Programme geprüft werden). Für entpackte Anhänge wird ausreichend Speicherplatz benötigt. Ist diese Option nicht belegt, wird die Umgebungsvariable TMPDIR verwendet.

Wenn alle Avira AntiVir MailGate-Komponenten ein gemeinsames temporäres Verzeichnis verwenden sollen, ändern Sie die Optionen `TemporaryDir` *in* /etc/avira/avmailgate.conf *und* `ScanTemp` *in* avmailgate-scanner.conf.

Syntax:

```
TemporaryDir "Pfadangabe"
```

Beispiel:

```
TemporaryDir  /var/FooBarBaz
```

Voreingestellt:

```
TemporaryDir /var/tmp
```

MatchMail AddressFor Local

Domain-Namen überprüfen

Diese Option legt fest, ob die Domain-Namen von RECIPIENT-, SENDER- oder BOTH-Adressen mit den Einträgen im Abschnitt `local:` der Datei avmailgate.acl verglichen werden sollen, bevor eine Email angenommen wird.

Syntax:

```
MatchMailAddressForLocal "Option"
MatchMailAddressForLocal  RECIPIENT | SENDER | BOTH
```

Beispiel:

```
MatchMailAddressForLocal  RECIPIENT
```

Weitere Informationen finden Sie unter Host-Konfiguration in avmailgate.acl –

Seite 96.
Voreingestellt:

```
MatchMailAddressForLocal RECIPIENT
```

SMTPBanner

SMTP-Banner

Legt die von Avira AntiVir MailGate versendeten Header fest. Sie können den Text ändern, wenn Sie beispielsweise die Art der verwendeten Sicherheits-Software nicht preisgeben möchten.

Syntax:

```
SMTPBanner "Zeichenfolge"
```

Beispiel:

```
SMTPBanner FooBarBaz
```

Voreingestellt:

```
SMTPBanner "AntiVir MailGate"
```

PidDir

PID-Verzeichnis

In diesem Verzeichnis werden die PID-Dateien für die Avira AntiVir MailGate-Hauptprozesse gespeichert. Sie müssen Avira AntiVir MailGate beenden, bevor Sie diesen Parameter ändern.

Syntax:

```
PidDir "Pfadangabe"
```

Beispiel:

```
PidDir /var/FooBarBaz
```

Voreingestellt:

```
PidDir /var/tmp
```

Syslog Facility

Syslog-Facility

Diese Option legt die Log-Kategorie fest, die Syslog für Avira AntiVir MailGate-Nachrichten verwendet.

Syntax:

```
SyslogFacility "Zeichenfolge"
```

Beispiel:

```
SyslogFacility local0
```

Voreingestellt:

```
SyslogFacility mail
```

LogFile

Logdatei

Die Option muss den vollständigen Pfad der Logdatei enthalten. Die Einträge in der Logdatei werden auch an Syslog gesendet.

Ist LogFile auf NO gesetzt (Standardeinstellung), wird keine Logdatei verwendet.

Die Einträge werden aber nach wie vor an Syslog gesendet.

Syntax:

```
LogFile "Pfadangabe"
```

Beispiel:

```
LogFile /var/log/avmailgate.log
```

Voreingestellt:

```
LogFile NO
```

LogAlertsForEachRecipient

LogAlertsForEachRecipient

Diese Option legt fest, ob Avira AntiVir MailGate einen Eintrag pro infizierter Email oder pro Empfänger in der Logdatei vornimmt.

Syntax:

```
LogAlertsForEachRecipient "YES | NO"
```

Voreingestellt:

```
LogAlertsForEachRecipient NO
```

DebugLevel

Debug-Meldungen

Mithilfe dieser Option wird festgelegt, ob bzw. wie detailliert Debug-Meldungen in Syslog oder, falls aktiviert, in der Logdatei festgehalten werden.

Die Detailgenauigkeit kann über die Stufen 0-5 bestimmt werden. Bei einem Wert von 0 werden keine Debug-Meldungen gelogged, bei 5 hingegen alle.

Syntax:

```
DebugLevel "nicht-negative Zahl"
```

Beispiel:

```
Debuglevel 2
```

Voreingestellt:

```
DebugLevel 0
```

ListenAddress

IP-Adresse

Die Netzwerk-Schnittstellen-Adresse und der Port, an dem der SMTP-Daemon abhören soll. Avira AntiVir MailGate hört voreingestellt an 0.0.0.0:25 ab (alle Netzwerk-Schnittstellen an Port 25). Sie kann durch eine spezielle Netzwerk-Schnittstellen-Adresse konfiguriert werden.

Syntax:

Für den SMTP-Modus:

```
ListenAddress "Zeichenfolge" Port "Zahl"
```

Für den Milter-Modus:

```
ListenAddress "Zeichenfolge":"Zahl"@"Zeichenfolge"
```

Voreingestellt:

```
ListenAddress 0.0.0.0 port 25
```

Der voreingestellte Wert wird nur akzeptiert, wenn die IPv4-Unterstützung aktiviert ist. Wenn Sie die IPv4-Unterstützung deaktiviert haben, müssen Sie an dieser Stelle eine gültige IPv6-Adresse angeben (Siehe auch Konfigurationsoption InetProtocols – Seite 61)

Beispiele

Für den SMTP-Modus:

```
ListenAddress 192.168.5.20 port 25
```

Für den Milter-Modus:

```
ListenAddress inet:3333@localhost
```

Wenn Sie sich nicht sicher sind, verwenden Sie die Standardeinstellung:

```
ListenAddress 0.0.0.0 port 25
```

Mit einer anderen Syntax können Sie Avira AntiVir MailGate im Milter-Modus starten. Weitere Informationen finden Sie unter Milter-Modus – Seite 13. Gegenwärtig arbeitet der Milter-Modus nur mit IPv4.

Aktivieren Sie die Ipv6-Unterstützung nur mithilfe der Option InetProtocols, müssen Sie für die Optionen ListenAddress und ForwardTo sowie in der avmailgate.acl*-Datei IPv6-Adressen angeben.*

MaxIncoming Connections

Maximale Anzahl gleichzeitiger Verbindungen (nicht im Milter-Modus)

Diese Option legt die Anzahl gleichzeitiger Client-Verbindungen fest, die von Avira AntiVir MailGate akzeptiert werden. Die Standardeinstellung 0 steht für eine unbegrenzte Anzahl.

Syntax:

```
MaxIncomingConnections "nicht-negative Zahl"
```

Beispiel:

```
MaxIncomingConnections 10
```

Voreingestellt:

```
MaxIncomingConnections 0
```

SMTP Timeout

SMTP-Timeout (nicht im Milter-Modus)

Diese Option legt den maximalen Timeout für SMTP-Verbindungen fest (in Sekunden).

Syntax:

```
SMTPTimeout "nicht-negative Zahl"
```

Beispiel:

```
SMTPTimeout 60
```

Voreingestellt:

```
SMTPTimeout 300
```

EnableLegacy Quarantine

EnableLegacyQuarantine

Mit dieser Option wählen Sie aus, welchen der beiden Quarantäne-Manager Sie nutzen möchten.

Voreingestellt ist der Quarantäne-Manager Classic:

```
EnableLegacyQuarantine Yes
```

Wollen Sie zum neuen Quarantäne-Manager Advanced wechseln, ändern Sie diesen Parameter zu:

```
EnableLegacyQuarantine No
```

Weitere Details über die Quarantäne-Manager erfahren Sie in Kapitel 6.4 - Quarantäne-Management – Seite 107.

MaxMessage Size

Maximale Nachrichtengröße (nicht im Milter-Modus)

Ein Wert größer als 0 bedeutet, dass nur Emails geprüft werden, die die angegebene Größe nicht überschreiten. Größere Emails werden zurückgewiesen. Der Wert 0 bewirkt, dass Emails von beliebiger Größe geprüft werden.

Syntax:

```
MaxMessageSize "Zahl""GB|MB|KB"
```

Beispiele:

```
MaxMessageSize 4KB, 3MB, 2GB.
```

Voreingestellt:

```
MaxMessageSize 0
```

MinFreeBlocks

Minimum an freiem Systemspeicher (nicht im Milter-Modus)

Avira AntiVir MailGate weist eingehende Verbindungen zurück, wenn der freie Platz auf der Festplatte unter dem angegebenen Wert liegt.

Syntax:

```
MinFreeBlocks "nicht-negative Zahl"
```

Beispiel:

```
MinFreeBlocks 50
```

Voreingestellt:

```
MinFreeBlocks 100
```

Max Recipients PerMessage

Maximale Anzahl der Empfänger pro Email (nicht im Milter-Modus)

Diese Option legt die maximale Anzahl der Empfänger einer Email fest. Die Einstellung 0 deaktiviert die Option und ermöglicht eine unbegrenzte Anzahl der Empfänger einer Email.

Syntax:

```
MaxRecipientsPerMessage "nicht-negative Zahl"
```

Beispiel:

```
MaxRecipientsPerMessage 50
```

Voreingestellt:

```
MaxRecipientsPerMessage 100
```

RefuseEmptyMailFrom

Emails ohne Absendernamen zurückweisen (nicht im Milter-Modus)

Manche Emails enthalten keinen Absendernamen. Bei der Standardeinstellung NO nimmt der SMTP-Server alle eingehenden Emails an. Diese Einstellung sollte nicht geändert werden.

Syntax:

```
RefuseEmptyMailFrom "YES|NO"
```

Voreingestellt:

```
RefuseEmptyMailFrom NO
```

Gemäß einer Empfehlung der Standards RFC2821, RFC821 und RFC2505 sollte ein SMTP-Server alle Emails annehmen, also auch solche ohne Absenderadresse. Die Standardeinstellung für den Parameter `RefuseEmptyMailFrom` *sollte daher nicht geändert werden.*

AllowSourceRouting

Source Routing zulassen (nicht im Milter-Modus)

Beim Source Routing wird folgende Adress-Syntax verwendet:

```
@ONE,@TWO:JOE@THREE
```

Diese Adresse legt die Route der Email fest. Sie wird über `ONE` und `TWO` an `JOE` auf Host `THREE` gesendet.

Die Option gibt an, ob alle Empfänger mit Ausnahme von `JOE@THREE` ausgeschlossen werden sollen (`NO`) oder ob die Adresse beibehalten werden soll (`YES`).

Syntax:

```
AllowSourceRouting "YES|NO"
```

Voreingestellt:

```
AllowSourceRouting NO
```

InEnvelopeAddressesBangIs

Ausrufezeichen in Umschlagadresse (nicht im Milter-Modus)

Wenn der Parameter auf `REFUSED` gesetzt ist und die Empfängeradresse ein Ausrufezeichen enthält, wird die Nachricht zurückgewiesen.

Bei der Einstellung `IGNORED` werden Ausrufezeichen in Empfängeradressen wie normale Zeichen behandelt.

Bei `INTERPRETED` wird die Empfängeradresse in das RFC821-Standardformat umgewandelt. Aus der Adresse
`hostA!hostB!hostC!user`
wird beispielsweise
`hostA,@hostB:user@hostC`

Wenn Source Routing aktiviert ist, wird die Email an hostA gesendet, andernfalls an hostC.

Syntax:

```
InEnvelopeAddressesBangIs "Option"
```

Beispiel:

```
InEnvelopeAddressesBangIs IGNORED | REFUSED | INTERPRE-
TED
```

Voreingestellt:

```
InEnvelopeAddressesBangIs  REFUSED
```

InEnvelope Addresses PercentIs

Prozentzeichen in Umschlagadresse (nicht im Milter-Modus)

Wenn der Parameter auf `REFUSED` gesetzt ist und die Empfängeradresse ein Prozentzeichen enthält, wird die Nachricht zurückgewiesen.

Bei der Einstellung `IGNORED` werden Prozentzeichen in Adressen wie normale Zeichen behandelt.

Bei `INTERPRETED` wird die Empfängeradresse in das RFC821-Standardformat umgewandelt. Aus der Adresse

```
user%hostC%hostB@hostA
```

wird beispielsweise

```
@hostA,@hostB:user@hostC
```

Wenn Source Routing aktiviert ist, wird die Email an hostA gesendet, andernfalls an hostC.

Syntax:

```
InEnvelopeAddressesPercentIs "Option"
```

Beispiel:

```
InEnvelopeAddressesPercentIs IGNORED | REFUSED |
INTERPRETED
```

Voreingestellt:

```
InEnvelopeAddressesPercentIs REFUSED
```

AcceptLoose DomainName

Syntax von Email-Domains prüfen (nicht im Milter-Modus)

Ein Domain-Name darf nur die folgenden Zeichen enthalten: [-.0-9A-Za-z]
Der Parameter `AcceptLooseDomainName` erlaubt auch Domain-Namen, in denen diese Regel verletzt wird.

Die Einstellung `NO` bewirkt, dass eine Nachricht blockiert wird, wenn der Domain-Name für die Nachrichtenzustellung nicht korrekt ist (abhängig vom Source Routing).

Bei der Einstellung `YES` wird der Domain-Name nicht geprüft. Die Email wird in jedem Fall weitergeleitet.

Syntax:

```
AcceptLooseDomainName  "YES | NO"
```

Voreingestellt:

```
AcceptLooseDomainName   NO
```

AddressFilter

Email-Adressen filtern

Diese Option aktiviert bzw. deaktiviert den Adressfilter. Bei `NO` (Standardeinstellung) wird bei der Standardinstallation kein Adressfilter verwendet.

Syntax:

```
AddressFilter "YES | NO"
```

Voreingestellt:

```
AddressFilter NO
```

Damit der Adressfilter verwendet werden kann, sind die folgenden Dateien erforderlich:

```
/etc/avira/avmailgate.ignore
```

und

```
/etc/avira/avmailgate.scan
```

Diese Dateien enthalten Zeilen mit Email-Adressen und optional die Flags S/s (Absender) und/oder R/r (Empfänger). Die angegebenen Email-Adressen werden nur vom SMTP-Protokoll geprüft (MAIL FROM und RCPT TO). Die Email-Adressen in den Email-Headern werden ignoriert.

Die Listen werden geprüft. Die Prüfung beginnt mit der ersten Liste in `FilterTableOrder`. Bei einer Übereinstimmung wird die Prüfung beendet und die vorgesehene Aktion durchgeführt.

Abhängig vom Ergebnis gibt es folgende Möglichkeiten:

- Gibt es in der ersten Liste keine Übereinstimmung, wird die nächste Liste geprüft.
- Gibt es auch in der zweiten Liste keine Übereinstimmung, wird die Email geprüft.
- Gibt es in der Ignore-Liste eine Übereinstimmung, wird die Email nicht geprüft.
- Gibt es in der Scan-Liste eine Übereinstimmung, wird die Email geprüft.

Die Email-Adressen dürfen reguläre Ausdrücke im Perl-Format enthalten, z. B.

```
/abc/
/^abc/
/xyz/i
/^abc@def\.tld/
```

Beispiel:

/etc/avira/avmailgate.ignore enthält folgende Zeilen:

```
/^somebody@somewhere\.tld$/ SR
/^virus@firm/ R
/^abc@def.*\.tld/i
```

Die Email wird nicht geprüft, wenn die Adresse somebody@somewhere.tld lautet.

Die Email wird nicht geprüft, wenn die Empfängeradresse virus@firm* lautet. In diesem Fall ist das R-Flag optional:

/^virus@firm/ R ist gleichbedeutend mit */^virus@firm/*.

Beim Start von Avira AntiVir MailGate werden Log-Einträge geschrieben, die anzeigen, ob der Adressfilter aktiv oder inaktiv ist:

```
addressfilter is active
table order is: ignore,scan
```

oder

```
addressfilter is not active
```

Empfängeradressen Gruppen zuordnen

Um detaillierte Statistiken über den Email-Verkehr zu erstellen, ist es hilfreich, die Empfänger Gruppen zuzuordnen. Dies kann entweder mithilfe eines ActiveDirectory-Servers oder einer einfachen Textdatei geschehen.

Um einen ActiveDirectory-Server zu verwenden, muss die Konfigurationsoption ActiveDirectoryURI (siehe ActiveDirectoryServerURI – Seite 44) auf die URI gesetzt werden, unter der der ActiveDirectory-Server erreicht werden kann.

Steht kein ActiveDirectory-Server zur Verfügung oder soll dieser nicht genutzt werden, muss ActiveDirectoryServerURI auf die zu verwendende Textdatei verweisen. Dabei muss der Dateiname als einfacher Dateipfad angegeben werden, z. B. als

/etc/avira/avmailgate.groups

Bitte verwenden Sie nur eindeutige, einzelne Pfadangaben, keine multiplen Dateipfade.

In dieser Datei werden die Email-Adressen mithilfe von regulären Ausdrücken den gewünschten Gruppen zugeordnet. Die verwendeten regulären Ausdrücke werden in PCRE-Syntax angegeben.

Zeilen, die mit einem Raute-Symbol (#) beginnen, werden dabei ignoriert.

Jede Zeile beginnt mit dem Schlüsselwort "grp", gefolgt von einem Leerzeichen. Auf das Leerzeichen folgt ein regulärer Ausdruck im Perl-Format. Den Abschluss bilden ein weiteres Leerzeichen und der Gruppenname. Diesem Gruppennamen werden alle Adressen zugeordnet, die dem angegebenen regulären Ausdruck

entsprechen.

Beispiel:

```
grp /^person\d+@example.com$/ groupOne
```

In diesem Fall würden alle Adressen, die mit der Angabe 'person' beginnen, gefolgt von einer oder mehreren Ziffern und '@example.com' der Gruppe 'groupOne' zugeordnet werden.

Zuordnung der Email-Adressen zu Organisationseinheiten

Mithilfe des ActiveDirectory-Servers kann Avira AntiVir MailGate eine Zuordnung der Email-Adressen von gegebenen Benutzern zu Organisationseinheiten vornehmen.

Nachstehende Erklärung bezieht sich auf die Verwendung eines ActiveDirectory-Servers und gilt nicht, falls Sie in ActiveDirectoryServerURI eine Textdatei angegeben haben.

Die Reihenfolge in der Liste ist die folgende:

- Die Liste beginnt mit den Organisationseinheiten der memberOf-Attribute und ihren zugeordneten Benutzern. Die Auflistung erfolgt in alphabetischer Reihenfolge.
- Falls eine der dem Benutzer zugeordneten Gruppen als primäre Gruppe (primary group) gekennzeichnet ist, wird der Distinguished Name dieser Gruppe ebenfalls in die Liste aufgenommen.
- Dann folgt der Distinguished Name des Elternelements des ActiveDirectory-Eintrags des Benutzers.

Haben Sie die Optionen ActiveDirectoryGroupBlackList – Seite 48 oder ActiveDirectoryGroup WhiteList – Seite 48 konfiguriert, schreibt Avira AntiVir MailGate anhand obiger Vorlage die Listeneinträge. Dadurch können Elemente aus der Liste ausgeblendet sein. Das erste Element der ausgegebenen Liste ist dann die Organisationseinheit des Benutzers.

Folgende Konfigurationsoptionen stehen zur Verfügung:

ActiveDirectory Support

ActiveDirectory Support

Diese Option aktiviert und deaktiviert die Funktion. Sie ist standardmäßig deaktiviert und kann durch

```
ActiveDirectorySupport YES
```

aktiviert werden.

Syntax:

```
ActiveDirectorySupport "YES | NO"
```

Voreingestellt:

```
ActiveDirectorySupport NO
```

Nun kann die Zuordnung der Email-Adressen zu Organisationseinheiten mithilfe des Active Directory Servers vorgenommen werden.

***Warnung**: Verzichten Sie bei der Konfiguration der InetProtocols auf IPv4-Unterstützung, werden automatisch sowohl die ActiveDirectory- als auch die SNMP-Unterstützung deaktiviert, da diese auf IPv4 zurückgreifen.Folgende Einstellungen erforden die IPv4-Unterstützung:*
Milter-Modus, ActiveDirectory Support und SNMP-Unterstützung.

ActiveDirectory ServerURI

Zugriff auf den ActiveDirectory-Server

Diese Option legt fest wie der ActiveDirectory-Server erreicht werden kann. Es kann auch ein Dateipfad angegeben werden, falls kein ActiveDirectory-Server, sondern eine Textdatei mit Gruppenzuordnung genutzt werden soll.

Syntax:

```
ActiveDirectoryServerURI "Zeichenfolge"
```

Voreingestellt:

```
ActiveDirectoryServerURI ldap://my.ad-server.com:389
```

Eine gültige LDAP-URI für einen Active Directory-Server ist wie folgt aufgebaut:

Beispiel:

```
ActiveDirectoryServerURI /path/to/file
```

Oder geben Sie einen absoluten Dateinamen ein, wie

```
ActiveDirectoryServerURI /etc/avira/avmailgate.groups
```

Wird kein ActiveDirectory-Server benötigt, werden die Zuordnungen der Email-Adressen zu den Gruppennamen automatisch aus der Datei ausgelesen.

Es können auch mehrere LDAP-URIs angegeben werden. Die einzelnen URIs müssen in diesem Fall durch ein Leerzeichen getrennt sein und müssen die gleichen Login-Daten haben.

Beispiel:

```
ActiveDirectoryServerURI ldap://my.ad-server1.com
ldap://my.ad-server2.com ldap://my.ad-server3.com
```

Es ist nicht möglich, sowohl einen Dateipfad als auch einen oder mehrere LDAP-URIs anzugeben.

ActiveDirectory BaseDN

ActiveDirectory BaseDN

Diese Option legt die Verzweigung des ActiveDirectory-Baumes fest, bei dem die Suche nach Email-Adressen begonnen werden soll. Wenn Sie die ActiveDirectory Unterstützung konfigurieren ist die Einstellung dieses Parameters obligatorisch.

Syntax:

```
ActiveDirectoryBaseDN "Zeichenfolge"
```

Voreingestellt:

```
ActiveDirectoryBaseDN
```

Beispiel:

```
ActiveDirectoryBaseDN dc=example,dc=com
```

ActiveDirectory Login

ActiveDirectoryLogin

Diese Option bestimmt den Benutzernamen, mit dem auf den ActiveDirectory-Server eingeloggt werden soll. Der Benutzername muss als Distinguished Name angegeben werden.

Syntax:

```
ActiveDirectoryLogin "Zeichenfolge"
```

Voreingestellt:

```
ActiveDirectoryLogin
```

Beispiel:

```
ActiveDirectoryLogin
cn=Administrator,cn=Users,dc=mail,dc=example,dc=com
```

Wird kein Benutzername angegeben, schickt Avira AntiVir MailGate anonyme Queries. Sollte Ihr ActiveDirectory-Server jedoch keine anonymen Abfragen erlauben, schlagen diese Queries fehl.

ActiveDirectory Password

ActiveDirectory Passwort

Diese Option bestimmt das zum `ActiveDirectoryLogin` zugehörige Passwort.

Syntax:

```
ActiveDirectoryPassword "Zeichenfolge"
```

Beispiel:

```
ActiveDirectoryPassword geheim
```

Voreingestellt:

```
ActiveDirectoryPassword ""
```

Für `ActiveDirectoryLogin` und `ActiveDirectoryPassword` kann nur jeweils eine Angabe (Benutzername oder Passwort) in der avmailgate.conf-Datei gemacht werden.

Ist kein `ActiveDirectoryLogin` angegeben, ist die Option `ActiveDirectoryPassword` hinfällig.

ActiveDirectory UseTLS

ActiveDirectoryUseTLS

Die Option `ActiveDirectoryUseTLS` ermöglicht die TLS-Verschlüsselung aller ActiveDirectory-Verbindungen. Sie aktivieren die TLS-Verschlüsselung, indem Sie die Option auf `YES` stellen:

```
ActiveDirectoryUseTLS YES
```

Syntax:

```
ActiveDirectoryUseTLS "YES | NO"
```

Voreingestellt:

```
ActiveDirectoryUseTLS NO
```

Warnung: *Um die TLS-Verschlüsselung zu nutzen, muss unter* `ActiveDirectoryCACertificates` *die entsprechende Datei angegeben sein. Beachten Sie außerdem, dass der unter* `ActiveDirectoryServerURI` *eingetragene Hostname dem Hostnamen entsprechen muss, der in der Zertifikatdatei hinterlegt ist.*

ActiveDirectory CACertificates

ActiveDirectoryCACertificates

Diese Option enthält den Pfad zu der Datei, die die Zertifikate aller Zertifizierungsstellen beinhaltet, die von Avira AntiVir MailGate anerkannt werden. Die einzelnen Zertifikate müssen Base64-kodiert sein.

Syntax:

```
ActiveDirectoryCACertificates "Pfadangabe"
```

Beispiel:

```
ActiveDirectoryCACertificates /etc/known_cas.crt
```

ActiveDirectory SASLAuth Mechanism

ActiveDirectorySASLAuthMechanisms

Mit dieser Option wird festgelegt, auf welche Weise Sie sich beim ActiveDirectory-Server authentifizieren. Zur Verfügung stehen `PLAIN` und `DIGEST-MD5`.

Syntax:

```
ActiveDirectorySASLAuthMechanism "Option"
```

Voreingestellt:

```
ActiveDirectorySASLAuthMechanism PLAIN
```

Es bei der Voreinstellung PLAIN zu belassen, birgt insofern ein Sicherheitsrisiko, als dass die Authentifizierung in diesem Fall als Klartext an den Server geschickt wird. Dadurch können Dritte, die Zugriff auf den Traffic im Netzwerk haben, an Ihre Login-Daten gelangen.
Es ist daher angeraten, PLAIN nur dann zu verwenden, wenn die Authentifizierung über eine mit TLS verschlüsselte Verbindung geschieht.

Warnung*: Wird DIGEST-MD5 verwendet, kann die Authentifizierung als Administrator u.U. fehlschlagen.*

ActiveDirectory SearchTimeout

ActiveDirectorySearchTimeout

Diese Option legt fest, nach wie vielen Millisekunden eine Suche abgebrochen werden soll (falls keine Antwort gesendet wurde).

Syntax:

```
ActiveDirectorySearchTimeout "nicht-negative Zahl"
```

Beispiel:

```
ActiveDirectorySearchTimeout 1000
```

Voreingestellt:

```
ActiveDirectorySearchTimeout 30000
```

ActiveDirectory BindTimeout

ActiveDirectoryBindTimeout

Diese Option legt fest, nach wie vielen Millisekunden Bind-Operationen abgebrochen werden sollen.

Syntax:

```
ActiveDirectoryBindTimeout "nicht-negative Zahl"
```

Beispiel:

```
ActiveDirectoryBindTimeout 1000
```

Voreingestellt:

```
ActiveDirectoryBindTimeout 5000
```

ActiveDirectory CacheSize

ActiveDirectoryCacheSize

Diese Option legt fest, wie viele LDAP-Abfragen von Avira AntiVir MailGate zwischengespeichert werden sollen. Dies hat den Vorteil, dass gleiche Abfragen nicht zum ActiveDirectory-Server gesendet werden müssen, sondern dass das Programm auf die im Cache gespeicherten Ergebnisse zurückgreifen kann. Dadurch lassen sich zukünftige Abfragen schneller bearbeiten.

Syntax:

```
ActiveDirectoryCacheSize "nicht-negative Zahl"
```

Beispiel:

```
ActiveDirectoryCacheSize 812
```

Voreingestellt:

```
ActiveDirectoryCacheSize 1024
```

Es können nicht beliebig viele Einträge gespeichert werden. Die Cache-Kapazität ist abhängig von der Größe des Arbeitsspeichers sowie der Länge des Suchergebnisses.

ActiveDirectory CacheTTL

ActiveDirectoryCacheTTL

Diese Option bestimmt, wie lange die LDAP-Abfragen im Cache gespeichert werden sollen. Die Einstellung `0` deaktiviert die Option.

Syntax:

```
ActiveDirectoryCacheTTL "timespan"
```

Beispiel:

```
ActiveDirectoryCacheTTL 10m
```

Voreingestellt:

```
ActiveDirectoryCacheTTL 30m
```

Empfängt Avira AntiVir MailGate innerhalb von 30 Minuten eine Email mit einem Empfänger, für den bereits eine Abfrage im Cache existiert, liest das Programm diesen Eintrag und muss nicht zusätzlich mit dem Active Directory Server kommunizieren.

ActiveDirectory CheckUser Account Control

ActiveDirectoryCheckUserAccountControl

Diese Option legt fest, dass beim Durchsuchen der Email-Adressen nur aktive ActiveDirectory-Konten als Suchergebnis geliefert werden, d.h. gesperrte Konten werden von den Suchergebnissen ausgeschlossen. Bei inaktiven Konten ist die Gruppenzuordnung nicht bestimmbar. In diesem Fall greift die OptionReject Unknown Recipients – Seite 49.

Syntax:

```
ActiveDirectoryCheckUserAccountControl "YES | NO"
```

Voreingestellt:

```
ActiveDirectoryCheckUserAccountControl YES
```

ActiveDirectory GroupBlackList

ActiveDirectoryGroup BlackList

Mithilfe dieser Option kann festgelegt werden, welche Organisationseinheiten in der Datenbank erfasst werden. Die Funktion Reject Unknown Recipients bleibt davon unberührt.

Die Namen dieser Einheiten sind in Form von Distinguished Names in eine Liste einzutragen und mit Semikolons zu separieren.

Syntax:

```
ActiveDirectoryGroupBlackList "Zeichenfolge"
```

Voreingestellt:

```
ActiveDirectoryGroupBlackList ErsterDN; ZweiterDN
```

Die aufgeführten Namen der Einheiten werden bei der Empfängersuche ignoriert. So besteht die Möglichkeit, bestimmte Organisationseinheiten von der Aufnahme in die Datenbank-Statistik auszuschließen.

Die Einstellungen der `ActiveDirectoryGroupBlackList` werden von den Einstellungen der `ActiveDirectoryGroupWhiteList` außer Kraft gesetzt.

ActiveDirectory Group WhiteList

ActiveDirectoryGroup WhiteList

Mithilfe dieser Option kann festgelegt werden, welche Organisationseinheiten in der Datenbank erfasst werden. Die Funktion Reject Unknown Recipients bleibt davon unberührt.

Die Namen dieser Einheiten sind in Form von Distinguished Names in eine Liste einzutragen und mit Semikolons zu separieren.

Syntax:

```
ActiveDirectoryGroupWhiteList "Zeichenfolge"
```

Voreingestellt:

```
ActiveDirectoryGroupWhite List ErsterDN; ZweiterDN
```

Diese aufgeführten Namen der Einheiten werden bei der Empfängersuche durchsucht. So besteht die Möglichkeit, ausschließlich diese Organisationseinheiten in die Datenbank-Statistik aufzunehmen.

Die Einstellungen der `ActiveDirectoryGroupWhiteList` setzen die Einstellungen der `ActiveDirectoryGroupBlackList` außer Kraft.

Reject Unknown Recipients

RejectUnknownRecipients

Diese Option sorgt dafür, dass Emails an Empfänger, die nicht im Verzeichnis stehen, einen nicht temporären Fehler (SMTP Code 550: „Angeforderte Maßnahme nicht ausgeführt: Mailbox nicht verfügbar“) auslösen. Vorübergehende Fehler lösen hingegen eine temporäre Fehlermeldung (SMTP-Code 450: „Angeforderte Email-Maßnahme nicht ausgeführt, Mailbox nicht verfügbar“) aus. Ein SMTP-Rückgabecode besteht typischwerweise aus einer dreistelligen Zahl, gefolgt von Text. Die erste Stelle des Rückgabecodes gibt den Grad der Schwere des Fehlers an, wobei 4xx eine Antwort über einen vorübergehenden negativen Abschluss und 5xx eine permanent negative Antwort klassifizieren. Die zweite Stelle gibt die Kategorie der Antwort an, wobei x5x der Kategorie Mail-System zugehörig ist. Die dritte Stelle spezifiziert die jeweilige Kategorie genauer.

Syntax:

```
RejectUnknownRecipients "YES | NO"
```

Voreingestellt:

```
RejectUnknownRecipients NO
```

Die Einstellung hat keinen Effekt, wenn der ActiveDirectorySupport ausgeschaltet ist.

Filter TableOrder

Prüfreihenfolge der Filtertabelle

Diese Option kann nur verwendet werden, wenn AddressFilter aktiv ist (`AddressFilter YES`).

Syntax:

```
FilterTableOrder "Option"
```

Die möglichen Parameter:

```
FilterTableOrder scan,ignore
```

oder

```
FilterTableOrder ignore,scan
```

Voreingestellt:

```
FilterTableOrder scan,ignore
```

SMTP Greeting Timeout

SMTPGreetingTimeout (nicht im Milter-Modus)

Diese Option legt das maximale Timeout (in Sekunden) für den Empfang der Grußmitteilung vom entfernten Host fest.

Syntax:

```
SMTPGreetingTimeout "nicht-negative Zahl"
```

Beispiel:

```
SMTPGreetingTimeout 100
```

Voreingestellt:

```
SMTPGreetingTimeout 300
```

SMTPHelo Timeout

SMTPHeloTimeout (nicht im Milter-Modus)

Diese Option legt das maximale Timeout (in Sekunden) für eine Antwort auf die SMTP-Befehle HELO und EHLO fest.

Syntax:

```
SMTPHeloTimeout "nicht-negative Zahl"
```

Beispiel:

```
SMTPHeloTimeout 100
```

Voreingestellt:

```
SMTPHeloTimeout 300
```

SMTP MailFrom Timeout

SMTPMailFromTimeout (nicht im Milter-Modus)

Diese Option legt das maximale Timeout (in Sekunden) für eine Antwort auf den Befehl MAIL FROM fest.

Syntax:

```
SMTPMailFromTimeout "nicht-negative Zahl"
```

Beispiel:

```
SMTPMailFromTimeout 100
```

Voreingestellt:

```
SMTPMailFromTimeout 300
```

SMTP Rcpt Timeout

SMTPRcptTimeout (nicht im Milter-Modus)

Diese Option legt das maximale Timeout (in Sekunden) für eine Antwort auf den Befehl RCPT TO fest.

Syntax:

```
SMTPRcptTimeout "nicht-negative Zahl"
```

Beispiel:

```
SMTPRcptTimeout 100
```

Voreingestellt:

```
SMTPRcptTimeout 300
```

SMTP Data Timeout

SMTPDataTimeout (nicht im Milter-Modus)

Diese Option legt das maximale Timeout (in Sekunden) für eine Antwort auf den Befehl DATA fest.

Syntax:

```
SMTPDataTimeout "nicht-negative Zahl"
```

Beispiel:

```
SMTPDataTimeout 100
```

Voreingestellt:

```
SMTPDataTimeout 120
```

SMTP DataBlock Timeout

SMTPDataBlockTimeout (nicht im Milter-Modus)

Diese Option legt das maximale Timeout (in Sekunden) beim Senden einzelner Datenblöcke fest.

Syntax:

```
SMTPDataBlockTimeout "nicht-negative Zahl"
```

Beispiel:

```
SMTPDataBlockTimeout 100
```

Voreingestellt:

```
SMTPDataBlockTimeout 180
```

SMTP DataPeriod Timeout

SMTPDataPeriodTimeout (nicht im Milter-Modus)

Diese Option legt das maximale Timeout (in Sekunden) für eine Antwort auf den abschließenden Punkt der Befehle DATA und QUIT nach dem Senden der Nachricht fest.

Syntax:

```
SMTPDataPeriodTimeout "nicht-negative Zahl"
```

Beispiel:

```
SMTPDataPeriodTimeout 100
```

Voreingestellt:

```
SMTPDataPeriodTimeout 600
```

Max Forwarders

Maximale Anzahl der Weiterleitungsprozesse (nicht im Milter-Modus)

Diese Option legt die maximale Anzahl gleichzeitiger Weiterleitungsprozesse fest. Der optimale Wert hängt von der Effizienz Ihres Email-Systems und von der Qualität der Email-Verbindung ab (Standardeinstellung: 10).

Syntax:

```
MaxForwarders "nicht-negative Zahl"
```

Beispiel:

```
MaxForwarders 5
```

Voreingestellt:

```
MaxForwarders 10
```

ForwardTo

Weiterleitung

Diese Option legt fest, wie Emails versendet werden (Standardeinstellung: durch Sendmail).

Voreingestellt:

```
ForwardTo /usr/lib/sendmail -oem -oi
```

Die Emails können auch durch SMTP versendet werden:

Syntax:

```
ForwardTo   SMTP: "Zeichenfolge" Port "Zeichenfolge"
```

oder

```
ForwardTo   SMTP: "Zeichenfolge" Port "Zahl"
```

z.B.:

```
ForwardTo   SMTP: localhost port 825
```

oder

```
ForwardTo   SMTP: localhost port smtp
```

Die SMTP-Einstellung ist nur wirksam, wenn Avira AntiVir MailGate im SMTP-Modus läuft. Im Milter-Modus können Emails nur vom Programm weitergeleitet werden. Der richtige Eintrag lautet in diesem Fall:

```
ForwardTo /path/to/file
```

Aktivieren Sie die IPv6-Unterstützung nur mithilfe der Option InetProtocols, müssen Sie für die Optionen ListenAddress, ForwardTo und ForwardTo2 sowie in der avmailgate.acl-Datei IPv6-Adressen angeben.

ForwardTo2

ForwardTo2

Über diese Option kann ein alternativer SMTP-Weiterleitungsserver eingerichtet werden, auf den zurückgegriffen wird, wenn die primäre Weiterleitung, die mit ForwardTo festgelegt wurde, fehlgeschlagen ist.

Syntax:

```
ForwardTo2 "Zeichenfolge"
```

Beispiel:

```
ForwardTo2 SMTP: smtp.example.com port 25
```

Avira AntiVir MailGate greift auf diese Einstellung zurück, wenn keine Verbindung zum primären Weiterleitungsserver hergestellt werden konnte oder ein SMTP-Befehl mit dem Status-Code 421 oder nicht in der festgelegten Zeit beantwortet wurde (Timeout).

UsePipelining InSMTPClient

UsePipeliningInSMTPClient

Diese Konfigurationsoption bestimmt, ob der in Avira AntiVir MailGate integrierte SMTP-Client die SMTP-Erweiterung Pipelining (nach RFC 2920) benutzt.

Syntax:

```
UsePipeliningInSMTPClient "YES | NO"
```

Voreingestellt:

```
UsePipeliningInSMTPClient NO
```

Zur Aktivierung dieser Option muss ein SMTP Server mithilfe der Option ForwardTo als Weiterleitungsagent eingerichtet sein und die Erweiterung Pipelining unterstützen. Die Zustellung der Emails wird durch diese Option erheblich beschleunigt, vor allem wenn Avira AntiVir MailGate auf einem anderen System als dem SMTP-Weiterleitungsserver installiert ist.

ScannerListen Address

ScannerListenAddress

Diese Option gibt den Speicherort des Scanner-Sockets an, damit Avira AntiVir MailGate die Verbindung herstellen und Prüfanfragen durchführen kann

Syntax:

```
ScannerListenAddress "Pfadangabe"
```

Voreingestellt:

```
ScannerListenAddress  /var/run/avmailgate/scanner
```

Wenn Sie diesen Parameter ändern, müssen Sie auch den Wert für `ListenAddress` *in* /etc/avira/avmailgate-scanner.conf *ändern (siehe Scanner-Konfiguration in avmailgate-scanner.conf – Seite 93).*

Max Attachments

Maximale Anzahl der Email-Anhänge (MIME)

Eine Email wird als verdächtig eingestuft, wenn sie die maximale Anzahl der Anhänge überschreitet (Standardeinstellung: `100`).
Siehe auch `BlockSuspiciousMime`.

Syntax:

```
MaxAttachments "nicht-negative Zahl"
```

Beispiel:

```
MaxAttachments 50
```

Voreingestellt:

```
MaxAttachments 100
```

Block Suspicious Mime

Verdächtige Emails blockieren (MIME)

Mithilfe dieser Option können Sie verdächtige MIME-Emails blockieren. Eine Email wird als verdächtig eingestuft, anhand von der `MaxAttachments`-Einstellung.

Syntax:

```
BlockSuspiciousMime "YES | NO"
```

Voreingestellt:

```
BlockSuspiciousMime NO
```

Block Fragmented Message

Fragmentierte Emails blockieren

Mithilfe dieses Parameters werden fragmentierte Emails blockiert. Weitere Informationen finden Sie unter „Message Fragmentation and Reassembly“ in RFC

2046 (http://www.faqs.org/rfcs/rfc2046.html, Absatz 5.2.2.1).

Syntax:

```
BlockFragmentedMessage "YES | NO"
```

Voreingestellt:

```
BlockFragmentedMessage NO
```

BlockPartial Archive

Aufgeteilte Archive blockieren

Ist diese Option aktiviert (YES), werden Emails mit Archiven blockiert, die Teil eines Multivolume-Archivs sind.

Syntax:

```
BlockPartialArchive  "YES | NO"
```

Voreingestellt:

```
BlockPartialArchive NO
```

Block Extensions

Emails mit bestimmten Erweiterungen blockieren

Avira AntiVir MailGate lässt sich so konfigurieren, dass Emails blockiert werden, die Anhänge mit bestimmten Dateierweiterungen enthalten (z. B. exe, scr oder pif). Die Sperre gilt auch für archivierte Dateien. Wenn dieser Parameter auf NO gesetzt ist, erlaubt MailGate jegliche Dateierweiterungen in Anhängen. Die zu blockierenden Dateierweiterungen müssen durch Semikolon getrennt sein.

Syntax:

```
BlockExtensions "extension1; extension2 | NO"
```

Voreingestellt:

```
BlockExtensions NO
```

Beispiel:

```
BlockExtensions exe;scr;pif
```

Jede einzelne Dateierweiterung darf aus maximal 120 Zeichen bestehen.

Expose Recipient Alerts

Alarme an Empfänger verdächtiger Emails senden

Sie können Alarme über Viren und unerwünschte Programme an den Empfänger senden. Die möglichen Werte:

- NO: der Empfänger erhält keinen Virenalarm.
- LOCAL: Alarmmeldungen werden nur gesendet, wenn der Empfänger ein lokaler Benutzer in Ihrer Domäne ist. Setzen Sie die Option in avmailgate.acl auf `local`.
- YES: der Empfänger erhält immer einen Virenalarm.

Syntax:

```
ExposeRecipientAllerts "Option"
ExposeRecipientAlerts YES | NO | LOCAL
```

Voreingestellt:

```
ExposeRecipientAlerts LOCAL
```

Expose SenderAlerts

Alarme an Absender verdächtiger Emails senden

Sie können Alarme über Viren und unerwünschte Programme an den Absender senden. Die möglichen Werte:

- NO: der Absender erhält keinen Virenalarm.
- LOCAL: Alarmmeldungen werden nur gesendet, wenn der Absender ein lokaler Benutzer in Ihrer Domain ist. Setzen Sie die Option in avmailgate.acl auf `local`.
- YES: der Absender einer verdächtigen Email erhält immer einen Virenalarm.

Syntax:

```
ExposeSenderAlerts "Option"
ExposeSenderAlerts YES | NO | LOCAL
```

Voreingestellt:

```
ExposeSenderAlerts LOCAL
```

Expose Postmaster Alerts

Alarme an den Postmaster senden

Sie können Alarme über Viren und unerwünschte Programme an den Postmaster senden.

Syntax:

```
ExposePostmasterAlerts "YES | NO"
```

Voreingestellt:

```
ExposePostmasterAlerts YES
```

AlertsUser

Absender von Warnungen

Spezifiziert den Absender einer Email-Benachrichtigung, wenn ein Virus oder ein unerwünschtes Programm entdeckt wird.

Syntax:

```
AlertsUser "Zeichenfolge"
```

Voreingestellt:

```
AlertsUser AvMailGate
```

***Warnung**: Verzichten Sie bei der Konfiguration der InetProtocols auf IPv4-Unterstützung, werden automatisch sowohl die ActiveDirectory- als auch die SNMP-Unterstützung deaktiviert, da diese auf IPv4 zurückgreifen. Folgende Einstellungen erforden die IPv4-Unterstützung:*
Milter-Modus, ActiveDirectory Support und SNMP-Unterstützung.

SNMP Recipient

SNMP Recipient

Avira AntiVir MailGate kann so konfiguriert werden, dass die Administratoren per SNMP-Traps über Ereignisse wie z. B. Virenfunde informiert werden. Eine Spezifikation dieser Traps wird im MIB-Format in den Dateien AVIRA-MIB.txt und

AVIRA-MAILGATE-V0-MIB.txt mitgeliefert.

Syntax:

```
SNMPRecipient Hostname|IP-Adresse[:Port]
```

Voreingestellt:

```
SNMPRecipient ""
```

Beispiel, geben Sie

```
SNMPRecipient localhost:162
```

in die *avmailgate.conf* ein, um den Hostnamen oder die IP-Adresse, an die die SNMP-Traps versendet werden sollen, festzulegen. Diese Angabe kann optional durch einen Doppelpunkt, gefolgt von der gewünschten Portnummer ergänzt werden, wenn z. B. nicht der Standard-Port genutzt werden soll.

Die Einstellung SNMPRecipient ist nur wirksam, wenn die SNMP-Benachrichtungen mit Hilfe der Notification Mechanisms aktiviert wurden.

SNMPSender

Absender für SNMP-Traps einstellen

Mit dieser Option kann festgelegt werden, welche IP-Adresse als Absender-Adresse in SNMP-Traps angegeben wird. Falls ein Hostname angegeben wird, wird dieser dazu genutzt, per DNS-Lookup die zu verwendende IP-Adresse zu ermitteln.

Syntax:

```
SNMPSender "IP-Adresse|Hostname"
```

Beispiel:

```
SNMPSender 192.168.1.100
```

Die Einstellung SNMPSender ist nur wirksam, wenn die SNMP-Benachrichtungen mit Hilfe der Notification Mechanisms aktiviert wurden.

SNMP Community

SNMP Community

Anwendungen, die SNMP unterstützen, können anhand ihrer Community-Zugehörigkeit gruppiert werden. Die Angabe der Gruppenzugehörigkeit ist auf 255 Zeichen begrenzt.

Syntax:

```
SNMPCommunity "Zeichenfolge"
```

Voreingestellt:

```
SNMPCommunity Avira
```

Die Einstellung SNMPCommunity ist nur wirksam, wenn die SNMP-Benachrichtungen mit Hilfe der Notification Mechanisms aktiviert wurden.

Notification Mechanisms

NotificationMechanisms

Sobald Avira AntiVir MailGate ein Problem feststellt, kann eine Email-

Benachrichtung an den Postmaster versendet werden. Zu diesen Problemen gehört z. B., dass MailGate versucht, eine Email zu scannen und dabei die Verbindung zu SAVAPI fehlschlägt.

Syntax:

```
NotificationMechanisms "Zeichenfolge"
```

Gültige Optionen:

```
NotificationMachanisms EMAIL; SNMP | NONE
```

Voreingestellt:

```
NotificationMechanisms EMAIL
```

Wenn die Konfiguration auf

```
EMAIL
```

gesetzt ist, wird eine Benachrichtigung per Email versendet.

Wenn die Konfiguration auf

```
EMAIL; SNMP
```

gesetzt ist, wird eine Beachrichtigung per Email und per SNMP-Traps versendet.

Wenn die Konfiguration auf

```
NONE
```

gesetzt ist, wird keine Benachrichtigung versendet.

Die Email-Benachrichtigungen sind standardmäßig aktiviert. SNMP-Traps sind standardmäßig deaktiviert. Um SNMP-Traps versenden zu können, müssen Sie einen gültigen SNMP-Empfänger (SNMP Recipient) angeben.

Mithilfe der Konfigurationsoption Postmaster legen Sie den Empfänger der Benachrichtigungen fest.

AddStatus InBody

Statusinformationen im Text der Email

Bei der Einstellung NO enthält die Email keine zusätzlichen Informationen.

Syntax:

```
AddStatusInBody "YES | NO"
AddStatusInBody /path/to/file
```

Voreingestellt:

```
AddStatusInBody NO
```

Bei der Einstellung YES gibt es folgende Möglichkeiten:

- Existiert im Vorlagen-Unterverzeichnis des Programms eine Datei namens `body-state`, wird der Text aus dieser Datei in die Email eingefügt (siehe Berichtvorlagen konfigurieren – Seite 97).

- Sie können `AddStatusInBody` auch den Namen einer Datei zuweisen. In diesem Fall wird der Inhalt der angegebenen Datei verwendet.

`AddStatusInBody` modifiziert die Email kurz vor der Weiterleitung, d. h. es

werden nur saubere Emails modifiziert.

MaxMessage SizeStatus

Statustext

Ist die Option `AddStatusInBody` auf `YES` gesetzt, wird einer Email, die die angegebene Größe überschreitet, kein Statustext hinzugefügt. Sie können die Größe in `Gigabytes (GB), Megabytes (MB), Kilobytes` (`KB`) oder `Bytes` eingeben.

Syntax:

```
MaxMessageSizeStatus "Größe"
```

Beispiele:

```
MaxMessageSizeStatus 4KB,3MB
```

Voreingestellt:

```
MaxMessageSizeStatus 0
```

ForwardAll EmailAsMIME

Emails als MIME weiterleiten (nicht im Milter-Modus)

Emails, die nicht im MIME-Format vorliegen, können in dieses Format umgewandelt werden. Sie verfügen dann über einen MIME-Header mit `content type: text/plain`, `content disposition: inline` und `content encoding: 7 bit` oder `8 bit`. Die Verschlüsselung hängt von der ursprünglichen Email ab.

Bei der Einstellung NO werden Emails, die nicht im MIME-Format vorliegen, ohne weitere Verarbeitung gesendet.

Bei der Einstellung YES werden diese Emails in das MIME-Format umgewandelt.

Syntax:

```
ForwardAllEmailAsMIME   "YES | NO"
```

Voreingestellt:

```
ForwardAllEmailAsMIME NO
```

ScanInArchive

Archive prüfen

Bei der Einstellung NO werden Archive nicht auf Viren und unerwünschte Programme geprüft.

Bei der Einstellung YES werden alle archivierten Dateien entpackt und geprüft. Dabei gelten die Einstellungen in `ArchiveMaxSize`, `ArchiveMaxRecursion` und `ArchiveMaxRatio`.

Syntax:

```
ScanInArchive     "YES | NO"
```

Voreingestellt:

```
ScanInArchive YES
```

Archive MaxSize

Maximale Größe archivierter Dateien im entpackten Zustand

Es gibt archivierte Dateien mit nutzlosem Inhalt, die sich beim Entpacken zu bedeutender Größe „aufblähen“, um in voller Absicht die Rechnerleistung herabzusetzen. Dieser Parameter verhindert, dass solche Archivdateien entpackt werden.

Bei der Einstellung 0 werden alle archivierten Dateien unabhängig von ihrer Größe entpackt.

Bei einer Einstellung >0 werden alle Archive entpackt und geprüft, die die angegebene Größe (in Byte) nicht überschreiten.

Wenn MailGate im Milter Modus läuft und der Wert der Option ArchiveMaxSize auf weniger als 5120 Bytes gesetzt wurde, gibt MailGate folgende Warnmeldung aus, die gespeichert wird:

Warnung: Der Wert der Option ArchiveMaxSize (n) ist kleiner als der empfohlene Wert (5120). Es wird dringend empfohlen, diesen Wert auf 5120 oder höher zu setzen, da sonst unter Umständen MailGates Benachrichtigungs-Emails blockiert werden.
Wobei (n) der Konfigurationswert von ArchiveMaxSize ist.

Syntax:

```
ArchiveMaxSize "Größe"
```

Beispiele:

```
ArchiveMaxSize 2KB (2 Kilobyte), 3MB (3 Megabyte)
```

Voreingestellt:

```
ArchiveMaxSize 0
```

ArchiveMax Ratio

„Mail-Bomben“ blockieren

So genannte „Mail-Bomben“ mit einer sehr hohen Kompressionsrate können blockiert werden. Sie können die maximale Differenz zwischen der gepackten und der entpackten Dateigröße festlegen.

Die Einstellung 0 deaktiviert die Option (**nicht** empfehlenswert). Die Standardeinstellung lautet 150.

Syntax:

```
ArchiveMaxRatio "nicht-negative Zahl"
```

Beispiel:

```
ArchiveMaxRatio 100
```

Voreingestellt:

```
ArchiveMaxRatio 150
```

ArchiveMax Recursion

Maximale Rekursionstiefe in Archiven

Bei der Einstellung 0 werden rekursive (verschachtelte) Archive unabhängig von ihrer Rekursionstiefe entpackt.

Bei einer Einstellung >0 werden alle Archive entpackt, die die angegebene Rekursionstiefe nicht überschreiten. Dadurch wird die Verarbeitungszeit herabgesetzt.

Syntax:

```
ArchiveMaxRecursion "nicht-negative Zahl"
```

Beispiel:

```
ArchiveMaxRecursion 10
```

Voreingestellt:

```
ArchiveMaxRecursion 20
```

Block Suspicious Archive

Emails mit verdächtigen Archiven blockieren

Ist diese Option aktiviert (YES), werden Archive gesperrt, die Avira AntiVir MailGate als verdächtig eingestuft hat.
Als verdächtig gelten alle Archive, die nicht vollständig gescannt werden konnten. Ausserdem gelten all jene Archive als verdächtig, die einen der in `ArchiveMaxSize`, `ArchiveMaxRecursion` und `ArchiveMaxRatio` festgelegten Grenzwerte überschreiten.

Syntax:

```
BlockSuspiciousArchive    "YES | NO"
```

Ist die Option deaktiviert (NO), werden auch verdächtige Archive weitergeleitet.

Voreingestellt:

```
BlockSuspiciousArchive NO
```

Block Encrypted Archive

Emails mit passwortgeschützten Archiven blockieren

Bei der Einstellung `YES` werden Emails mit passwortgeschützten Dateien in Archiven blockiert.

Syntax:

```
BlockEncryptedArchive    "YES | NO"
```

Bei `NO` werden auch Emails mit verschlüsselten Archiven zugestellt.

Voreingestellt:

```
BlockEncryptedArchive NO
```

Encrypted EmailAction

Handhabung verschlüsselter Emails

Avira AntiVir MailGate kann mit verschlüsselten Emails auf drei unterschiedliche Weisen verfahren.

Syntax:

```
EncryptedEmailAction "Option"
```

Voreingestellt:

```
EncryptedEmailAction IGNORE
```

1. Die Email wird ohne Log-Eintrag oder Benachrichtigung zugestellt/weitergeleitet (voreingestellt).
   ```
   EncryptedEmailAction IGNORE
   ```
2. Die Email wird zugestellt/weitergeleitet und der Postmaster wird darüber benachrichtigt.
   ```
   EncryptedEmailAction NOTIFY_POSTMASTER
   ```
3. Die Email wird als verdächtig ('suspicious') eingestuft. D.h. sie wird nicht zugestellt/weitergeleitet.
   ```
   EncryptedEmailAction TREAT_AS_SUSPICIOUS
   ```

Um Benachrichtigungen über das Eintreffen verschlüsselter Emails zu erhalten, ist es nowendig, in den Notification Mechanisms `EMAIL` *anzugeben.*

`EncryptedEmailAction` *kann nur auf vollständig verschlüsselte Emails angewendet werden. Bei Emails, bei denen z. B. nur der Anhang verschlüsselt ist, greift die Option nicht.*

InetProtocols

InetProtocols

Es ist möglich, zusätzlich zu dem voreingestellten IPv4 ebenfalls IPv6 zu verwenden. Auch eine alleinige Nutzung von IPv6 kann gewählt werden.

Syntax:

```
InetProtocols "Zeichenfolge"
```

Voreingestellt:

```
InetProtocols IPv4
```

Ändern Sie dazu die Voreinstellung

```
InetProtocols IPv4
```

entsprechend Ihrer Wünsche, z. B. in

```
InetProtocols IPv4 ; IPv6
```

Aktivieren Sie nur die IPv6-Unterstützung, müssen Sie für die Optionen ListenAddress und ForwardTo sowie in der avmailgate.acl-Datei IPv6-Adressen angeben.

***Warnung**: Verzichten Sie auf IPv4-Unterstützung, werden automatisch sowohl die ActiveDirectory- als auch die SNMP-Unterstützung deaktiviert, da diese auf IPv4 zurückgreifen. Folgende Einstellungen erforden die IPv4-Unterstützung: Milter-Modus, ActiveDirectory Support und SNMP-Unterstützung.*

Detect...

Erkennung weiterer unerwünschter Programme

Neben Viren gibt es weitere schädliche oder unerwünschte Software, die in

avmailgate.conf beschrieben wird. Die Erkennung dieser Software kann mithilfe nachstehender Optionen aktiviert werden, deren Voreinstellungen die folgenden sind:

Voreingestellt:

- `DetectADSPY yes`
  Erkennt Software, die unerwünschte Werbe-Pop-ups anzeigt, oder benutzerspezifische Daten an Dritte sendet.
- `DetectAPPL no`
  Erkennt Anwendungen fragwürdiger Herkunft und Anwendungen, deren Nutzung gefährlich sein kann.
- `DetectBDC yes`
  Erkennt Zugriffskontroll-Software für Backdoors. Normalerweise sind diese harmlos.
- `DetectDIAL yes`
  Erkennt Dial-up Programme, die kostenpflichtige Verbindungen herstellen. Dial-up Programme können immense Kosten verursachen.
- `DetectGAME no`
  Entdeckt Spiele-Software, die keinen Schaden auf Ihrem Computer anrichtet.
- `DetectHIDDENEXT yes`
  Entdeckt Dateien mit ausführbaren Datei-Erweiterungen, die hinter harmlosen Dateien versteckt sind.
- `DetectJOKE no`
  Entdeckt harmlose Spaß-Software.
- `DetectPCK yes`
  Entdeckt Dateien, die durch ein ungewöhnliches Laufzeitverkürzung-Packprogramm komprimiert wurden. Vergewissern Sie sich, dass die Herkunft der Dateien vertrauenswürdig ist.
- `DetectPHISH yes`
  Entdeckt gefälschte Emails, die den Benutzer auffordern, vertrauliche Informationen wie Benutzerkonten, Kennwörter oder Online-Banking Daten an bestimmte Webseiten weiterzugeben.
- `DetectSPR no`
  Entdeckt Software, die die Sicherheit Ihres Systems gefährdet, unerwünschte Programme startet, in Ihren privaten Daten Schaden verursacht oder Ihr Benutzerverhalten ausspioniert.

Heuristics Macro

Makrovirus-Heuristik

Diese Option aktiviert die Heuristik für Makroviren in Dokumenten.

Syntax:

```
Heuristicsmacro "YES | NO"
```

Voreingestellt:

```
HeuristicsMacro YES
```

Heuristics Level

Win32-Heuristik

Diese Option legt die Erkennungsstufe der Win32-Heuristik fest. Zulässige Werte sind `0` (Aus), `1` (Niedrig), `2` (Mittel) und `3` (Hoch).

Syntax:

```
HeuristicsLevel "nicht-negative Zahl"
```

Beispiel:

```
HeuristicsLevel 1
```

Voreingestellt:

```
HeuristicsLevel 3
```

Block OnError

Emails bei Prüffehler blockieren

Bei der Einstellung YES werden Emails blockiert, wenn beim Prüfen von Archiven im Anhang ein Fehler auftritt oder der Prüfvorgang durch ein Timeout beendet wurde.

Syntax:

```
BlockOnError "YES | NO"
```

Voreingestellt:

```
BlockOnError NO
```

Block Unsupported Archive

Emails mit nicht unterstützten Archiven blockieren

Emails mit Archiven, die der Scanner nicht unterstützt, werden blockiert.

Syntax:

```
BlockUnsupportedArchive "YES | NO"
```

Voreingestellt:

```
BlockUnsupportedArchive NO
```

Reject AlertMail

Emails blockieren, die als infiziert erkannt sind

(Nur im Milter-Modus verfügbar) Wenn `RejectAlertMail` auf `YES` gesetzt ist, werden Emails, die als infiziert erkannt sind, mit der Meldung „Alert found in email“ blockiert und in das Quarantäneverzeichnis gelegt (abhängig von der Einstellung für QuarantineAlert).

Syntax:

```
RejectAlertMail "YES | NO"
```

Wenn `RejectAlertMail` auf `NO` gesetzt ist, wird die Email angenommen und in das Quarantäneverzeichnis gelegt.

Voreingestellt:

```
RejectAlertMail NO
```

Quarantäneverzeichnis

Blockierte Emails werden in das Quarantäneverzeichnis abgelegt. Sie können aus diesem Verzeichnis manuell entfernt werden. Geben Sie Folgendes ein, um alle blockierten Emails zu entfernen (siehe auch 6.4 Quarantäne-Management und nachstehende Option **AlertAction**)

```
avmailgate.bin --avq --remove=all
```

Quarantine Alert

Alarm-Emails in Quarantäne nehmen

(Nur im Milter-Modus verfügbar) Wenn sowohl `QuarantineAlert` als auch `RejectAlertMail` auf `YES` gesetzt sind, werden Emails, die als infiziert erkannt sind, blockiert und in Quarantäne genommen.

Wenn `QuarantineAlert` auf `NO` und `RejectAlertMail` auf `YES` gesetzt ist, wird die Email blockiert und nicht in Quarantäne genommen.

Syntax:

```
QuarantineAlert "YES | NO"
```

Voreingestellt:

```
QuarantineAlert YES
```

AlertAction

AlertAction

Diese Option legt fest, ob infizierte oder verdächtige Emails in Quarantäne genommen oder sofort gelöscht werden. Unabhängig davon, wie Sie `EnableLegacyQuarantine` konfiguriert haben, werden folgende Werte akzeptiert:

- `QUARANTINE` Emails, die als infiziert erkannt oder verdächtig sind, werden in Quarantäne genommen.
- `DELETE_ALERTS` Emails, die als infiziert erkannt sind, werden gelöscht. Verdächtige Emails werden in Quarantäne genommen.
- `DELETE_ALL` Sowohl verdächtige als auch Emails, die als infiziert erkannt sind, werden gelöscht.

Syntax:

```
AlertAction "Option"
```

Voreingestellt:

```
AlertAction QUARANTINE
```

Enhanced QueueHandling

Länge der Warteschlangen einschränken

(Nicht im Milter-Modus verfügbar) Sowohl die Warteschlange der eingehenden (`incoming`) als auch die der ausgehenden (`outgoing`) Emails kann in ihrer Auslastung beschränkt werden. Sie können diese Funktion separat für jede Warteschlange aktivieren.

Die festzulegenden Parameter für die Warteschlange der eingehenden Emails lauten:

Syntax:

```
IncomingHighFillLevel "nicht-negative Zahl"
IncomingLowFillLevel "nicht-negative Zahl"
```

Für die Warteschlange der ausgehenden Emails:

Syntax:

```
OutgoingHighFillLevel "nicht-negative Zahl"
OutgoingLowFillLevel "nicht-negative Zahl"
```

Voreingestellt für alle Parameter ist:

```
0
```

Dazu werden ein maximaler (`HighFillLevel`) und ein minimaler Schwellwert (`LowFillLevel`) festgelegt. Sobald der maximale Wert erreicht ist, werden weitere Emails durch eine temporäre Fehlermeldung (SMTP Code 452: ungenügender Speicherplatz) blockiert. Je nach Leistung und Auslastung des Systems kann der Schwellwert auch geringfügig überschritten werden. Indem Sie einen gültigen Schwellwert festlegen, spezifizieren Sie, bei welcher Anzahl von Emails die `incoming` oder `outgoing` Warteschlange als „ausgelastetet“ oder „verfügbar“ gilt. Neue Verbindungen werden solange nicht akzeptiert, bis die Anzahl der Emails in der Warteschlange auf den Minimalwert `(LowFillLevel)` oder darunter gesunken ist.
Beim Starten wird der Status jeder Warteschlange auf „verfügbar“ zurückgesetzt. Wenn die Anzahl der Emails gleich oder größer ist als der definierte `HighFillLevel`, wird die Warteschlange als „ausgelastet“ eingestuft. Ist die Anzahl der Emails gleich oder kleiner ihres `LowFillLevels` wird die Warteschlange als „verfügbar“ eingestuft. Ist die Anzahl der Emails in einer Warteschlange kleiner als der definierte `HighFillLevel` aber größer als der eingegebene `LowFillLevel` gilt die Warteschlange als „ausgelastet“ und bleibt in diesem Status. Um diesen Stand zu ändern, muss die Anzahl der Emails dieser Warteschlange unter den eingestellten `LowFillLevel` sinken.

Bei Neustart akzeptiert Avira AntiVir MailGate neue Emails unabhängig vom vorherigen Status. Das System behält ein vorheriges „ausgelastet“ nicht.

Beim Erreichen des eingestellten Schwellwertes wird der Postmaster mithilfe der Notification Mechanisms-Funktion per SNMP-Trap oder Email informiert.

Bitte beachten Sie, dass auch von Avira AntiVir MailGate erstellte Emails gezählt werden.

Folgende Angaben sind gültig:

- Der Schwellwert für sowohl `HighFillLevel` als auch `LowFillLevel` beträgt 0 (voreingestellt).
- Der Schwellwert für `HighFillLevel` ist höher als der für `LowFillLevel`.

Falls ungültige Angaben gemacht werden, startet Avira AntiVir MailGate nicht.

PollPeriod

Warteschlange prüfen (nicht im Milter-Modus)

Diese Option legt das Intervall fest, in dem das Programm die Email-Warteschlange nach Viren und Malware durchsucht (in Sekunden).

Syntax:

```
PollPeriod "nicht-negative Zahl"
```

Beispiel:

```
PollPeriod 30
```

Voreingestellt:

```
PollPeriod 60
```

Queue Lifetime

Aufbewahrungszeit für Emails in der Warteschlange

(Nicht im Milter-Modus verfügbar) Die maximale Zeit, die eine Email in der Warteschlange verbringt, bevor sie blockiert wird.
Der Wert kann in Sekunden, Minuten, Stunden oder Tagen angegeben werden.
Beispiele:
10s, 10m, 10h, 10d.

Syntax:

```
QueueLifetime "timespan"
```

Beispiel:

```
QueueLifetime 1h
```

Die Einstellung 0 deaktiviert die Option.

Voreingestellt:

```
QueueLifetime 0
```

Forwarder RetryDelay

Weiterleitungsintervall einrichten (nicht im Milter-Modus)

Mithilfe dieser Option können Sie das maximale Intervall setzen, in dem Avira AntiVir MailGate versucht, eine Email erneut weiterzuleiten. Wenn der Wert von `ForwarderRetryDelay` unter dem Wert von `PollPeriod` liegt, wird MailGate die Email in dem für `PollPeriod` eingestellten Intervall weiterleiten. D.h. das Weiterleitungs-Intervall ist das Maximum von `ForwarderRetryDelay` und `PollPeriod`.

Syntax:

```
ForwarderRetryDelay "timespan"
```

Beispiel:

```
ForwarderRetryDelay 1h
```

Sie können den Wert in Sekunden (`s`), Minuten (`m`), Stunden (`h`) oder Tagen (`d`) angeben.

Voreingestellt:

```
ForwarderRetryDelay 30m
```

Jedes Mal, wenn Avira AntiVir MailGate mithilfe des `ForwarderRetryDelay` versucht, die Emails, die sich in der Warteschlange befinden, weiterzuleiten, werden diese gleichzeitig auf ihre maximale Aufbewahrungszeit überprüft.
Daher sollte der für die `QueueLifetime` festgelegte Wert ein Vielfaches des bei `ForwarderRetryDelay` Wertes betragen.

Beispiel:

```
QueueLifetime 3d
```

```
ForwarderRetryDelay 30m
```

Throttle Message Count

Maximale Anzahl zu bearbeitender Emails (nicht im Milter-Modus)

Diese Option wird benötigt, wenn sich in der Warteschlange zu viele Emails angesammelt haben und Avira AntiVir MailGate neu gestartet wird.

In diesem Fall werden alle Emails so schnell wie möglich verarbeitet. Dabei kann es zu Ladeproblemen kommen.

Der angegebene Wert ist die maximale Anzahl der Emails, die von `ThrottleDelay` verarbeitet werden (siehe folgendes Beispiel).

Es ist wichtig, dass keine weiteren Emails angenommen werden, während diese Option aktiv ist. Diese Emails würden nicht sofort verarbeitet werden.

Die Option sollte nur vorübergehend eingesetzt werden.

Die Option `ThrottleDelay` muss ebenfalls eingestellt sein.

Syntax:

```
ThrottleMessageCount "nicht-negative Zahl"
```

Voreingestellt:

```
ThrottleMessageCount 0
```

Throttle Delay

Maximale Anzahl zu sendender Emails

Diese Option legt fest, wie viele Emails (`ThrottleMessageCount`) in einem bestimmten Zeitraum (in Sekunden) gesendet werden (nicht im Milter-Modus). Standardeinstellung: 0 (deaktiviert die Option).

Syntax:

```
ThrottleDelay "nicht-negative Zahl"
```

Voreingestellt:

```
ThrottleDelay 0
```

Beispiel:

In der Warteschlange befinden sich 100 Emails. `ThrottleMessageCount` ist auf 10 gesetzt, `ThrottleDelay` auf 1. Bei dieser Einstellung werden maximal 10 Emails pro Sekunde verarbeitet.

Bounce MessageUser

Absender für unzustellbare ("Bounce-")Emails (nicht im Milter-Modus)

Der Benutzer, der als Absender einer Email angegeben ist, die nicht durch den MTA zugestellt werden konnte

Syntax:

```
BounceMessageUser "Zeichenfolge"
```

Voreingestellt:

```
BounceMessageUser MAILER-DAEMON
```

oder

```
BounceMessageUser MAILER-DAEMON@domainname
```

Bounce Message SizeBody

Umfang des Inhaltes der Bounce-Email (nicht im Milter-Modus)

Legt fest, in welchem Umfang der ursprüngliche Email-Text in der Bounce-Email wiedergegeben wird (in Byte). Der Wert 0 bedeutet, dass es keine Obergrenze gibt.

Syntax:

```
BounceMessageSizeBody "Zahl""GB|MB|KB"
```

Beispiele:

```
BounceMessageSizeBody 4KB, 3MB, 2GB.
```

Voreingestellt:

```
BounceMessageSizeBody 0
```

Bounce Message SizeHeader

Länge des Headers der Bounce-Email (nicht im Milter-Modus)

Legt fest, in welchem Umfang der ursprüngliche Email-Header von der Bounce-Email wiedergegeben wird (in Byte). Der Wert 0 bedeutet, dass es keine Obergrenze gibt.

Syntax:

```
BounceMessageSizeHeader "Zahl""GB|MB|KB"
```

Beispiele:

```
BounceMessageSizeHeader 2KB (2 Kilobyte), 3MB
(3 Megabyte), 2GB (2 Gigabyte)
```

Voreingestellt:

```
BounceMessageSizeHeader 0
```

AddXHeader

X-Header hinzufügen

Bei der Einstellung YES werden dem Header der Email die Warteschlangen-ID und Informationen über den Prüfstatus hinzugefügt. Ein Beispiel: **X-AntiVirus: checked by AntiVir MailGate...**
Der Text kann nicht geändert werden.

Syntax:

```
AddXHeader "YES | NO"
```

Voreingestellt:

```
AddXHeader YES
```

AddReceived ByHeader

„Received:“- Stempel zum Header hinzufügen (nicht im Milter-Modus)

Bei der Einstellung YES enthält die geprüfte Email einen Hinweis über die Eingangszeit.

Syntax:

```
AddReceivedByHeader "YES | NO"
```

Voreingestellt:

```
AddReceivedByHeader YES
```

MaxHop Count

Mail-Schleifen vermeiden

Enthält der Header mehr „Received“-Zeilen als in dieser Option angegeben, wird die Email gesperrt.

Syntax:

```
MaxHopCount "nicht-negative Zahl"
```

Beispiel:

```
MaxHopCount 50
```

Voreingestellt:

```
MaxHopCount 100
```

ScanTimeout

Maximale Zeit für Email-Prüfung

Diese Option legt die maximale Zeit für die Email-Prüfung fest (in Sekunden).

Syntax:

```
ScanTimeout "nicht-negative Zahl"
```

Beispiel:

```
ScanTimeout 100
```

Voreingestellt:

```
ScanTimeout 300
```

External Program

Ausführen eines externen Programms oder Skripts, wenn ein Virus/unerwünschtes Programm entdeckt wird

Ruft ein externes Programm oder Skript auf, wenn ein Virus/unerwünschtes Programm erkannt wird. Der Parameter ist die ID der zurückgewiesenen Email (siehe Avira AntiVir MailGate-Spool-Verzeichnisse – Seite 30).

Syntax:

```
ExternalProgram "Pfadangabe"
```

Beispiel:

```
ExternalProgram /path/to/program
ExternalProgram /dir/my_own_script
```

Voreingestelltes Programm:

```
keines
```

NotifyEnd OfLicense

Informationen über das Ablaufdatum der Lizenz

Sendet vor dem Ablaufdatum der Lizenz täglich eine Nachricht an den Postmaster (Angabe in Tagen). Beim Wert 0 wird keine Nachricht gesendet.

Syntax:

```
NotifyEndOfLicense "Zahl"
```

Beispiel:

```
NotifyEndOfLicense 15
```

Voreingestellt:

```
NotifyEndOfLicense 30
```

Add Precedence Header

Precedence-Header hinzufügen

Bei der Einstellung YES wird dem Header der Benachrichtigungs-Email die folgende Zeile hinzugefügt:
Precedence: junk.

Programme, die automatisch auf eingehende Emails antworten (z. B. vacation) reagieren nicht auf diesen Bericht. Die Einträge YES und NO können durch speziellen Text ersetzt werden.

Syntax:

```
AddPrecedenceHeader "YES | NO | eigener Text"
```

Voreingestellt:

```
AddPrecedenceHeader NO
```

AddHeaderTo Notice

Email-Header für Postmaster hinzufügen

Sie können den Header einer zurückgewiesenen Email in die Warnmeldung aufnehmen, die an den Postmaster gesendet wird. Mögliche Werte sind `YES` und `NO`.

Syntax:

```
AddHeaderToNotice "YES | NO"
```

Voreingestellt:

```
AddHeaderToNotice YES
```

GUISupport

Aktivierung der GUI-Unterstützung

Diese Option muss aktiviert werden, damit Avira AntiVir MailGate mit der SMC-GUI kommunizieren kann. Erforderliche Parameter (Standardeinstellungen):

Syntax:

```
GuiSupport "YES | NO"
```

Voreingestellt:

```
GuiSupport NO
GuiCAFile /usr/lib/AntiVir/mailgate/gui/cert/
cacert.pem
GuiCertFile /usr/lib/AntiVir/mailgate/gui/cert/ser-
ver.pem
GuiCertPass antivir_default
GuiRandFile /path/to/file
```

Zusätzlich müssen folgende Ports geöffnet sein:

```
udp: 59411
tcp: 50360
```

Wenn diese Parameter fehlen oder unzulässig sind, steht die GUI nicht zur Verfügung.

OpenMax **OpenMax**

Diese Option legt die maximale Anzahl geöffneter Dateien für die Avira AntiVir MailGate-Prozesse fest. Der Standardwert wird nur eingestellt, wenn der derzeitige Systemwert unter diesem Standardwert liegt.

```
OpenMax 1024
```

Ist der hier angegebene Wert kleiner als 1, sorgt MailGate dafür, dass mindestens 1024 Dateien gleichzeitig geöffnet werden können.

Wird ein Wert größer als 0 angegeben, legt MailGate diesen Wert als Maßgabe für die maximale Anzahl zu öffnender Dateien fest.

Für gewöhnlich ist es nicht notwendig, diesen Wert zu verändern.

Syntax:

```
OpenMax "nicht-negative Zahl"
```

Beispiel:

```
OpenMax 1
```

Voreingestellt:

```
OpenMax 0
```

5.2.1 Datenbank Unterstützung (Database Support)

Ab Avira AntiVir MailGate 3.1.0 unterstützt das Programm die Protokollierung von Statistiken in einer Datenbank. Details über die Einrichtung der Datenbank und andere Anforderungen finden Sie weiter unten, siehe Einrichtung.

Die Datenbank enthält zwei Tabellen, namens `alerts` (Warnmeldungen) und `counter` (Zähler).

Die Tabelle `alerts` enthält Informationen über jede blockierte Email.

Das bedeutet, dass jede Warnmeldung protokolliert wird, auch wenn bei derselben Email mehrere auftraten.

Die Tabelle `counter` enthält zusammenfassende Informationen über die verarbeiteten Emails.

Das Avira AntiVir MailGate-Paket enthält auch Beispieldateien, die unter OpenOffice verwendet werden können (siehe OpenOffice).

Anforderungen

Hier eine Liste von Versionsnummern von MySQL-Servern, MySQL-ODBC-Treibern und ODBC-Treibermanagern, die kompatibel sein sollten:

MySQL 5.0.70
MySQL-ODBC-Treiber 3.51.11
iODBC 3.52.4

Einrichtung

Bevor Sie die Datenbankunterstützung aktivieren, müssen Sie einen ODBC-Treibermanager installieren und einrichten. Es sind zwei Treibermanager verfügbar:

iODBC - www.iodbc.org (empfohlen)
unixODBC - www.unixodbc.org

Unten finden Sie eine Beschreibung, wie Sie ODBC unter Debian 5.0 installieren und einrichten können. (Informationen über die Installation und Einrichtung von ODBC bei Verwendung eines anderen Betriebssystems finden Sie im Distributions- bzw. im Managerhandbuch.)

***Warnung**: Bei Avira AntiVir MailGate handelt es sich um ein 32-Bit-Binärprogramm, das keine 64-Bit-Bibliothek verwenden kann.*
Das heißt, dass es auch keinen 64-Bit-ODBC-Treibermanager verwenden kann.

Auf 64-Bit-Rechnern sollten Sie darauf achten, dass es sich bei der ODBC-Verbindung um eine 32-Bit-Bibliothek handelt. Details über die Einrichtung der Datenbankunterstützung in Avira AntiVir MailGate auf einem 64-Bit-Rechner finden Sie in der Datei README.db-support-SLES10-SP2-64bit.

Diese Datei enthält eine Beispieleinrichtung für ODBC unter SuSE Linux Enterprise 10 SP2.

1. Richten Sie die Datenbank ein

Wenn Sie noch keinen Benutzer mit Zugriffsrechten auf die Datenbank eingerichtet haben, sollten Sie jetzt einen einrichten.
Informationen darüber, wie Sie einen Benutzer zu Ihrer Datenbank hinzufügen und diesem Zugriff geben können, finden Sie im Handbuch zu Ihrer Datenbank.

Details zum Datenbanklayout finden Sie in der Datei /usr/lib/AntiVir/mailgate/create-db.sql. Das Datenbanklayout ist das Skript zur Erstellung einer MySQL-Datenbank.

Sie können die Datenbank mit diesem Skript erstellen (Beispiel für MySQL, wobei der Server auf dem angegebenen Host läuft):

```
# mysql -u <db-Benutzer> -p -h <Name Ihres SQL-Server-Hosts> < create-db.sql
```

Geben Sie das Passwort ein.

Um über die aktuellste Version der Avira AntiVir MailGate Datenbank zu verfügen, können Sie mit folgendem Skript das neue Layout anpassen:

```
/usr/lib/AntiVir/mailgate/upgrade-db.sql
```

Spalten, die mithilfe des Skripts hinzugefügt werden, stehen erst nach dem Neustart des Programms zur Verfügung.

2. Installieren Sie iODBC

Sie sollten eine threadsichere Bibliothek wählen. Überprüfen Sie anhand des Handbuchs der Distribution, ob Ihre ODBC-Bibliothek mit Threadunterstützung eingerichtet wurde.

```
# apt-get install libiodbc2
```

3. Installieren Sie den entsprechenden Datenbanktreiber für Ihre Datenbank

Sie sollten einen threadsicheren Treiber wählen. Überprüfen Sie anhand des Handbuchs der Distribution, ob Ihr ODBC-Treiber threadsicher ist.

Beispiel für MySQL-ODBC-Treiber:

```
# apt-get install libmyodbc
```

4. Richten Sie odbc.ini ein (unter 5. finden Sie ein Beispiel für odbc.ini)

Zur Einrichtung gibt es verschiedene Möglichkeiten:

- Erstellen und/oder bearbeiten Sie die Datei /etc/odbc.ini
  oder
- Kopieren Sie /etc/avira/avmailgate-odbc.ini in /etc/odbc.ini und bearbeiten Sie die Datei
  oder
- Bearbeiten Sie /etc/avira/avmailgate-odbc.ini, und setzen Sie die Konfigurationsoption "`DBodbcIni`" in /etc/avira/avmailgate.conf auf " /etc/avira/avmailgate-odbc.ini".

Warnung: Wenn Sie die Datenbank Unterstützung (DB support) konfigurieren und die Datei avmailgate-odbc.ini *verändern, achten Sie bitte darauf, dass keine Leerzeichen vor dem Optionsnamen stehen. Anderenfalls erhalten Sie eine Fehlermeldung.*

Wenn Sie "DBodbcIni" in /etc/avira/avmailgate.conf *nicht angeben, entscheidet die Bibliothek, wo nach odbc.ini gesucht wird.*

Die Bibliothek verwendet möglicherweise auch eine andere odbc.ini*-Datei, wenn die angegebene Datei vorhanden, aber durch den Benutzer, in dessen Namen MailGate ausgeführt wird, nicht lesbar bzw. beschreibbar ist.*

5. Beispiel für odbc.ini

Dies ist ein Beispiel für eine minimale odbc.ini-Datei.

Details zu den verfügbaren Optionen finden Sie in der Dokumentation zu Ihrem Datenbanktreiber.

[MailGate]
Driver = /usr/lib/odbc/libmyodbc.so
Server = hostname.of.my.sql.server
User = username
Password = password
Database = mailgate

[MailGate]: Der von MailGate verwendete DSN
Driver: Der Pfad zur Bibliothek des Treibers
Server: Der Datenbankserver
User: Der Benutzername für den Zugriff auf die Datenbank
Password: Das Passwort des Benutzernamens
Database: Der Name der zu verwendenden Datenbank

6. Aktivieren Sie die Datenbankunterstützung in avmailgate.conf

Setzen Sie `DBSupport` in /etc/avira/avmailgate.conf auf YES

7. Testen Sie Ihre ODBC-Einrichtung

Sie können die Datenbankverbindung mit dem Tool `avmg_stats` prüfen. Das Tool wird durch Avira AntiVir MailGate gestartet, wenn `DBSupport` oder `GuiSupport` aktiviert sind. Zunächst analysiert `avmg_stats` die Konfigurationsdatei nach Validität. Das Tool wird für die Kommunikation zwischen Datenbank und Client, Datenbank und SMC sowie für Datenbankprotokolleinträge verwendet.

```
/usr/lib/AntiVir/mailgate/gui/bin/avmg_stats -S
```

Das Tool gibt bei Erfolg Folgendes aus:

```
$ /usr/lib/AntiVir/mailgate/gui/bin/avmg_stats -S
Using these settings:
ODBC ini:    <using system's odbc.ini>
ODBC library: libodbc.so.1
ODBC source:  MailGate

Preparing connection ...
=> OK
Connecting ...
=> OK
Disconnecting ...
=> OK

Successfully verified database connectivity!
```

... und beim Auftreten von Fehlern eine ähnliche Liste (Beispiel für MySQL; die Fehlermeldung kann sich je nach Fehlertyp unterscheiden):

```
Using these settings:
ODBC ini:    <using system's odbc.ini.>
ODBC library: libodbc.so.1
ODBC source:  MailGate

Preparing connection ...
=> OK
Connecting ...
Failed to connect to ODBC data source (error code: -2)
([MySQL][ODBC 3.51 Driver]Lost connection to MySQL server at 'reading
initial communication packet', system error: 111)
```

Ausgabe einer CSV-Liste

Avira AntiVir MailGate kann die Tabelleninhalte als CSV-Liste (durch Komma getrennte Werte) ausgeben.
Standardmäßig wird nur die Tabelle `alerts` ausgegeben. Sie können mit der Befehlszeilenoption `-t` auch eine andere Tabelle ausgeben lassen.

Die erste Zeile der ausgegebenen Liste enthält die Spaltennamen. Alle anderen Zeilen bilden die Tabellenzeilen. Die Ergebnisse sind nicht sortiert.

Beispiel:

Ausgabe der Tabelle `alerts`:

```
# /usr/lib/AntiVir/mailgate/gui/bin/avmg_stats -o csv
```

Ausgabe der Tabelle `counter`:

```
# /usr/lib/AntiVir/mailgate/gui/bin/avmg_stats -o csv -
t counter
```

CSV-Trennzeichen:

Geben Sie ein einzelnes Feldtrennzeichen an:

```
-o csv:s
```

Sie müssen das Trennzeichen in Anführungszeichen angeben, da es andernfalls eventuell von der Shell interpretiert wird.

Beispiel:

Ausgabe der Tabelle `alerts` mit ";" als Trennzeichen:

```
# /usr/lib/AntiVir/mailgate/gui/bin/avmg_stats -o
csv:';'
```

Zeitabschnitte:

Sie können das Ergebnis auf die Auflistung von Zeilen innerhalb eines bestimmten

Zeitabschnitts beschränken:

```
-R "YYYY-MM-DD HH:MM:SS/YYYY-MM-DD HH:MM:SS"
```

Beispiel:

Ausgabe der Tabelle `alerts` unter Beschränkung auf einen bestimmten Zeitabschnitt:

```
# /usr/lib/AntiVir/mailgate/gui/bin/avmg_stats -o csv -
R "2009-05-15 00:00:00/2009-05-15 15:35:43"
```

Hierdurch werden alle Warnmeldungen aufgelistet, die zwischen 2009-05-15 00:00:00 und 2009-05-15 15:35:43 protokolliert wurden.

Beschreibung der Tabelle `alerts`

Sobald eine Email blockiert wird, werden Angaben zur Warnmeldung/zu den Warnmeldungen in die Datenbank geschrieben.

Spalte	Beschreibung
id	Diese Spalte hat keine besondere Bedeutung. Es handelt sich lediglich um eine automatisch generierte aufsteigende Zahl.
reason	Der Grund, warum die Email blockiert wurde. Es gibt folgende Gründe: Alert - Der Scanner hat Malware gefunden. Spam - Der Spamfilter hat Spam oder eine andere Kategorie erkannt. (Details über Kategorien finden Sie unter "Spamfilter".) Error - Fehler beim Scannen Incomplete - Nicht vollständig gescannt Encrypted - Die Email enthält einen verschlüsselten Anhang. Extension - Die Email enthält einen Anhang mit einer verbotenen Dateinamenerweiterung. Limit - Es wurde ein Grenzwert erreicht. Suspicious - (wird noch nicht verwendet) Unsupported - Ein Archiv mit einem nicht unterstützten Komprimierungsverfahren Unknown reason - Der Grund ist unbekannt (wird noch nicht verwendet). ***Hinweis**: Nach Produktaktualisierungen werden in dieser Spalte zukünftig möglicherweise noch andere Gründe aufgeführt.*
alertname	Vom Grund abhängig: Alert - Die Bezeichnung der Warnmeldung All other reasons - Eine detaillierte Beschreibung des Grundes
queueid	Die Warteschlangen-ID der Email

Spalte	Beschreibung
alerttype	Alert -adware, backdoor, trash, dialer, heuristic, joke, program, riskware, trojan, virus, worm *(**Hinweis**: In dieser Spalte werden möglicherweise auch andere Kategorien verwendet. Die Kategorien hängen vom Scanner ab und können sich ändern, oder es stehen nach einer Aktualisierung des Scanners möglicherweise neue zur Verfügung.)* All other reasons - Eine kurze Beschreibung der Bezeichnung der Warnmeldung.
filename	Der Name der Datei, in der die Warnmeldung gefunden wurde; Vom Grund abhängig: Alert - Der Name der Datei, die die Warnmeldung verursachte All other reasons - Die Spalte enthält "<no file name available>". ***Hinweis**: Der Dateiname ist auf 100 Zeichen beschränkt. Wenn der Dateiname abgeschnitten wird, wird er um" ..." ergänzt.*
action	Umfasst zur Zeit nur `quarantined`.
source	Die Email-Adresse des Absenders (auf 40 Zeichen beschränkt) Wenn die Adresse abgeschnitten wird, wird sie um" ..." ergänzt.
alterurl	Nicht verwendet ("").
missed	Aufgrund interner Pufferbeschränkungen kann möglicherweise nicht jede Warnmeldung in die Datenbank geschrieben werden. In diesem Fall enthält die Spalte "missed" eine Angabe zur Anzahl der Warnmeldungen, die nicht in die Datenbank geschrieben werden konnten.
product	Enthält den Produktnamen "MailGate".
rcpt	Diese Spalte speichert Empfänger von Emails wie folgt: - Wenn `DBStoreAlertsForEachRecipient` deaktiviert ist, wird nur der erste Empfänger einer Email hier gespeichert. - Ist `DBStoreAlertsForEachRecipient` aktiviert, und steht in der Tabelle für jeden Empfänger eine Reihe zur Verfügung, wird jeder Empfänger hier zurückgeschrieben.

Spalte	Beschreibung
vdf	Versionsinformationen zu der zum Scannen verwendeten VDF.
engine	Versionsinformationen zu der zum Scannen verwendeten Engine.
hostname	Der Wert von "MyHostName" (/etc/avira/avmailgate.conf) Wenn "MyHostName" nicht festgelegt ist, ist dies der von gethostname() zurückgegebene Wert; wenn gethostname() fehlschlägt, "localhost".
ou	Wenn ActiveDirectorySupport aktiviert und ein Lookup für eine Gruppe durchgeführt wurde, wird der gefundene Wert in diese Spalte zurückgeschrieben.
date 	Das Datum und die Uhrzeit, zu der der Statistik-Daemon die Angaben zur Warnmeldung erhielt. Die Werte für Datum und Uhrzeit werden von `localtime_r()` empfangen. Das Format ist JJJJ-MM-TT hh:mm:ss. ***Hinweis:*** *Details zum Speichern des Datums finden Sie unter "Hinweise zum Datum".*

Beschreibung der Tabelle counter

Die Spalten in der Tabelle `counter` werden regelmäßig ausgefüllt. Die Standardeinstellung ist zu jeder vollen Stunde.

Sie können den Zeitraum zwischen den Einträgen über die Konfigurationsoption `DBUpdateDelay` in /etc/avira/avmailgate.conf ändern.

Beispiel:

```
DBUpdateDelay 30m
```

Informationen werden alle 30 Minuten in die Datenbank geschrieben.
Mögliche Einheiten sind: keine Einheit/, s=Sekunden, m=Minuten, h=Stunden

Spalte	Beschreibung
id	Diese Spalte hat keine besondere Bedeutung. Es handelt sich lediglich um eine automatisch generierte aufsteigende Zahl.
accepted	Die Anzahl der vom SMTP-Daemon akzeptierten Emails.
clean	Die Anzahl der unverdächtigen Emails.
alerts	Die Anzahl der gefundenen Malware.

Spalte	Beschreibung
spam	Die Mengen an Spam (blockiert und nicht blockiert). ***Hinweis**: Blockierte Emails sind auch in der Tabelle `alerts` enthalten.*
sent	Die Anzahl der erfolgreich weitergeleiteten Emails. ***Hinweis:** Es werden auch Benachrichtigungs-Emails gezählt.*
notify_admin	Anzahl der Postmaster-Benachrichtigungen.
notify_sender	Anzahl der Absender-Benachrichtigungen.
notify_recipient	Anzahl der Empfänger-Benachrichtigungen.
total_size	Die Zusammenfassung der Größe der Emails.
errors	Die Anzahl der Emails, die bei der Verarbeitung einen Fehler verursacht haben.
incomplete	Die Anzahl der Emails, die nicht vollständig gescannt werden konnten.
unsupported	Die Anzahl der Emails mit einem nicht unterstützten Komprimierungsverfahren.
encrypted	Die Anzahl der Emails mit verschlüsselten Anhängen.
extension	Die Anzahl der Emails mit einer Datei im Anhang, deren Dateiname eine verbotene Erweiterung enthält.
limits	Die Anzahl der Emails, bei deren Verarbeitung ein Archivgrenzwert erreicht wurde.
unknown	Nicht verwendet (0).
product	Der Produktname "MailGate".
ou	Wenn `ActiveDirectorySupport` aktiviert und ein Lookup für eine Gruppe durchgeführt wurde, werden die Organisationseinheiten mit Anzahl der verarbeiteten Emails in diese Spalte zurückgeschrieben.
rcpt	Wenn `DBStoreAlertsForEachRecipient` aktiviert wurde, werden alle Empfänger der Email aus der Tabelle `alerts` in diese Spalte zurückgeschrieben.

Spalte	Beschreibung
hostname	Der Wert von "MyHostName" (/etc/avira/avmailgate.conf). Wenn "MyHostName" nicht festgelegt ist, ist dies der von gethostname() zurückgegebene Wert. Wenn gethostname() fehlschlägt, "localhost".
date	Das Datum und die Uhrzeit, zu der die Zählerergebnisse zusammengestellt und in die Datenbank geschrieben wurden. Die Werte für Datum und Uhrzeit werden von localtime_r() empfangen. Das Format ist JJJJ-MM-DD hh:mm:ss. ***Hinweis**: Details zum Speichern des Datums finden Sie unter Hinweise zum Datum.*

Hinweise zum Datum

Die Datumsspalte enthält das lokale Datum und die lokale Uhrzeit des Servers, auf dem Avira AntiVir MailGate ausgeführt wird. Das Datenbankskript legt die Datumsspalte als Datentyp `DATETIME` an.

Bitte beachten Sie, dass Datum/Uhrzeit nicht konvertiert werden. Es wird nicht erwartet, dass der Datenbankserver Datum und Uhrzeit konvertiert, da der Datentyp der Datumsspalte `DATETIME` und nicht `TIMESTAMP` ist.

OpenOffice

Für die Beschreibung unten ist es erforderlich, dass ODBC auf dem Rechner, auf dem OpenOffice ausgeführt wird, ordnungsgemäß konfiguriert ist.

Informationen über die Einrichtung von ODBC finden Sie im Abschnitt Einrichtung. Außerdem finden Sie Informationen über die Einrichtung von ODBC in der Dokumentation Ihres Betriebssystems.

Das Avira AntiVir MailGate-Paket enthält zwei OpenOffice-Dateien, MailGate.odb und Alerttype+Counter.ods, im Verzeichnis doc. Mit diesen Dateien können Sie OpenOffice eine Datenbank hinzufügen und in der Datenbank enthaltene Informationen erhalten und anzeigen.

MailGate.odb enthält Datenbankinformationen:

- Es wird eine ODBC-Datenquelle verwendet (Bezeichnung: "MailGate").
- Benutzername und Passwort sind "mailgate".

Außerdem enthält die Datei ein Makro, das die Datenbank automatisch in OpenOffice registriert. Details finden Sie unter Makro. (Dies funktioniert nur bei OpenOffice 3.1 oder höher)

Alerttype+Counter.ods:

- Enthält einen von der Datenbank erhaltenen Datensatz. Die Daten können aktualisiert werden, um den neuesten Datenbankinhalt zu erhalten.
- Enthält Beispieltabellen

Makro

Mit dem Makro wird die Datenbank beim Öffnen des odb-Dokuments automatisch registriert. Dieses Makro funktioniert nur bei OpenOffice 3.1 (oder höher).

Dies ist das in MailGate.odb enthaltene Makro:

```
***** BASIC *****
' The purpose of this macro is to register a database if it isn't already registered.
' The macro is linked to the "Open Document" event.
' This means it is always executed when opening the document.

Sub Main
Dim DatabaseName as String
Dim DatabaseCtx as Object
DatabaseName = "MailGate"

' Get context to access datasource
DatabaseCtx = CreateUnoService("com.sun.star.sdb.DatabaseContext")

' Check if database is already registered
If not DatabaseCtx.hasByName (DatabaseName) Then
Dim URL as String
    Dim DB as Object
URL = thisComponent.getURL
DB = DatabaseCtx.getByName (URL)
' Register database
DatabaseCtx.registerObject (DatabaseName, DB)
End If
End Sub
```

OpenOffice < 3.1

In diesem Abschnitt wird beschrieben, wie die OpenOffice-Dateien unter

OpenOffice < 3.1 verwendet werden.

Versionen von OpenOffice < 3.1 können das in MailGate.odb enthaltene Makro nicht verwenden. Die Datenbank muss daher manuell hinzugefügt werden.

▶ 1. Kopieren Sie "MailGate.odb" aus dem Paket auf Ihre Festplatte. (Die Datei muss vorhanden sein, wenn Sie zukünftig Alertype+Counter.ods verwenden möchten.)

▶ 2. Starten Sie OpenOffice.

▶ 3. Ignorieren Sie die Warnung zur Makrosicherheit.

▶ 4. Fügen Sie die Datenbank manuell hinzu:

↳ Tools -> Options

↳ OpenOffice.org Base -> Databases

↳ New

▶ Wechseln Sie zu "MailGate.odb"

↳ OK

↳ OK

▶ 5. Fahren Sie mit "6." im Abschnitt unten fort.

OpenOffice 3.1

In diesem Abschnitt wird beschrieben, wie die OpenOffice-Dateien unter OpenOffice 3.1 verwendet werden.

▶ 1. Kopieren Sie "MailGate.odb" aus dem Paket auf Ihre Festplatte. (Die Datei muss vorhanden sein, wenn Sie zukünftig "Alertype+Counter.ods" verwenden möchten.)

▶ 2. Starten Sie OpenOffice.

▶ 3. Setzen Sie die Makrosicherheit herab:

↳ Tools -> Options

↳ OpenOffice.org -> Security

↳ Macro Security -> Medium

↳ OK

↳ OK

▶ 4. Öffnen Sie MailGate.odb:

↳ File -> Open -> MailGate.odb

↳ Enable Macros

5. Die Datenbank sollte jetzt in OpenOffice verfügbar sein.

Gehen Sie folgendermaßen vor, um das Vorhandensein der Datenbank zu überprüfen:

↳ Tools -> Options

↳ OpenOffice.org Base -> Databases

Es sollte ein Eintrag namens "MailGate" vorhanden sein.

↳ Cancel

▶ 6. Jetzt können Sie mit dem Dokument "Alerttype+Counter.ods" den aktuellen Datenbankinhalt anzeigen und Tabellen erstellen oder vorhandene Tabellen verwenden:

↳ File -> Open -> Alerttype+Counter.ods

Aktualisieren von Daten:

▶ Klicken Sie mit der rechten Maustaste auf die Daten, die Sie aktualisieren möchten (eine der Zellen A3, D3, G3).

▶ (Geben Sie auf Anfrage den Benutzernamen und das Passwort für die Datenbank ein.)

▶ Wählen Sie "Refresh".

Wenn in der Datenbank Daten vorhanden sind, sollten einige Zähler oder sogar Warnmeldungstypen unter "alerttype" angezeigt werden, wenn eine Email in Quarantäne genommen wurde, nachdem Avira AntiVir MailGate mit Datenbankunterstützung gestartet wurde.

Die Zählertabellen werden automatisch aktualisiert, wenn sich Zähler ändern.

Die Tabelle "alerttype" muss bei neuen Typen manuell aktualisiert werden:

▶ Doppelklicken Sie auf die Tabelle "alerttype".

▶ Klicken Sie mit der rechten Maustaste auf die Tabelle "Data ranges"

▶ Ändern Sie die Zeilen entweder manuell oder wählen Sie mit der Schaltfläche mit dem grünen Pfeil neue Warnmeldungstypen aus.

Wählen Sie nicht die Zellen A3 und B3 aus. Wählen Sie nur die Zellen aus, die den Warnmeldungstyp und den Zähler enthalten.

↳ OK

Die Tabelle sollte den neuen Warnmeldungstyp enthalten.

▶ 7. Eventuell sollten Sie die Makrosicherheitsebene auf "High" setzen:

↳ Tools -> Options

↳ OpenOffice.org -> Security

↳ Macro Security -> High

↳ OK

↳ OK

Optionen

DBSupport

DBSupport

Wenn Sie diese Option aktivieren, trägt Avira AntiVir MailGate Statistiken in einer Datenbank ein. Die Datenbank besteht aus zwei Tabellen: alerts (protokolliert Informationen über jeden Malware-Fund) und counter (zählt die Emails, die MailGate verarbeitet).

Syntax:

```
DBSupport "YES | NO"
```

Voreingestellt:

```
DBSupport NO
```

Möchten Sie `DBSupport` aktivieren, ändern Sie den Parameter zu `YES` und vergewissern Sie sich, dass folgende Ports geöffnet sind, sofern Sie mit der Loopback-Schnittstelle arbeiten:

```
udp: 59411
```

```
tcp: 50360 (nur für SMC-Anwender)
```

Wenn Sie `DBSupport` in Verbindung mit der Funktion SpamFilter Exceptions benutzen, kann es vorkommen, dass Sie Datenbankeinträge erhalten, die inkonsistent wirken. Trägt eine Email verschiedene Sender- oder Empfängeradressen oder stehen diese Adressen in SpamFilter Exceptions nicht zur Verfügung, wird die Email vervielfältigt. Aufgrund dieses Multiplikationsfaktors kann die Datenbanktabelle `counter` folgende, inkonsistente Zeileneinträge zeigen:

accepted	1
clean	2

DBodbcIni

DBodbcIni

Wenn Sie die Option `DBSupport` aktiviert haben, benutzt der ODBC-Driver-Manager die hier angegebene odbc.ini. Standardeinstellung: Der installierte ODBC-Driver-Manager entscheidet selbst, welche odbc.ini-Datei er lädt.

Syntax:

```
DBodbcLib "Pfadangabe"
```

Beispiel:

```
DBodbcLib /path/to/odbc-library
```

DBodbcLib

DBodbcLib

Wenn Sie die Option `DBSupport` aktiviert haben, lädt Avira AntiVir MailGate die hier angegebene Bibliothek und benutzt sie als ODBC-Driver-Manager. Standardeinstellung: Eine von folgenden Dateien aus dem voreingestellten Bibliothekspfad wird der Reihe nach geladen: libodbc.so.1, libodbc.so, libiodbc.so

Syntax:

```
DBodbcLib "Pfadangabe"
```

Beispiel:

```
DBodbcLib /path/to/odbc-library
```

DBodbcData Source

DBodbcDataSource

Wenn Sie die Option `DBSupport` aktiviert haben, wird die angegebene Datenbank als Quelle verbunden.

Syntax:

```
DBodbcDataSource "Zeichenfolge"
```

Voreingestellt:

```
DBodbcDataSource MailGate
```

DBUpdate Delay

DBUpdateDelay

Wenn Sie die Option `DBSupport` aktiviert haben, werden die Statistiken in regelmäßigen Intervallen in die Datenbank geschrieben. Sie können das Intervall in Sekunden (s), Minuten (m) oder Stunden (h) eintragen. Voreingestellt: zur vollen Stunde.

Syntax:

```
DBUpdateDelay "timespan"
```

Voreingestellt:

```
 DBUpdateDelay 1h
```

DBStoreAlerts ForEach Recipient

DBStoreAlertsForEachRecipient

Wenn diese Option aktiviert ist, wird eine Zeile für jeden Empfänger einer Email in die Tabelle `alerts` geschrieben. Haben Sie die Option nicht aktiviert, wird nur eine Zeile pro Email geschrieben, die den Namen des ersten Empfängers beinhaltet. Die Standardeinstellung schreibt eine Zeile pro Email in die Tabelle `alerts`.

Syntax:

```
DBStoreAlertsForEachRecipient "YES | NO"
```

Voreingestellt:

```
DBStoreAlertsForEachRecipient NO
```

DBLog CleanMails

DBLogCleanMails

Mit Hilfe dieser Option werden Informationen über saubere, unbedenkliche Emails in der Datenbank gespeichert.

Die Informationen werden in den Kategorien `reason`, `queueid`, `action`, `source`, `product`, `vdf`, `engine`, (`ou`) und `date` festgehalten. `reason` wird auf `clean` und `action` auf `processed` gesetzt.

Syntax:

```
DBLogCleanMails "YES | NO"
```

Voreingestellt:

```
DBLogCleanMails NO
```

5.3 Spam-Filter konfigurieren (nur für **Avira MailGate Suite**)

Der in Avira MailGate Suite integrierte Spam-Filter filtert Spam und andere unerwünschte Emails heraus. Der Spam-Filter öffnet für jede Email eine Verbindung zum Spam-Datenbankserver, um ihren Spam-Status zu prüfen. Dazu muss die Verbindung auf Port 55555 via TCP aktiviert sein.

Wenn der Spam-Filter aktiv ist, werden Emails gesperrt, die als „Outbreak“ markiert sind. Alle anderen Emails werden nur gekennzeichnet. Alle genannten Optionen werden in avmailgate.conf eingestellt.

Optionen und Parameter für den Spam-Filter

Enable SpamCheck

EnableSpamCheck

Aktiviert bzw. deaktiviert den Spam-Filter.

Syntax:

```
EnableSpamCheck "YES | NO"
```

Voreingestellt:

```
EnableSpamCheck NO
```

SpamAction

SpamAction

Legt eine Aktion für Spam-Emails fest: BLOCK, TAG, NONE.

Syntax:

```
SpamAction "Option"
```

- TAG fügt der Email eine Header-Zeile hinzu. Ein Beispiel:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 3.2.1.16; spam filter version: 3.2.0/2.3; host: host.your.site)
- BLOCK verschiebt die Email in das Verzeichnis rejected.
- NONE deaktiviert alle Aktionen für Spam-Emails.

Voreingestellt:

```
SpamAction TAG
```

Dangerous Outbreak Action

DangerousOutbreakAction

Führt die angegebene Aktion durch, wenn Emails aufgrund eines Outbreaks vom Virenscanner nicht erkannt werden. Gültige Optionen sind BLOCK, TAG und NONE.

Syntax:

```
DangerousOutbreakAction "Option"
```

- TAG fügt der Email eine Header-Zeile hinzu. Ein Beispiel:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 3.2.1.16; spam filter version: 3.2.0/2.3; host: host.your.site)
- BLOCK verschiebt die Email in das Verzeichnis rejected.
- NONE deaktiviert alle Aktionen für gefährliche Outbreaks.

Voreingestellt:

```
DangerousOutbreakAction BLOCK
```

Dangerous Attachment Action

DangerousAttachmentAction

Führt die angegebene Aktion durch, wenn ein Email-Anhang möglicherweise gefährlich ist. Gültige Optionen sind TAG, BLOCK und NONE. Die Email-Anhänge werden anhand ihrer Suffixe identifiziert:
.ade, .adp, .bas, .bat, .bhx, .ceo, .cer, .chm, .cmd, .com, .cpl, .crt, .exe, .hlp, .hta, .inf, .ins, .isp, .js, .jse, .lnk, .mde, .mim, .msc, .msi, .msp, .mst, .ole, .pcd, .pi, .pif, .reg, .scr, .sct, .shb, .shs, .vb, .vbe, .vbs, .wmd, .wmz, .wsc, .wsf, .xxe

Syntax:

```
DangerousAttachmentAction "Option"
```

- TAG fügt der Email eine Header-Zeile hinzu. Ein Beispiel:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 3.2.1.16; spam filter version: 3.2.0/2.3; host: host.your.site)
- BLOCK verschiebt die Email in das Verzeichnis rejected.
- NONE deaktiviert alle Aktionen für gefährliche Email-Anhänge.

Voreingestellt:

```
DangerousAttachmentAction TAG
```

Dangerous IFrameAction

DangerousIFrameAction

Führt die angegebene Aktion durch, wenn ein gefährlicher IFRAME entdeckt wird. Gültige Optionen sind TAG, BLOCK und NONE.

Syntax:

```
DangerousFrameAction "Option"
```

- TAG fügt der Email eine Header-Zeile hinzu. Ein Beispiel:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 3.2.1.16; spam filter version: 3.2.0/2.3; host: host.your.site)
- BLOCK verschiebt die Email in das Verzeichnis rejected.
- NONE deaktiviert alle Aktionen für gefährliche iFrames.

Voreingestellt:

```
DangerousIFrameAction TAG
```

Dangerous Alert Action

DangerousAlertAction

Führt die angegebene Aktion durch, wenn der Spam-Filter eine Email als gefährlich einstuft. Gültige Optionen sind TAG, BLOCK und NONE.

Syntax:

```
DangerousAlertAction "Option"
```

- TAG fügt der Email eine Header-Zeile hinzu. Ein Beispiel:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 3.2.1.16; spam filter version: 3.2.0/2.3; host: host.your.site)
- BLOCK verschiebt die Email in das Verzeichnis rejected.
- NONE deaktiviert alle Aktionen für als gefährlich eingestufte Emails.

Voreingestellt:

```
DangerousAlertAction BLOCK
```

Dangerous Unknown Action

DangerousUnknownAction

Führt die angegebene Aktion durch, wenn eine unbekannte Gefahr entdeckt wird. Gültige Optionen sind TAG, BLOCK und NONE.

Syntax:

```
DangerousUnknownAction "Option"
```

- TAG fügt der Email eine Header-Zeile hinzu. Ein Beispiel:
  X-AntiVirus-Spam-Check: clean (checked by Avira MailGate: version: 3.2.1.16; spam filter version: 3.2.0/2.3; host: host.your.site)
- BLOCK verschiebt die Email in das Verzeichnis rejected.
- NONE deaktiviert alle Aktionen für unbekannte Gefahren.

Voreingestellt:

```
DangerousUnknownAction TAG
```

LibAsmailgate

LibAsmailgate

Gibt den Pfad zur Bibliothek des Spam-Filters an.

Syntax:

```
LibAsmailgate "Pfadangabe"
```

Voreingestellt:

```
LibAsmailgate /usr/lib/AntiVir/mailgate/
libasmailgate.so
```

Spam Header Name

SpamHeaderName

Gibt den Spam-Header an, der in den Email-Header eingefügt werden soll. Nur der Anfang des Textes kann geändert werden (`X-AntiVirus-Spam-Check`).

Syntax:

```
SpamHeaderName "Zeichenfolge"
```

Beispiel:

```
SpamHeaderName X-AntiVirus-Spam-Check
```

Ergebnis:

```
X-AntiVirus-Spam-Check: spam (checked by Avira Mail-
Gate: version: 3.2.1.16; spam filter version:
3.2.0/2.3; host: host.your.site);id=5506-x4KZ25
```

SpamFilter Exceptions

SpamFilterExceptions

Legt die Liste der Ausnahmen für Blacklists/Whitelists und die dazugehörigen Aktionen fest.

Syntax:

```
SpamFilterExceptions "Pfadangabe"
```

Voreingestellt:

```
SpamFilterExceptions /etc/avira/asmailgate.except
```

Die Aktionen des Spam-Filters können mithilfe der Datei asmailgate.except überschrieben werden. In dieser Datei können Sie Email-Adressen und die dazugehörigen Aktionen angeben. Außerdem kann die Datei als Blacklist/Whitelist für den Spam-Filter verwendet werden.

Jede Liste besteht aus einer Adresse in Form eines regulären Ausdrucks, z. B.:

```
/^someone@somewhere\.tld$/i blacklist
```

Dieses Beispiel behandelt Emails von someone@somewhere.tld unabhängig vom Ergebnis der Spam-Prüfung als Spam. `Blacklist` ist die Aktion für die angegebene Adresse.

Bei Avira AntiVir MailGate v 2.1.3 betrifft eine Übereinstimmung in dieser Liste alle Empfänger, also auch solche, die selbst nicht in der Liste stehen. Ein Beispiel (in asmailgate.except*):*

```
/^someone@somewhere\.tld$/i r block_spam
```

Wenn Avira AntiVir MailGate eine an someone@somewhere.tld und abc@def.tld adressierte Email verarbeitet, die als Spam eingestuft wurde, erhält abc@def.tld die Email nicht, da sie aufgrund der Regel für someone@somewhere.tld gesperrt wurde. Dieses Verhalten wird in zukünftigen Versionen geändert.

Aktionen:

Aktionen haben Vorrang vor den Einstellungen für den Spam-Filter in avmailgate.conf (mit Ausnahme von Blacklists/Whitelists). Für jede Adresse können mehrere Aktionen festgelegt werden:

- `blacklist` – Email wird als Spam behandelt
- `whitelist` – Email wird als sauber behandelt
- `block_spam` – Email wird gesperrt, wenn sie als Spam eingestuft wurde
- `block_dangerous_attachment` – Email wird gesperrt, wenn sie einen gefährlichen Anhang hat
- `block_dangerous_alert` – Email wird gesperrt, wenn sie einen gefährlichen Alarm enthält
- `block_dangerous_iframe` – Email wird gesperrt, wenn sie einen gefährlichen IFRAME hat
- `tag_spam` – Email wird gekennzeichnet, wenn sie als Spam eingestuft wurde
- `tag_dangerous_attachment` – Email wird gekennzeichnet, wenn sie einen gefährlichen Anhang hat
- `tag_dangerous_alert` – Email wird gekennzeichnet, wenn sie einen gefährlichen Alarm enthält
- `tag_dangerous_iframe` – Email wird gekennzeichnet, wenn sie einen gefährlichen IFRAME enthält

Beispiel für /etc/avira/asmailgate.except:

```
/^spam@somewhere\.tld$/i blacklist
```

Emails von spam@somewhere.tld werden unabhängig vom Ergebnis der Spam-Prüfung als Spam behandelt.

Aktionen können auch ausgeschaltet werden. **Beispiel**:

- in /etc/avira/avmailgate.conf:
  ```
  SpamAction BLOCK
  ```
- in /etc/avira/asmailgate.except:
  ```
  /^me@here\.tld$/i r !block_spam
  ```

Für die angegebene Empfängeradresse wird Spam nicht gesperrt.

`r` ist das Flag für Empfänger. Es bedeutet, dass die angegebene Adresse nicht mit der Absenderadresse, sondern mit der Empfängeradresse verglichen werden soll.

In der Standardeinstellung (ohne das Flag `r`) wird die Adresse mit der Absenderadresse verglichen.

Ein weiteres **Beispiel**:

- in /etc/avira/avmailgate.conf:
  ```
  DangerousAttachmentAction TAG
  DangerousIFrameAction TAG
  ```
- in /etc/avira/asmailgate.except:
  ```
  /^me@here\.tld$/i r !tag_dangerous_attachment
  !tag_dangerous_iframe
  ```

DangerousAttachment- und DangerousIFrame-Emails werden nicht gekennzeichnet.

Warnung: *Der Status „DangerousOutbreak“ hat eine höhere Priorität als die Einträge in Black- und Whitelists. Bei einem „DangerousOutbreak“ werden Black- und Whitelists nicht überprüft.*

SpamFilter DetectGTUBE

SpamFilterDetectGTUBE

Die GTUBE-Testzeichenkette kann verwendet werden, um den integrierten Spam-Filter zu testen. Sie finden diese Zeichenkette und eine vollständige RFC-822-Email unter: http://spamassassin.apache.org/gtube/

Eine Email, die diese Zeichenkette enthält, sollte von Spam-Filtern als **Spam** eingestuft werden. Kopieren Sie die Zeichenkette einfach in den Text der Nachricht und senden Sie sie über Avira AntiVir MailGate. Der Spam-Filter arbeitet korrekt, wenn Sie eine Nachricht wie die folgende erhalten:

```
...
spam filter: result=spam; action=tagged; id=15025-btMzMR
spam filter: spam mail detected (queue id: 15025-btMzMR)
...
```

GTUBE wird standardmäßig nicht erkannt. Um die GTUBE-Erkennung zu

aktivieren, setzen Sie diese Option auf YES und starten Sie Avira AntiVir MailGate neu:

Syntax:

```
SpamFilterDetectGTUBE "YES | NO"
```

Voreingestellt:

```
SpamFilterDetectGTUBE NO
```

SpamFilter Startup Timeout

SpamFilterStartupTimeout

Diese Option legt fest, wie lange Avira AntiVir MailGate warten soll, bis der externe Spam-Daemon hochgefahren ist (in Sekunden).

Syntax:

```
SpamFilterStartupTimeout "nicht-negative Zahl"
```

Voreingestellt:

```
SpamFilterStartupTimeout 60
```

SpamFilter ServiceConnect Timeout

SpamFilterServiceConnectTimeout

Diese Option legt fest, wie lange Avira AntiVir MailGate warten soll, bis vom externen Spam-Filter-Daemon eine Antwort auf eine Konfigurationsanfrage eingeht (in Sekunden).

Syntax:

```
SpamFilterServiceConnectTimeout "nicht-negative Zahl"
```

Voreingestellt:

```
SpamFilterServiceConnectTimeout 30
```

SpamFilter ServiceMax Sessions

SpamFilterServiceMaxSessions

Diese Option legt die Höchstzahl gleichzeitig laufender Verbindungen zum externen Spam-Filter-Daemon fest.

Syntax:

```
SpamFilterServiceMaxSessions "nicht-negative Zahl"
```

Voreingestellt:

```
SpamFilterServiceMaxSessions 50
```

SpamFilter HandleBulk ADVLikeSpam

SpamFilterHandleBulkADVLikeSpam

Mithilfe dieser Option können Sie Werbe-Emails als Spam einstufen.

Syntax:

```
SpamFilterHandleBulkADVLikeSpam "YES | NO"
```

Voreingestellt:

```
SpamFilterHandleBulkADVLikeSpam NO
```

SpamFilter HandleBulk PornLikeSpam

SpamFilterHandleBulkPornLikeSpam

Mithilfe dieser Option können Sie Emails mit pornografischem Inhalt als Spam einstufen.

Syntax:

```
SpamFilterHandleBulkPornLikeSpam "YES | NO"
```

Voreingestellt:

```
SpamFilterHandleBulkPornLikeSpam NO
```

SpamFilter ModifySubject

SpamFilterModifySubject

Diese Option fügt das Ergebnis der Spam-Prüfung in die Header-Zeile „Subject:“ ein.

Subject: [spamcheck: spam] Ursprünglicher Betreff-Text

Dies ist die Standardmeldung. Sie kann mithilfe einer Vorlage überschrieben werden: „spamfilter-subjects“. In dieser Vorlage können Sie für jedes Ergebnis einer Spam-Prüfung eine Zeichenkette angeben. Die entsprechende Zeichenkette ersetzt die Header-Zeile „Subject:“.

Eine Beispielvorlage finden Sie in /usr/lib/AntiVir/mailgate/templates/examples.

Syntax:

```
SpamFilterModifySubject "YES | NO"
```

Voreingestellt:

```
SpamFilterModifySubject NO
```

SpamFilter CheckFailed Keep

SpamFilterCheckFailedKeep

Wenn die Spam-Prüfung fehlschlägt, wird die Email zurück in die Warteschlange geschickt, um erneut geprüft zu werden. Die Email wird bearbeitet solange der Fehler auftritt. Zur Zeit können Sie die Weiterleitung einer in der Warteschlange blockierten Email nicht erzwingen.

Syntax:

```
SpamFilterCheckFailedKeep "YES | NO"
```

Voreingestellt:

```
SpamFilterCheckFailedKeep NO
```

5.4 Scanner-Konfiguration in avmailgate-scanner.conf

Beginnend mit Avira AntiVir MailGate 3.0.0 wurde eine neue Konfigurationsdatei eingeführt: avmailgate-scanner.conf. Diese Datei enthält spezielle Konfigurationsoptionen für das neue Scanner-Backend. Die Optionen in dieser Datei brauchen nur in einigen wenigen Ausnahmefällen geändert zu werden.

User Group

Benutzer, Gruppe

Wenn Sie eine dieser Optionen ändern, müssen Sie sicherstellen, dass die Dateien

avmailgate-scanner.conf und avmailgate.conf die gleichen Werte für diese Optionen enthalten.

Außerdem müssen Sie avmailgate-scanner.conf anpassen, wenn Sie von einer früheren Avira AntiVir MailGate-Version (< 3.0.0) aktualisiert haben und die derzeitigen Einstellungen für `User/Group` von den Standardeinstellungen abweichen. Standardeinstellungen:

```
User uucp
Group antivir
```

Änderungen an `User/Group` erfordern einige weitere Änderungen:

In /etc/avira/avmailgate-scanner.conf:

- Ändern Sie den Eigentümer bzw. die Gruppe des in `ListenAddress` angegebenen Pfades (Hinweis: Die Option setzt sich aus einem Pfad und einer Socket-Datei zusammen. Beenden Sie Avira AntiVir MailGate, bevor Sie Änderungen vornehmen. Wenn die Socket-Datei existiert, löschen Sie sie und ändern Sie nur den Eigentümer bzw. die Gruppe des Verzeichnisses.)

Wenn Sie an dieser Stelle den Benutzer und/oder die Gruppe ändern, müssen Sie auch die Optionen `User` *und* `Group` *in der MailGate-Konfigurationsdatei* /etc/avira/avmailgate.conf *ändern.*

In /etc/avira/avmailgate.conf:

- Ändern Sie die Option `User/Group`.
- Ändern Sie den Eigentümer bzw. die Gruppe des in `SpoolDir` angegebenen Verzeichnisses und seiner Unterverzeichnisse (Voreingestellt: /var/spool/avmailgate).

Socket Permissions

SocketPermissions

Der Eigentümer und die Berechtigungen für den Socket des Scanner-Backends. Das Scanner-Backend muss dieselbe Benutzerkennung wie Avira AntiVir MailGate verwenden.

```
SocketPermissions 0600
```

ListenAddress

ListenAddress

Die Optionen `ListenAddress` (in avmailgate-scanner.conf) und `ScannerListenAddress` (in avmailgate.conf) legen fest, wie das Scanner-Backend zu erreichen ist. Beide Optionen müssen auf denselben Pfad verweisen (die Zeichenkette „unix:“ darf in der Option ScannerListenAddress nicht verwendet werden):

```
ListenAddress unix:/var/run/avmailgate/scanner
ScannerListenAddress /var/run/avmailgate/scanner
```

PoolScanners

PoolScanners

Um Prüfungen effizienter durchführen zu können, wird ein Pool von Scannern verwendet. Mit der Option `PoolScanners` wird die Größe dieses Pools

festgelegt.
Beachten Sie aber, dass zu viele Scanner den Rechner überlasten können, während eine zu geringe Anzahl höhere Wartezeiten für die Anwendungen verursacht.

Syntax:

```
PoolScanners "nicht-negative Zahl"
```

Voreingestellt:

```
PoolScanners 24
```

Pool Connections

PoolConnections

Die maximale Anzahl gleichzeitiger Verbindungen, die Avira AntiVir MailGate für den Scanner-Pool zulässt.

Syntax:

```
PoolConnections "nicht-negative Zahl"
```

Voreingestellt:

```
PoolConnections 128
```

Syslog Facility

SyslogFacility

Diese Option legt die Log-Kategorie fest, die Syslog für Scanner-Nachrichten verwendet.

Syntax:

```
SyslogFacility "Zeichenfolge"
```

Voreingestellt:

```
SyslogFacility mail
```

ReportLevel

ReportLevel

Der Scanner kann auf verschiedene Protokollstufen eingestellt werden:
- 0 – Fehler
- 1 – Fehler und Alarme
- 2 – Fehler, Alarme und Warnungen
- 3 – Fehler, Alarme, Warnungen und Debug-Meldungen

Ein „Alarm“ enthält Informationen über potentiell schädlichen Code.

Syntax:

```
ReportLevel "nicht-negative Zahl"
```

Voreingestellt:

```
ReportLevel 0
```

ScanTemp

ScanTemp

Das Verzeichnis, in dem der Scanner temporäre Dateien ablegt, z. B. entpackte

Archive oder gesperrte Dateien.

Das Scanner-Backend erkennt die Umgebungsvariable „TMPDIR“ nicht.

Wenn alle Avira AntiVir MailGate-Komponenten ein gemeinsames temporäres Verzeichnis verwenden sollen, ändern Sie die Optionen `TemporaryDir` *in* /etc/avira/avmailgate.conf *und* `ScanTemp` *in* avmailgate-scanner.conf.

Voreingestellt:

```
ScanTemp /var/tmp
```

LogFileName

LogFileName

Der Pfad der Scanner-Logdatei.

```
LogFileName /path/to/logfile
```

5.5 Host-Konfiguration in avmailgate.acl

Anhand der Schlüsselwörter `local` und `relay` entscheidet avmailgate.acl, welche Rechner über Avira AntiVir MailGate Emails versenden dürfen. Dabei wird die Domain oder die IP-Adresse des Absenders bzw. Empfängers verwendet.

▶ Legen Sie die lokalen Hosts und/oder Domains fest. Ein Beispiel:

```
local: localhost
local: avira.com
```

▶ Legen Sie fest, welche Hosts und Netzwerke Emails senden dürfen. Ein Beispiel:

```
relay: 127.0.0.1/8 192.168.0.0/16
```

IP-Adressen

IP-Adressen

IP-Adressen können auf verschiedene Arten angegeben werden:

```
192.168.0.0/16 oder 192.168
```

Beide Angaben haben dieselbe Bedeutung. /16 bedeutet 16 Bit und bezeichnet die ersten beiden Zahlen der IP-Adresse. Daher sind alle IP-Adressen erlaubt, die mit 192.168 beginnen.

Ein Beispiel für /etc/avira/avmailgate.acl:

```
# Access lists for AVIRA MailGate
# These hosts and/or domains are local.
local: localhost 127.0.0.1
local: avira.com
# These hosts and networks are allowed to relay.
relay: 127.0.0.1/8  192.168.0.0/16
```

Aktivieren Sie die IPv6-Unterstützung nur mithilfe der Option InetProtocols, müssen Sie für die Optionen ListenAddress und ForwardTo sowie in der avmailgate.acl-Datei IPv6-Adressen angeben.

5.6 Konfiguration der Warnungen in avmailgate.warn

Sie können optional eine weitere Datei verwenden, um die Warnmeldungen festzulegen:
/etc/avira/avmailgate.warn. Diese Datei steuert zusammen mit avmailgate.conf die Alarm-Meldungen, die an den Empfänger, den Absender und den Postmaster gesendet werden.

Ein Befehl in dieser Datei setzt sich aus zwei Einträgen zusammen:

- Am Anfang steht der Name des erkannten Virus bzw. unerwünschten Programms. Dabei dürfen auch Platzhalterzeichen verwendet werden.
- Der zweite Teil besteht aus einem oder mehreren der folgenden Buchstaben:
  - S: für den Absender
  - R: für den Empfänger
  - P: für den Postmaster
  - T: um eine SNMP-Trap zu versenden

Beispiel

Der Befehl

```
/klez/ RP
```

weist Avira AntiVir MailGate an, eine Alarm-Email an den Empfänger und den Postmaster zu senden, wenn der Virus namens Klez erkannt wird.

Im Fall der Erkennung eines speziellen Virus bzw. unerwünschten Programms haben die Einstellungen in avmailgate.warn *Vorrang vor denjenigen in* avmailgate.conf.

5.7 Berichtvorlagen konfigurieren

Sie können die Texte festlegen, die als Email-Benachrichtigungen verwendet werden, wenn die Software Viren, unerwünschte Programme oder verdächtige Dateien entdeckt.

▶ Kopieren Sie die Beispielvorlagen in der gewünschten Sprache aus dem Vorlagenverzeichnis /usr/lib/AntiVir/mailgate/templates/examples/<Sprache>/ in das Verzeichnis
/usr/lib/AntiVir/mailgate/templates.

▶ Ändern Sie das Verzeichnis in /usr/lib/AntiVir/mailgate/templates. Dieses Verzeichnis enthält die folgenden Dateien:
patho-administrator
patho-recipient
patho-sender
alert-administrator

alert-recipient
alert-sender

- Schreiben Sie die gewünschten Texte in die genannten Dateien. Behalten Sie den Aufbau der Datei bei:
  - Die erste Zeile ist der Betreff der Email.
  - Es folgt eine Leerzeile (neue Zeile).
  - Den Abschluss bildet der Text der Email.

Schlüsselwörter

Schlüsselwörter

Die Dateien alert-* und patho-* können die folgenden Schlüsselwörter enthalten, die durch den entsprechenden Text ersetzt werden:

Schlüsselwort	Text
SENDER	Die Email-Adresse des Absenders der infizierten Email.
ALERTS	Die Liste der in der Email erkannten Viren und unerwünschten Programme. Jede Zeile enthält den Namen eines Virus. Präfix und Postfix werden wiederholt.
REASON	Der Grund dafür, dass eine Email nicht geprüft wurde (in Kurzform).
ADVICE	Ein Hinweis zur Behebung des Problems (ca. 1 Zeile, siehe REASON).
QUEUEID	Die ID der Email in der Warteschlange von Avira AntiVir MailGate.
SUBJECT	Der Betreff der infizierten Email.
CONCERNING_ FILE_NAMES	Dieses Schlüsselwort wird durch eine Liste der Dateien ersetzt, in denen die Alarme entdeckt wurden.
PRODUCT_ VERSION	Die Versionsnummer des Produkts.
ENGINE_ VERSION	Die Versionsnummer der Scan-Engine.
VDF_VERSION	Die VDF-Versionsnummer.
VDF_DATE	Das Erstellungsdatum der VDF.

Beispiel für alert-sender

Beispiel für alert-sender

```
SUBJECT: AntiVir ALARM [Ihre Email: "SUBJECT"]
**********AntiVir ALARM**********
AntiVir hat in einer Email mit Ihrer Absenderadresse die
folgenden Viren/unerwünschten Programme entdeckt:
```

```
                    ALERTS
Die Email wurde nicht gesendet, sondern auf Ihrem Server
isoliert. Überprüfen Sie Ihr System umgehend auf eine
mögliche Vireninfektion.
Säubern Sie Ihr System, bevor Sie weitere Email-Nach-
richten versenden.
```

5.8 Updater-Konfiguration in avupdate-mailgate.conf

Aktualisierungen stellen sicher, dass die Komponenten von Avira AntiVir MailGate (MailGate, Scanner, VDF und Engine), die für den Schutz vor Viren und unerwünschten Programmen sorgen, stets auf dem neuesten Stand sind.

Mit Avira Updater können Sie die Avira-Software auf Ihrem Rechner mithilfe von Avira-Update-Servern aktualisieren.

Um den Aktualisierungsvorgang zu konfigurieren, verwenden Sie die Optionen in /etc/avira/avupdate-mailgate.conf, die weiter unten beschrieben sind. Alle Parameter in avupdate-mailgate.conf können dem Updater in der Kommandozeile übergeben werden. Ein Beispiel:

– Parameter in avupdate-mailgate.conf:

```
temp-dir=/tmp
```

– Befehl in der Kommandozeile:

```
/usr/lib/AntiVir/mailgate/avupdate-mailgate.bin
--temp-dir=/tmp
```

internet-srvs Die Liste der Internet-Update-Server.

```
internet-srvs=http://dl1.pro.antivir.de, http://
dl2.pro.antivir.de, http://dl3.pro.antivir.de
```

intranet-srvs Die Liste der Intranet-Update-Server.

```
intranet-srvs=http://iumserver:7080
```

master-file Die master.idx-Datei.

```
master-file=/idx/master.idx
```

install-dir Das Installationsverzeichnis für aktualisierte Produktdateien.

```
install-dir=/usr/lib/AntiVir
```

temp-dir Temporäres Verzeichnis für heruntergeladene Aktualisierungsdateien.

```
temp-dir=/tmp/avira_update
```

Email-Aktualisierungsberichte einstellen

Alle Berichte über Avira AntiVir MailGate-Aktualisierungen werden an die Email-Adressen gesendet, die in avupdate-mailgate.conf angegeben sind:

mailer

Die Berichte können via `smtp` oder via `sendmail` geschickt werden:

Voreingestellt:

```
mailer=smtp
```

smtp...

Authentifizierung der smtp-Verbindung. Aktivieren Sie die Option `auth-method` und geben Sie den smtp-Server, den Port, den Benutzer und das Passwort an.

```
auth-method=password
smtp-user=<Ihr_Benutzername>
smtp-password=<Ihr_Passwort>
smtp-server=<Servername>
smtp-port=<Port>
```

notify-when

Email-Benachrichtigungen können auf vier Werte eingestellt werden:

- 0 – Es werden keine Email-Benachrichtigungen gesendet.
- 1 – Email-Benachrichtigungen werden in folgenden Fällen gesendet: „Aktualisierung erfolgreich“, „Aktualisierung nicht erfolgreich“ und „Auf dem neuesten Stand“.
- 2 – Eine Email-Benachrichtigung wird nur bei „Aktualisierung nicht erfolgreich“ gesendet.
- 3 - Eine Email-Benachrichtigung wird nur bei „Aktualisierung erfolgreich“ gesendet

Voreingestellt:

```
notify-when=3
```

email-to

Der Empfänger der Email-Benachrichtigungen.

Voreingestellt:

```
email-to=root@localhost
```

Logdatei-Einstellungen

log

Geben Sie den vollständigen Pfad und Namen der Datei an, in die Avira AntiVir Updater seine Log-Meldungen schreibt.

```
log=/var/log/avupdate-mailgate.log
```

log-append

Die Logdatei wird standardmäßig überschrieben. Sie können diese Option benutzen, um die Log-Meldungen am Ende der Logdatei zu schreiben.

```
log-append
```

Einstellungen für Intranet-Aktualisierungen

Wenn Sie statt der voreingestellten Aktualisierung über das Internet ein Update über das Intranet bevorzugen, müssen Sie einige Parameter in der Datei avupdate-mailgate.conf konfigurieren (siehe intranet-srvs), oder selbige in der Kommandozeile eingeben:

```
intranet-srvs
```

Legt eine Liste der IUM Server, die durch Komma getrennt werden, fest.

```
product-root
```

Legt das Verzeichnis für die Aktualisierung auf dem IUM Server fest (`/update`).

```
intranet
```

Legt fest, dass die Aktualisierung statt über das Internet durch das Intranet erfolgt.

Beispiel:

```
intranet-svrs=http://iumserver:7080
product-root=/update
intranet
```

Mit dem Avira Internet Update Manager (IUM) können Sie für eine Vielzahl Ihrer Aviraprodukte automatische Updates herunterladen lassen. Die einzelnen Clientrechner in Ihrem Netzwerk müssen die Updates nicht selber über das Internet laden, stattdessen erstellt IUM einen Spiegel innerhalb Ihres lokalen Netzwerks. Weitere Informationen entnehmen Sie bitte dem IUM-Handbuch (http://www.avira.com).

Einstellungen für Fallback-Aktualisierungsserver

Wenn Sie einen Fallback-Aktualisierungsserver einrichten möchten, zum Beispiel für den Fall, dass der Intranetserver nicht ordnungsgemäß arbeitet und Sie doch über das Internet aktualisieren möchten, können Sie mithilfe der Option `peak-handling-srvs` in der Konfigurationsdatei oder in der Kommandozeile, diesen einrichten. Die Option folgt der gleichen Syntax wie `intranet-srvs`.

Beispiel:

```
peak-handling-srvs=http://dl1.pro.antivir.de,
http://dl2.pro.antivir.de, dl3.pro.antivir.de
```

Integration in Avira Security Management Center (SMC)

Damit Sie Aktualisierungen über das Avira Security Management Center (SMC) konfigurieren können, müssen Sie dem SMC-Repository das Paket mit dem Aktualisierungs-Plugin hinzufügen. Danach steht das neue Produkt „Avira Updater“ auf Rechnern, die über SMC verwaltet werden, für Installationszwecke zur Verfügung.

Das Produkt „Avira Updater“ ermöglicht die Konfiguration von Aktualisierungen für alle Produkte, die auf SMC-Rechnern installiert sind. Weitere Informationen finden Sie in der SMC-Dokumentation.

6 Bedienung

Nach Abschluss der Installation und Konfiguration und nach dem Start von Avira AntiVir MailGate ist die lückenlose Überwachung Ihres Systems durch MailGate gewährleistet. Der Verlauf des Nutzungsprozesses kann gelegentliche Änderungen an der Konfiguration erfordern. Erläuterungen dazu finden Sie im Kapitel Konfiguration – Seite 29.

In manchen Fällen ist es erforderlich, Avira AntiVir MailGate manuell zu bedienen oder die von Avira AntiVir MailGate gefilterten Dateien manuell zu verarbeiten.

In diesem Kapitel werden die folgenden Themen beschrieben:

Außerdem finden Sie hier Informationen über

6.1 Avira AntiVir MailGate manuell starten und beenden

Wenn Sie Avira AntiVir MailGate nach der Beschreibung im Kapitel Installation – Seite 17 installiert haben, wird es vom System automatisch gestartet und beendet.

In bestimmten Fällen muss Avira AntiVir MailGate jedoch manuell gestartet und beendet werden. Alle Änderungen in Konfigurationsdateien werden erst nach einem Neustart des Programms aktiviert.

Das Skript /usr/lib/AntiVir/mailgate/avmailgate startet und beendet den Scanner und den Avira AntiVir MailGate-Daemon.

Seit Version 3.0.0 verwendet Avira AntiVir MailGate einen neuen Scanner, der vor avmailgate.bin gestartet werden muss. Aus diesem Grund muss MailGate mithilfe des Skripts „avmailgate“ gestartet und beendet werden:

```
/usr/lib/AntiVir/mailgate/avmailgate start
/usr/lib/AntiVir/mailgate/avmailgate stop
```

Wenn Sie ein eigenes Skript verwenden, sollten Sie darauf achten, dass der Scanner zuerst gestartet wird. Im Skript „avmailgate“ finden Sie ein Beispiel dafür, wie das Scanner-Backend gestartet werden kann.

Wenn Sie bestimmte Kommandozeilenoptionen an Avira AntiVir MailGate übergeben möchten, können Sie sie dem Parameter „DAEMONPARAMS“ im Skript hinzufügen (siehe Parameter für avmailgate.bin).

Um Avira AntiVir MailGate manuell starten oder beenden zu können, müssen Sie als **root***-Benutzer angemeldet oder mit den erforderlichen Zugriffsrechten ausgestattet sein.*

Avira AntiVir MailGate starten

▶ Geben Sie Folgendes ein:

```
/usr/lib/AntiVir/mailgate/avmailgate start
```

↳ Das Programm wird mit der folgenden Meldung gestartet:

```
Starting AVIRA AntiVir MailGate...
Starting savapi
```

Avira AntiVir MailGate beenden

▶ Geben Sie Folgendes ein:

```
/usr/lib/AntiVir/mailgate/avmailgate stop
```

↳ Das Programm wird mit der folgenden Meldung beendet:

```
Stopping AVIRA AntiVir MailGate...
Stopping: avmailgate.bin
Shutting down Avira MailGate...
Stopping: savapi
```

Avira AntiVir MailGate neu starten

Avira AntiVir MailGate muss neu gestartet werden, wenn Sie beispielsweise Änderungen an Konfigurationsskripts vorgenommen haben.

▶ Geben Sie Folgendes ein:

```
/usr/lib/AntiVir/mailgate/avmailgate restart
```

↳ Das Programm zeigt zuerst die folgende Meldung an und startet dann neu:

```
Stopping AVIRA AntiVir MailGate...
Stopping: avmailgate.bin
Shutting down Avira MailGate...
Stopping: savapi

Starting AVIRA AntiVir MailGate...
Starting savapi
```

Avira AntiVir MailGate-Status prüfen

▶ Geben Sie Folgendes ein:

```
/usr/lib/AntiVir/mailgate/avmailgate status
```

↳ Das Programm zeigt Informationen über die MailGate-Daemons an:

```
Status: avmailgate.bin running
Status: savapi running
```

6.2 Parameter für den SMTP- und Scanner-Daemon

Die folgenden Tabellen beschreiben die möglichen Kommandozeilenparameter, die die Einstellungen in avmailgate.conf außer Kraft setzen.

Syntax:

```
avmailgate.bin [ -V | --version ] [ -C config file ] [ -A
ACL file ] [-p milter listen address ] [ --start ] [ --stop
] [ --status ] [--avq ] [ --dump-config ] [--test-active-
directory] [ --runtime-versions ] [--rebuild-quarantine-
db] [ -D debug level ]
```

Parameter für avmailgate.bin

Parameter	Beschreibung
`-V oder --version`	Zeigt die Versionsnummer an.
`-C config-file`	Verwendet eine andere Konfigurationsdatei anstelle von /etc/avira/avmailgate.conf. Wenn Sie hier `-C` angeben, müssen Sie dies auch für `--stop` und `--status` tun.
`-A ACL-file`	Verwendet eine andere ACL-Datei anstelle der Standardeinstellung /etc/avira/avmailgate.acl
`-p milter listen address`	Aktiviert den Milter-Modus und legt die `ListenAddress` (die Adresse und der Port, an die sich der SMTP-Daemon binden soll) fest.
`--start`	Startet Avira AntiVir MailGate.
`--stop`	Fährt Avira AntiVir MailGate herunter.
`--status`	Zeigt an, ob Avira AntiVir MailGate läuft.
`--avq`	Ruft den Warteschlangen-Manager auf.
`--dump-config`	Zeigt die momentan gültigen Konfigurationswerte unter Ausschluss aller in der Konfigurationsdatei vorhandenen Kommentare und deaktivierter Konfigurationseinstellungen an.

Parameter	Beschreibung
`--test-active-directory` 	Verifiziert die Konfigurationseinstellungen der Verbindungen zum ActiveDirectory Support. Mit dieser Option, die eine Abfrage zu einer gegebenen Email-Adresse durchführt und eine Liste der entsprechenden Organisationseinheiten ausgibt, testen Sie die Verbindung zum ActiveDirectory Server. Fehler werden in die Standardausgabe und in die Protokolldateien geschrieben. Verwenden Sie diesen Befehl für die Fehlersuche in Avira AntiVir MailGate ActiveDirectorySupport. *Wenn Sie dieselbe Email-Adresse für mehrere Benutzer verwenden, kann es vorkommen, dass dieselben Organisationseinheiten mehrfach zurückgegeben werden.*
`--runtime-versions` 	Zeigt Versionsinformationen über den derzeit genutzten Scanner an. Beispiel: AVE:8.2.1.172 VDF:7.10.4.134 SAVAPI:3.0.5.22 AVE ist die Versionsnummer der Scan-Engine. VDF ist die Versionsnummer der Musterdatei. SAVAPI ist die Versionsnummer des Scan-Dienstes. Eine weitere Möglichkeit besteht darin, die Parameter `-C`, `-A` und `-p` zur Variable DAEMONPARAMS im Start-/Stop-Skript `/usr/lib/AntiVir/mailgate/avmailgate` hinzuzufügen.
`--rebuild-quarantine-db`	Stellt die Quarantäne-Datenbank aus bestehenden Quarantäne-Dateien wieder her. Die Kommandozeile ist sinnvoll, wenn Sie den Quarantäne-Manager Advanced verwenden. Der Wert des Parameters `EnableLegacyQuarantine` muss auf NO gesetzt sein.
Die folgenden Optionen werden beim Debugging verwendet	
Parameter	**Beschreibung**
`-D debug-level`	Bestimmt die Genauigkeit, mit der Debug-Meldungen gespeichert werden. (Stufen 0-5, 0 = keine Speicherung, 5 = detaillierte Speicherung).

6.3 Warteschlangen-Manager avq

Der Warteschlangen-Manager avq ist in avmailgate.bin integriert. Er ermöglicht die Bearbeitung der Avira AntiVir MailGate-Spool-Verzeichnisse „incoming“ und „outgoing“ in /var/spool/avmailgate/.
Hier können Sie den Status der unbearbeiteten und in die Quarantäne verschobenen Emails anzeigen und ändern (siehe Avira AntiVir MailGate-Spool-Verzeichnisse – Seite 30).

Die Ausgabe lässt sich mithilfe der folgenden Parameter für `--avq` steuern (in der Hilfe, die Sie mit `--avq --help` aufrufen können, finden Sie weitere Parameter). Erfolgt kein Eintrag in die Kommandozeile, wird der Inhalt der Warteschlange „rejected“ ausgegeben.

Die folgenden Parameter steuern die Ausgabe:

Parameter	**Beschreibung**
`--queue=incoming`	Die Emails in der Warteschlange „incoming“ werden ausgegeben.
`--queue=outgoing`	Die Emails in der Warteschlange „outgoing“ werden ausgegeben.
`--queue=rejected`	Die Emails in der Warteschlange „rejected“ werden ausgegeben.
`--list=all`	Zeigt alle Emails in den Warteschlangen „rejected“, „incoming“ und „outgoing“. Die erste Spalte zeigt den Status der Email. In der zweiten Spalte wird die Warteschlangen-ID ausgegeben. Die dritte Spalte zeigt die Größe der Email in Bytes an. In der vierten Spalte wird die Ankunftszeit der Email wiedergegeben und die letzte Spalte zeigt den Absender- und den Empfängernamen. Siehe Beispiel unten.
`--nosort`	Deaktiviert die Sortierung. Die Emails in der Warteschlange werden standardmäßig nach Datum (nach Zeitmarke der wartenden Datei) sortiert: Die neueste Email nimmt die letzte Stelle.

Beispiel:

```
v 2402-mhLKEG 838 TUE MAY 17 12:16:56 Sender: test@example.com
                                      Recipients: test@example.com
```

Die Email mit der Warteschlangen-ID 2402-mhLKEG ist 838 Bytes groß und wurde als `v` klassifiziert. Mögliche Status-Klassifikationen sind:

Status	**Beschreibung**
`v`	Malware gefunden
`m`	Verdächtige Email gefunden

Status	Beschreibung
y	Email wird gerade erstellt
q	Email zur Verarbeitung bereit
f	Auslieferung erzwungen
x	Email wird bearbeitet

6.4 Quarantäne-Management

Avira AntiVir MailGate stellt zwei unterschiedliche Quarantäne-Manager zur Verfügung: der ursprüngliche Quarantäne-Manager Classic und der neuere Quarantäne-Manager Advanced. Es kann immer nur einer dieser Manager genutzt werden. Die Aktivierung des einen bedeutet die Deaktivierung des anderen.

***Warnung**: Die beiden Quarantäne-Manager sind nicht kompatibel. Demzufolge können Emails, die mit dem einen Quarantäne-Manager in Quarantäne verschoben wurden, nicht in das Format des jeweils anderen Quarantäne-Managers konvertiert werden.*

6.4.1 Quarantäne-Manager Classic

Möchten Sie mit der klassischen Form des Quarantäne-Managers arbeiten, behalten Sie den voreingestellten Parameter in der Konfigurationsdatei bei. Er lautet standardmäßig:

```
EnableLegacyQuarantine Yes
```

Email-Status in der Quarantäne

▶ Geben Sie Folgendes ein:

```
/usr/lib/AntiVir/mailgate/avmailgate.bin --avq
```

↳ Der Status aller Emails in der Quarantäne wird angezeigt.

Die erste Zeile enthält den Namen der angezeigten Quarantäne. Ein Beispiel:

```
Queue: rejected.
```

Am Ende der Liste wird die Anzahl der Emails in der Quarantäne ausgegeben:

```
5 mails in the rejected queue.
```

Der Quarantäne-Manager zeigt für jede Email die folgenden Statusinformationen an:

- `--> Not processed yet`
- `--> OK`
- `--> MIME problem` (Rekursion zu tief usw.)
- `--> Found e.g. (1x) Eicar Test Signature (type: virus)`

Die folgenden Statusinformationen werden in Abhängigkeit vom Ergebnis des Spam-Filters angezeigt (siehe Berichtvorlagen konfigurieren – Seite 97):

- `--> Outbreak detected`
- `--> Dangerous attachment found`
- `--> Dangerous iframe found`
- `--> Dangerous alert found`
- `--> Spam`

Die Ausgabe lässt sich mithilfe der folgenden Parameter für `--avq` steuern (in der Hilfe, die Sie mit `--avq --help` aufrufen können, finden Sie weitere Parameter).

Die folgenden Parameter steuern die Ausgabe:

Parameter	**Beschreibung**
`--list=all`	Alle Warteschlangen werden ausgegeben.
`--nosort`	Deaktiviert die Sortierung. Die Emails in der Warteschlange werden standardmäßig nach Datum (nach Zeitmarke der wartenden Datei) sortiert: Die neueste Email nimmt die letzte Stelle ein.
`--flush`	Glättet die Emails der „incoming“ und „outgoing“ Warteschlangen.

Emails aus der Warteschlange löschen

Emails in der rejected-*Warteschlange müssen manuell gelöscht werden.*

Um blockierte Emails sofort zu löschen, können Sie die Option `AlertAction` *in* avmailgate.conf *verwenden.*

Um blockierte Emails manuell zu löschen, gehen Sie wie folgt vor (siehe auch Quarantäne-Manager Advanced – Seite 109):

▶ Ermitteln Sie die Queue-ID der Email. Avira AntiVir MailGate gibt diese Queue-ID in seinen Logs und in der Email aus, die an den Postmaster gesendet wird.

Beispiel:

```
Avira MailGate has detected the following in a mail sent
through your server:
    (1x) Eicar-Test-Signature (type: virus)
The mail was not delivered.
It has been quarantined with the following queue id:
    13881-wS6dUU
```

▶ Geben Sie den folgenden Befehl ein (ID ist die <ID> der infizierten Email):

```
/usr/lib/AntiVir/mailgate/avmailgate.bin --avq --remo-
ve=<ID>
```

↳ Die Email wird aus der Warteschlange gelöscht

.

Mit den folgenden Parametern können Sie den Löschvorgang steuern:

Parameter	**Beschreibung**
`--remove=<ID>`	Löscht die Email mit der angegebenen ID.

`--remove=all`	Löscht alle Emails. Der Benutzer wird aufgefordert, die Aktion zu bestätigen:
	`# ./avmailgate.bin --avq --remove=all`
	`All mails in the directory "/var/spool/avmailgate/rejected/" will be deleted.`
	`Are you sure? [y/N] y`
	`Removing vf-14375-AZ2SEl`
	`Removing df-14375-AZ2SEl`

Email-Weiterleitung erzwingen

Warnung: *Bei diesem Vorgang können potentiell gefährliche Viren weitergeleitet werden.*

▶ Achten Sie stets darauf, welche Art Email weitergeleitet werden soll.

▶ Ermitteln Sie die ID der infizierten Email. Avira AntiVir MailGate gibt diese ID in seinen Logs und in der Email aus, die an den Postmaster gesendet wird.

```
The mail was not delivered.
It has been quarantined with the following queue id:
13881-wS6dUU
```

↳ Die Email wurde nicht zugestellt.

▶ Geben Sie den folgenden Befehl ein (ID ist die <ID> der infizierten Email):

```
/usr/lib/AntiVir/mailgate/avmailgate.bin --avq --deli-
ver=<ID>
```

↳ Die Email wird unabhängig vom Ergebnis der Virenprüfung zugestellt und aus der Quarantäne gelöscht.

6.4.2 Quarantäne-Manager Advanced

Der Quarantäne-Manager Advanced ist standardmäßig deaktiviert. Um diesen

Manager zu aktivieren, müssen Sie die Konfigurationsdatei

```
/etc/avira/avmailgate.conf
```

editieren. Stellen Sie hier die Option

```
EnableLegacyQuarantine
```

auf `NO` und speichern Sie die Änderung ab. Starten Sie Avira AntiVir MailGate.

Der Quarantäne-Manager Advanced steht im Milter-Modus nicht zur Verfügung.

Die Syntax für Aufrufe des Quarantäne-Management-Tools lautet wie folgt:

```
# avqmc-mgt [ARGUMENTE] [BEFEHL] [BEFEHLSARGUMENTE]
```

6.4.3 Funktionen des Quarantäne-Tools avqmc-mgt

Folgende Argumente stehen zur Verfügung:

```
avqmc-mgt[ -f ] [ -m ] [ -h, --help ] [--print-alert-types]
[-u <username> ] [ --version ] [ --force-root ]
```

Argument	Beschreibung
`-f`	Ein Befehl, z. B. `deliver`, wird umgehend ausgeführt, ohne, dass Sie ihn erneut bestätigen müssen.
`-m`	Die Informationen über die unter Quarantäne gestellten Emails werden mit Kommata separiert und maschinenlesbar dargestellt.
`-h, --help`	Dieses Argument listet eine kurze Beschreibung des Quarantäne-Management-Tools und der zur Verfügung stehenden Befehle und Parameter auf.
`--print-alert-types`	Gibt eine Liste der bekannten Alarm-Arten aus. Sie können mit Hilfe des Befehls `avqmc-mgt search alert_type=` nach einer spezifischen Alarm-Art suchen.
`-u <username>`	Ermöglicht, einen Benutzer direkt auszuwählen, anstatt dass dieser anhand der avqmd- Socket Permissions bestimmt wird.
`avqmd --version`	Zeigt die Versionsnummer der `avqmd`-Binärdatei an.
`avqmc-mgt --version`	Zeigt die Versionsnummer der `avqmc-mgt`-Binärdatei an.
`--force-root` 	Standardmäßig wechselt `avqmc-mgt` zu dem Benutzer, dem der Socket des Quarantäne-Management-Daemons gehört. `--force-root` verhindert, dass `avqmc-mgt` den Benutzer wechselt. Somit läuft `avqmc-mgt` als Benutzer `root`. *Bitte nutzen Sie diese Option mit Vorsicht! Sie dient allein dem Debugging.*

Folgende Befehle und Befehlsargumente stehen zur Verfügung:

```
avqmc-mgt[ list ] [ view <ID> ] [ count ] [delete all ] [
delete <ID> ] [ delete <date> ][ reprocess <ID>] [ deliver
```

```
<ID> ] [ search ]
```

Befehl/Befehlsargument	Beschreibung
`list`	Listet alle unter Quarantäne gestellten Emails auf.
`view <ID>`	Zeigt die Email mit der entsprechenden ID an.
`count`	Zeigt die Anzahl der unter Quarantäne gestellten Emails an.
`delete all`	Löscht alle unter Quarantäne gestellten Emails.
`delete <ID>`	Löscht die Email mit der entsprechenden ID.
`delete <date>`	Löscht Emails, die zu einem bestimmten Zeitpunkt oder innerhalb eines bestimmten Zeitraums unter Quarantäne gestellt wurden.
`reprocess <ID>`	Schickt die Email mit der entsprechenden ID zur erneuten Bearbeitung durch Avira AntiVir MailGate.
`deliver <ID>`	Erzwingt die Weiterleitung der Email mit entsprechender ID.
`search`	Ermöglicht das Durchsuchen der Quarantäne-Datenbank.

Quarantäne-Datenbank anzeigen

Mithilfe des Befehls

```
avqmc-mgt
```

können Sie Informationen über alle unter Quarantäne gestellten Emails anzeigen lassen, z. B.

```
...
ID: 62
 Queue-ID: 16113-Gw2lMB
 Quarantine date: Thu Sep 23 18:25:20 CEST 2010 (2010-
 09-23)
 Envelope sender: Absender@example.com
 Envelope recipient: Empfaenger@example.com
 Subject: Betreff
 Message-ID: 2010-09-23.5338@Absender
 Date: Thu, 23 Sep 2010 18:25:20 +0200
 To: Absender@example.com
 From: Empfaenger@example.com
 Alert: W32/Avira-Signatur (virus) (2)
 AVE version: 8.2.4.2
 VDF version: 7.10.4.182
ID: 63
...
```

Jede Email erhält zwei IDs, eine Datenbank-ID (z. B. `62`) und eine Queue-ID (z. B. `16113-Gw2lMB`). Die Datenbank-ID wird chronologisch, gemäß der zeitlichen Erfassung der Email in der Quarantäne vergeben. Die Queue-ID ist statisch und an

eine bestimmte Email gebunden.

```
ID: 62
Queue-ID: 16113-Gw2lMB
```

Darüber hinaus werden Datum und Uhrzeit angezeigt, zu denen eine Email in Quarantäne verschoben wurde, sowie die Eckdaten der Email (Absender, Empfänger, Betreff, Sendedatum und Message-ID) und des Scan-Ergebnisses.

Es wird festgehalten, weshalb die Email unter Quarantäne gestellt wurde (`Alert`). Enthaltene Viren, Würmer, Malware oder andere Faktoren, die zur Quarantäne geführt haben, werden nach Namen sortiert und unter Angabe ihrer Art und der Anzahl der gefundenen Malware aufgelistet.

```
Alert: W32/Avira-Signatur (virus) (2)
```

Wenn Sie den Quarantäne-Manager Advanced verwenden, werden folgende Ergebnisse ausgegeben:

```
Alert: Eicar-Test-Signatur (virus) (3)
Alert: HIDDENTEXT/Worm.Gen (heuristic) (1)
```

Außerdem finden sich hier die Versionsnummern von AVE und VDF (für Begriffserklärungen siehe 9.3 Glossar), mit denen der Email-Scan durchgeführt wurde.

```
AVE version: 8.2.4.2
VDF version: 7.10.4.182
```

Unter Quarantäne gestellte Email anzeigen

Sie können die vergebene ID dazu nutzen, sich die unter Quarantäne gestellten Emails anzeigen zu lassen.
Verwenden Sie dazu den Befehl:

```
avqmc-mgt view <ID>
```

Beispielsweise zeigt Ihnen der Befehl

```
avqmc-mgt view 62
```

die Email mit der Datenbank-ID 62 an. Mithilfe des Befehls

```
avqmc-mgt view 16113-Gw2lMB
```

können Sie sich die Email mit der Queue-ID `16113-Gw2lMB` anzeigen lassen. Die Email wird vollständig angezeigt. Die Funktionalität des view-Befehls entspricht nicht der eines Mail-Clients. Der Quarantäne-Manager Advanced verwendet das mithilfe der Variablen `$PAGER` festgelegte Programm, um die Emails anzuzeigen.

Wurde kein Programm festgelegt, wird `/usr/bin/less` aufgerufen. Ist dies nicht vorhanden, versucht der Manager auf `/usr/bin/more` zuzugreifen. Schlägt dies ebenfalls fehl, wird eine Fehlermeldung angezeigt.

Anzahl der unter Quarantäne gestellten Emails anzeigen

Geben Sie den Befehl

```
avqmc-mgt count
```

ein, wird die Anzahl der unter Quarantäne gestellten Emails angezeigt.

Unter Quarantäne gestellte Emails löschen

Es gibt verschiedene Möglichkeiten, die unter Quarantäne gestellten Emails zu löschen.

Um sämtliche Emails vollständig aus der Quarantäne zu löschen, benutzen Sie den Befehl

```
avqmc-mgt delete all
```

Möchten Sie nur eine bestimmte Email löschen, können Sie dies mit folgendem Befehl:

```
avqmc-mgt delete <ID>
```

Verwenden Sie die entsprechende Datenbank- oder Queue-ID.

Sie können eine Email auch anhand des Quarantänedatums löschen.

Das Quarantänedatum jeder Email ist in den Informationen über alle unter Quarantäne gestellten Emails enthalten, die Sie mithilfe des Befehls `avqmc-mgt` anzeigen lassen können:

```
Quarantine date: Thu Sep 23 18:25:20 CEST 2010 (2010-09-23)
```

Nutzen Sie den Befehl:

```
avqmc-mgt delete date:<YYYY-MM-DD>
```

Möchten Sie also alle Emails löschen, die am 23. September 2010 unter Quarantäne gestellt wurden, geben Sie Folgendes an:

```
avqmc-mgt delete date:2010-09-23
```

Ergänzen Sie die Angabe durch eine genaue Uhrzeit, löschen Sie alle Emails, die zu diesem Zeitpunkt unter Quarantäne gestellt wurden.

```
avqmc-mgt delete date:<YYYY-MM-DD>T<HH:MM:SS>
```

Beispiel: Mithilfe von

```
avqmc-mgt delete date:2010-09-23T09:30:00
```

werden alle Emails, die am 23.09.2010 um 9:30 Uhr unter Quarantäne gestellt wurden, gelöscht.

Alternativ können Sie auch alle Emails löschen, die in einem bestimmten Zeitraum unter Quarantäne gestellt wurden. Erweitern Sie dazu den Befehl wie folgt:

```
avqmc-mgt delete date:<YYYY-MM-DD>/<YYYY-MM-DD>
```

Geben Sie also ein:

```
avqmc-mgt delete date:2010-10-21/2010-10-24
```

löschen Sie alle Emails, die zwischen dem 21.10.2010 um 00:00 Uhr und dem

24.10.2010 um 23:59 Uhr unter Quarantäne gestellt wurden. Der Löschzeitraum würde in diesem Fall also 4 vollständige Tage umfassen.

Auch dieser Befehl kann durch eine genaue Zeitangabe in Form von Stunden, Minuten und Sekunden ergänzt werden:

```
avqmc-mgt delete date:<YYYY-MM-DD[T<HH:MM:SS>]>[/
<YYYY-MM-DD[T<HH:MM:SS>]>]
```

Beispiel:

```
avqmc-mgt delete date:2010-10-21T08:30:00/2010-10-
24T22:30:00
```

Auf diese Weise werden alle Emails, die zwischen dem 21.10.2010 um 8:30 Uhr und dem 24.10.2010 um 22:30 Uhr unter Quarantäne gestellt wurden, gelöscht.

Konnte der Befehl einwandfrei ausgeführt werden, erhalten Sie in der Kommandozeile eine entsprechende Bestätigung.

Unter Quarantäne gestellte Email erneut scannen

Mit dem Befehl

```
avqmc-mgt reprocess <ID>
```

z. B.

`avqmc-mgt reprocess 62` oder `reprocess 16113-Gw2lMB`

schicken Sie die Email zur erneuten Bearbeitung durch Avira AntiVir MailGate. Dies bietet sich an, wenn z. B. die Vermutung besteht, dass es sich um einen Fehlalarm (false positive) und somit bei der Verschiebung der Email in die Quarantäne um einen Irrtum handelt.

Mithilfe des Befehls wird die Email von Avira AntiVir MailGate erneut verschickt und damit aus der Quarantäne gelöscht. Falls sie nach dem Scan-Vorgang wieder in die Quarantäne verschoben wird, hat sie nun eine neue Datenbank-ID, die Queue-ID ist jedoch gleich geblieben.

Zustellung einer unter Quarantäne gestellten Email erzwingen

***Warnung**: Bei diesem Vorgang kann gefährliche Malware weitergeleitet werden.*

Sollte eine Email aufgrund eines Fehlalarms (false positive) oder aufgrund vorgenommener Einstellungen (z. B. hinsichtlich der Archivtiefe oder der Anhangsgröße) in die Quarantäne verschoben worden sein, können Sie die Zustellung dieser Email erzwingen.

Nutzen Sie dazu den Befehl

```
avqmc-mgt deliver
```

in Kombination mit der entsprechenden Datenbank- oder Queue-ID, z. B.:

`avqmc-mgt deliver 62` oder `avqmc-mgt deliver 16113-Gw2lMB`

Sie werden aufgefordert, die erzwungene Zustellung zu bestätigen:

Sie versuchen, Emails zu versenden, die möglicherweise infiziert sind! Möchten Sie trotzdem fortfahren? [y/N]

Mit Hilfe des Arguments -f im Befehl

```
avqmc-mgt -f deliver 62
```

werden die Emails versendet, ohne, dass Sie dies bestätigen müssen.

Quarantäne durchsuchen

Die Quarantäne-Datenbank können Sie mithilfe des folgenden Befehls durchsuchen:

```
avqmc-mgt search <search-key>=<search-value>
```

Als search-key kann entweder alert-type oder alert-name angegeben werden. Das search-value definiert diese Art oder den Namen genauer.

Beispiel für eine Suche nach einer bestimmten Alarm-Art:

```
avqmc-mgt search alert-type=virus
```

Beispiel für eine Suche nach einem bestimmten Alarm-Namen:

```
avqmc-mgt search alert-name=Eicar
```

Desweiteren kann bei der Suche **?** als Platzhalter für ein Zeichen dienen, z. B.:

```
avqmc-mgt search alert-name=Eica?
```

Das Symbol ***** können Sie als Platzhalter für eine beliebige Zeichenfolge verwenden, beispielsweise für folgende Suche:

```
avqmc-mgt search alert-name=*Signatur
```

Die Liste der alert-types*, nach denen gesucht werden kann, ist dynamisch und kann sich jederzeit ändern.*

Quarantäne-Datenbank wiederherstellen

Mithilfe der folgenden Parameter können Sie die Quarantäne-Datenbank aus bestehenden Quarantäne-Dateien wiederherstellen:

```
--rebuild-quarantine-db
```

Dies kann sinnvoll sein, wenn Sie die Datenbank-Dateien gelöscht haben. Beachten Sie hierbei Folgendes:

1. Sie müssen die Wiederherstellung manuell vornehmen:

```
# /usr/lib/AntiVir/mailgate/avmailgate.bin --rebuild-quarantine-db
```

2. Avira AntiVir MailGate darf während des Wiederherstellungsprozesses nicht laufen.

3. Die Datenbank-Datei wird gelöscht, bevor sie wiederhergestellt wird. Sie werden aufgefordert den Löschvorgang zu bestätigen, bevor der Wiederherstellungsprozess startet.

Beispiel:

```
Die Datenbank-Datei avqm.db wird vor der Wiederherstellung gelöscht.
Möchten Sie fortfahren? [y/N] y
Das Unterverzeichnis virus wird bearbeitet ...
In Quarantäne genommene Dateien wurden erfolgreich in die Datenbank eingefügt.
Die Datenbank wurde wiederhergestellt.
```

Fehlermeldungen werden wie folgt ausgegeben:

```
Das Unterverzeichnis virus wird bearbeitet ...
Fehler beim Bearbeiten der Quarantäne-Datei 55f5a870.qua.
Es sind keine Dateien vorhanden, um sie der Datenbank hinzuzufügen.
Detailinformationen wurden im Syslog, Kategorie 'daemon' geloggt.
```

6.5 Verfahren beim Erkennen von Viren oder unerwünschten Programmen

Wenn Sie Avira AntiVir MailGate richtig konfiguriert haben, werden alle wichtigen Antivirus-Aufgaben in Ihrem System automatisch erledigt:

- Infizierte Emails werden nicht weitergeleitet.
- Infizierte Emails werden nach /var/spool/avmailgate/rejected verschoben (oder in ein anderes in avmailgate.conf angegebenes Verzeichnis), wo sich die Datendatei (df-) und die Steuerdatei (vf- oder mf-) befinden. Weitere Informationen finden Sie unter Avira AntiVir MailGate-Spool-Verzeichnisse – Seite 30.
- Datendateien enthalten möglicherweise Emails, in denen Viren oder unerwünschte Programme gefunden wurden. Diese Dateien können zusammen mit der Steuerdatei direkt gelöscht oder mit dem Warteschlangen-Manager (--avq) verarbeitet werden.
- Abhängig von den Einstellungen in avmailgate.conf kann der Postmaster Alarme an die Absender und/oder Empfänger infizierter Emails senden.
- Abhängig von den Einstellungen in avmailgate.conf können infizierte Emails durch externe Programme oder Skripts weiterverarbeitet werden.

Diese Verfahren verringern die Gefahr, dass sich eine Infektion ausbreitet.

Die folgenden Schritte sollten immer durchgeführt werden:

▶ Versuchen Sie herauszufinden, auf welchem Weg der Virus oder das unerwünschte Programm in Ihr System eingedrungen ist.

▶ Prüfen Sie jeden beteiligten Datenträger gezielt.

▶ Informieren Sie Ihr Team, Ihre Vorgesetzten und Ihre Geschäftspartner.

▶ Informieren Sie Ihren Systemadministrator und Ihren Sicherheitsanbieter.

Infizierte Dateien an Avira GmbH senden

▶ Senden Sie uns die Viren, unerwünschten Programme und verdächtigen Dateien zu, die von unseren Produkten noch nicht erkannt oder entdeckt werden. Der Virus oder das unerwünschte Programm sollte gepackt (PGP, gzip, WinZIP, PKZip, Arj) und als Anlage einer Email an virus@antivir.com gesendet werden.

Verwenden Sie beim Packen das Passwort virus. *So wird die Datei nicht von Virenscannern auf Email-Gateways gelöscht.*

7 Aktualisierungen

Mit Avira Updater können Sie die Avira-Software auf Ihren Rechnern mithilfe von Avira-Update-Servern aktualisieren. Das Programm kann entweder durch Bearbeiten der Konfigurationsdatei (siehe 5.8 Updater-Konfiguration in avupdate-mailgate.conf) oder über Parameter in der Kommandozeile konfiguriert werden.

Es wird empfohlen, den Updater als **root** auszuführen. Wenn der Updater nicht als **root** ausgeführt wird, fehlen ihm die notwendigen Berechtigungen zum Neustart der Avira AntiVir MailGate-Daemons, und der Neustart muss manuell als **root** durchgeführt werden.

Dies hat den Vorteil, dass alle laufenden Prozesse von Avira AntiVir MailGate-Daemons (z. B. Scanner und MailGate) automatisch mit den neuesten Antivirendateien aktualisiert werden, ohne die laufenden Prüfprozesse zu unterbrechen. Auf diese Weise ist sichergestellt, dass alle Dateien geprüft werden.

7.1 Internet-Aktualisierungen

Manuell

Wenn Sie Avira AntiVir MailGate oder einige seiner Komponenten aktualisieren möchten:

▶ Verwenden Sie den folgenden Befehl:

```
/usr/lib/AntiVir/mailgate/avupdate-mailgate
--product=[Produkt]
```

Als `[Produkt]` können Sie Folgendes eingeben:

- `Scanner` – (empfohlen) die Scannerkomponenten wie Engine und VDF-Dateien werden aktualisiert.
- `MailGate` – vollständige Aktualisierung (MailGate, Scanner, Engine und VDF-Dateien).

Wenn Sie nur nach einer neuen Avira AntiVir MailGate-Version suchen möchten, ohne Avira AntiVir MailGate zu aktualisieren:

▶ Verwenden Sie den folgenden Befehl:

```
/usr/lib/AntiVir/mailgate/avupdate-mailgate
--check --product=[Produkt]
```

Die Werte für `[Produkt]` sind die gleichen wie im obigen Beispiel.

Automatische Aktualisierungen mit dem Cron-Daemon

Regelmäßige Aktualisierungen werden mit dem Cron-Daemon durchgeführt.

Die entsprechenden Einstellungen für den Cron-Daemon **sind bereits vorhanden, wenn** Sie, während der Avira AntiVir MailGate-Installation mit dem install-Skript, die Frage, ob Avira AntiVir Updater installiert und automatisch gestartet werden soll, mit `Ja` beantwortet haben.

Weitere Informationen über den Cron-Daemon finden Sie in Ihrer UNIX-Dokumentation.

So können Sie die Einstellungen für automatische Aktualisierungen in der Cron-Konfiguration manuell festlegen oder ändern:

▶ Fügen Sie der Datei /etc/cron.d/avira_updater den gewünschten Eintrag hinzu oder bearbeiten Sie ihn (siehe folgendes Beispiel).

Beispiel: Um die Aktualisierung stündlich (immer um *:23) durchzuführen, geben Sie den folgenden Befehl ein:

```
23 * * * * root /usr/lib/AntiVir/mailgate/avupdate-mailgate
--product=[Produkt]
```

Als `[Produkt]` können Sie Folgendes eingeben:

- `Scanner` – (empfohlen) der Scanner wird aktualisiert.
- `MailGate` – vollständige Aktualisierung (MailGate, Scanner, Engine und VDF-Dateien).

▶ Starten Sie den Aktualisierungsprozess, um die Einstellungen zu überprüfen:

```
/usr/lib/AntiVir/mailgate/avupdate-mailgate
--product=[Produkt]
```

Die Werte für `[Produkt]` sind die gleichen wie im obigen Beispiel.

↳ War die Aktualisierung erfolgreich, wird ein Bericht in die Logdatei /var/log/avupdate-mailgate.log geschrieben.

8 Service

8.1 FAQs

8.1.1 Überwachung von SNMP Traps unter Debian 5

1.) Installieren Sie das snmpd Paket:

```
$ apt-get install snmpd
```

2.) Kopieren Sie die MIB-Dateien des Avira AntiVir MailGate Pakets nach /usr/share/snmp/mibs:

```
$ cp antivir-mailgate-prof-<Version>/etc/AVIRA-*-MIB.txt
/usr/share/snmp/mibs
```

3.) Konfigurieren Sie snmpd so, dass die Avira AntiVir MailGate MIB-Dateien gelesen werden:

```
$ echo "+mibs AVIRA-MIB" >> /etc/snmp/snmp.conf
$ echo "+mibs AVIRA-MAILGATE-V0-MIB" >>
/etc/snmp/snmp.conf
```

4.) Konfigurieren Sie snmpd, indem Sie /etc/snmp/snmptrapd.conf editieren. Geben Sie an, dass Avira AntiVir MailGate SNMP Traps akzeptiert werden sollen:

```
$ echo "authCommunity log,execute,net SNMP_COMMUNITY" >>
/etc/snmp/snmptrapd.conf
```

Ersetzen Sie SNMP_COMMUNITY mit dem für die SNMPCommunity Option gültigen Wert (voreingestellt `Avira`).

Anschließend konfigurieren Sie snmptrapd so, dass bei Empfang einer bestimmten SNMP Trap ein benutzerdefiniertes Programm aufgerufen wird.

Mit folgender Zeile beispielsweise

```
traphandle AVIRA-MAILGATE-V0-MIB::mgtAlert /usr/local/
bin/mailgate_alert
```

wird snmptrapd jedes Mal /usr/local/bin/mailgate_alert ausführen, wenn eine mgtAlert Trap empfangen wird.

/usr/local/bin/mailgate_alert kann z.B. folgendermaßen aussehen:

```
#!/bin/bash

read host
read ip
vars=

name=
klass=
qid=

while read oid val
do
  if [ "$oid" = "AVIRA-MAILGATE-V0-MIB::mgtMalwareName.0" ]
  then
    name=$val
  fi

  if [ "$oid" = "AVIRA-MAILGATE-V0-MIB::mgtMalwareClass.0" ]
  then
    klass=$val
  fi

  if [ "$oid" = "AVIRA-MAILGATE-V0-MIB::mgtQueueItemID.0" ]
  then
    qid=$val
  fi
done

echo "MailGate found $name (classification: $klass) in $qid"
```

5.) Führen Sie `snmptrapd -f` aus und warten Sie bis Avira AntiVir MailGate die mgtAlert Trap versendet. (Sie könnten z.B. den Eicar Test Virus durch Avira AntiVir MailGate verschicken, um ein Versenden der Trap auszulösen).

Im Terminal, in dem Sie `snmptrapd` gestartet haben, sollte nun Folgendes zu lesen sein:

```
MailGate found "Eicar-Test-Signature" (classification:
"virus") in "XXX"
```

(XXX steht für die Queue-ID der Email)

8.2 Support

Support-ServiceAuf unserer Website http://www.avira.com/de/support finden Sie alle erforderlichen Informationen zu unserem umfangreichen Support-Service.

Forum FAQ

Forum FAQ

Bevor Sie die Hotline kontaktieren, empfehlen wir Ihnen einen Besuch in unserem Benutzerforum unter http://forum.antivir.de.
Lesen Sie auch den Abschnitt FAQ auf unserer Website.
Möglicherweise sind Ihre Fragen hier schon von anderen Benutzern gestellt und beantwortet worden.

Email-Support

Email-Support

Support per Email erhalten Sie unter der Adresse support@avira.com

8.3 Kontakt

Adresse

Avira GmbH
Kaplaneiweg 1
88069 Tettnang
Deutschland

Internet

Weitere Informationen über uns und unsere Produkte finden Sie unter http://www.avira.com.

9 Anhang

9.1 Versendete SNMP-Traps

mgtUp:

Avira AntiVir MailGate wurde gestartet.

mgtDown:

Avira AntiVir MailGate wurde beendet.

mgtSmtpServerDown:

Der SMTP-Server (avgated) wurde unerwartet beendet, d.h. er wurde durch ein Signal heruntergefahren oder mit einem anderen Exit Code als 0 beendet.

mgtSmtpSessionDown:

Eine SMTP-Sitzung wurde unerwartet beendet, d.h. sie wurde durch ein Signal heruntergefahren oder mit einem anderen Exit Code als 0 beendet. Übermittelte Parameter: Der Exit Code sowie das empfangene Signal. Einer dieser beiden Parameter ist mit 0 angegeben.

mgtForwarderDown:

Der Weiterleitungsserver (avgatefwd) wurde unerwartet beendet, d.h. er wurde durch ein Signal heruntergefahren oder mit einem anderen Exit Code als 0 beendet.

mgtForwarderSessionDown:

Der Weiterleitungsprozess wurde unerwartet beendet, d.h. er wurde durch ein Signal oder mit einem anderen Exit Code als 0 beendet. Übermittelte Parameter: Der Exit Code sowie das empfangene Signal. Einer dieser beiden Parameter ist mit 0 angegeben.

mgtCannotForwardMail:

Der Weiterleitungsprozess konnte keine Email versenden.

mgtAlert:

Der Scanner hat Malware gefunden. Übermittelte Parameter: Malware-Name, Zuordnung und die ID des Warteschlangenelements, in dem die Malware gefunden wurde.

Diese SNMP-Benachrichtigung muss vom Anwender ausdrücklich aktiviert werden, indem /etc/avira/avmailgate.warn angepasst wird.

mgtSuspicious:

Der Scanner konnte den Scanprozess nicht abschließen, so dass die Email als verdächtig ('suspicious') eingeordnet wurde. Übermittelte Parameter: Der Grund, aus dem der Scanner die Email als verdächtig eingestuft hat and die ID des entsprechenden Warteschlangenelements.

mgtMalwareScannerUnreach:

Es kann keine Verbindung zum Malware-Scanner hergestellt werden.

mgtQuarantineDaemonDown:

Der Quarantäne-Daemon wurde unerwartet beendet, d.h. er wurde durch ein Signal oder mit einem anderen Exit Code als 0 beendet.

mgtScannerSpamCheckerUnreach:

Es kann keine Verbindung zum Spam-Filter (eXpurgate) hergestellt werden.

mgtLicenceWillExpireSoon:

Die Lizenz läuft in weniger als N Tagen ab (die Zahl N wird mit der Option NotifyEnd OfLicense – Page 69 festgelegt). Übermittelte Parameter: Anzahl der Tage, für die die Lizenz noch gültig ist.

mgtLicenceExceeded:

Avira AntiVir MailGate wird dazu verwendet, Emails einer höheren Anzahl an Benutzern zu bearbeiten, als es gemäß der Lizenz gestattet ist (Lizenz erwerben – Page 18).

mgtQueueReachedHighFillLevel:

Der maximale Schwellwert der eingehenden oder ausgehenden Emails in der Warteschlange ist erreicht. Eine Integer-Variable identifiziert die entsprechende Warteschlange, für die das Trap gesendet wird . Das Trap wird nur gesendet, wenn die Einstellung QueueFillLevel aktiviert ist (siehe Enhanced QueueHandling – Page 64).

mgtQueueReachedLowFillLevel:

Nach Erreichen des maximalen Schwellwertes, ist der minimale Schwellwert eingehender oder ausgehender Emails in der Warteschlange wieder erreicht. Eine Integer-Variable identifiziert die entsprechende Warteschlange, für die das Trap gesendet wird. Das Trap wird nur gesendet, wenn die Einstellung QueueFillLevel aktiviert ist (siehe Enhanced QueueHandling – Page 64).

9.2 Versendete Benachrichtigungs-Emails

Benachrichtigungs-Emails

Der SMTP Server wurde unerwartet beendet (avgated), d.h. er wurde durch ein Signal oder mit einem anderen Exit Code als 0 beendet.

Ein untergeordneter Prozess des SMTP Server (avgated) wurde unerwartet beendet, d.h. er wurde durch ein Signal oder mit einem anderen Exit Code als 0 beendet.

Der Weiterleitungs-Daemonprozess (avgatefwd) wurde unerwartet beendet, d.h. er wurde durch ein Signal oder mit einem anderen Exit Code als 0 beendet.

Ein Weiterleitungsprozess wurde unerwartet beendet, d.h. er wurde durch ein Signal oder mit einem anderen Exit Code als 0 beendet.

Avira AntiVir MailGate kann die Verbindung zum Malware-Server (SAVAPI) nicht herstellen.

Der Quarantäne-Daemon wurde unerwartet beendet, d.h. er wurde durch ein Signal oder mit einem anderen Exit Code als 0 beendet.

Avira AntiVir MailGate kann keine Verbindung zum Spam-Filter herstellen (eXpurgate).

Der maximale Schwellwert der eingehenden oder ausgehenden Emails in der Warteschlange ist erreicht (wird nur gesendet, wenn die Einstellung QueueFillLevel aktiviert ist).

Der minimale Schwellwert der eingehenden oder ausgehenden Emails in der Warteschlange ist erreicht (wird nur gesendet, wenn die Einstellung QueueFillLevel aktiviert ist).

Eine verschlüsselte Email wurde gefunden (wird nur gesendet, wenn die Konfigurationsoption EncryptedEmailOption auf `NOTIFY_POSTMASTER` gesetzt ist).

9.3 Glossar

Begriff	Bedeutung
AVE (Anti Virus Engine)	AVE bezeichnet die Scan-Engine, die der Virenscanner nutzt, um die Emails nach potentiell schadhaften Programmen zu durchsuchen.
cron (Daemon)	Ein Daemon, der zu vorgegebenen Zeiten andere Programme startet.
Daemon	Ein im Hintergrund laufender Prozess zur Systemverwaltung unter UNIX. Im Schnitt werden auf einem Rechner einige Dutzend Daemons ausgeführt. Diese Prozesse werden normalerweise zusammen mit dem Rechner gestartet und heruntergefahren.
Eicar	Das European Institute for Computer Antivirus Research bietet einen Testvirus zum Testen von Antiviren-Programmen an. Weitere Informationen finden Sie unter http://www.eicar.org
IUM	Avira Internet Update Manager
Logdatei	Auch: Berichtdatei. Eine Datei mit Berichten, die vom Programm zur Laufzeit generiert werden, wenn bestimmte Ereignisse eintreten.
Malware	Ein Oberbegriff für „Fremdkörper“ jeglicher Art. Dies können Störungen wie z. B. Viren sein, aber auch andere Software, die vom Nutzer im Allgemeinen als unerwünscht betrachtet wird (siehe auch „Unerwünschte Programme“).

Begriff	Bedeutung
MIME	Multipurpose Internet Mail Extensions: Internet-Erweiterungen, die dazu dienen, Binärdateien in Emails zu integrieren. MIME unterstützt so genannte Multipart-Emails. Dadurch werden verschiedene Dateitypen in einer Email, binäre Anhänge und HTML-Emails ermöglicht.
MTA	Mail Transport Agent: ein Programm, das Emails per SMTP versendet. Beispiele: Sendmail, Postfix, Exim.
Quarantäneverzeichnis	Das Verzeichnis, in dem infizierte Dateien abgelegt werden, um sie dem Zugriff des Benutzers zu entziehen (z. B. rejected).
root	Ein Benutzer mit unbeschränkten Zugriffsrechten (z. B. der Systemadministrator unter Windows).
Scan-Engine	Das Avira AntiVir MailGate-Softwaremodul, das die Suche nach Viren und unerwünschten Programmen steuert.
SAVAPI	Secure AntiVirus Application Programming Interface
Skript	Eine Textdatei mit Befehlen, die von UNIX ausgeführt werden (ähnlich einer Batch-Datei unter DOS).
SMC	Avira Security Management Center
SMTP	Simple Mail Transfer Protocol: Ein Protokoll für die Email-Kommunikation im Internet.
syslog-Daemon	Ein Daemon, der von Programmen zur Protokollierung unterschiedlicher Informationen verwendet wird. Die Berichte werden in verschiedene Logdateien geschrieben.
Unerwünschte Programme	Ein Oberbegriff für Programme, die ohne Zustimmung des Benutzers oder Administrators installiert wurden und daher unerwünscht sind, obwohl sie auf dem Rechner keinen direkten Schaden anrichten. Dazu zählen u. a. Backdoors (BDC), Dialer, Witzprogramme und Spiele.
VDF (Virus Definition File)	Eine Datei mit festgelegten Regeln, die der Erkennung von Malware dienen. In vielen Fällen ist es für eine Aktualisierung ausreichend, die neueste Version dieser Datei zu laden.

9.4 Weitere Informationen

Weitere Informationen zu Viren, Würmern, Makroviren und anderen unerwünschten Programmen finden Sie unter http://www.avira.com.

9.5 Goldene Regeln zum Schutz vor Viren

- Erstellen Sie Startdisketten für Ihre Netzwerkserver und Workstations.
- Nehmen Sie Disketten nach Beenden der Arbeit immer aus dem Laufwerk. Auch Disketten ohne ausführbare Programme können Programmcode im Bootsektor enthalten und dadurch Träger eines Bootsektorvirus sein.
- Fertigen Sie regelmäßig Backups Ihrer Daten an.
- Beschränken Sie den Austausch von Programmen. Dies gilt insbesondere für andere Netzwerke, Mailboxen, das Internet und Bekannte.
- Prüfen Sie neue Programme vor der Installation und führen Sie danach eine Prüfung des Datenträgers durch. Liegt das Programm komprimiert vor, lässt sich ein Virus in der Regel erst nach dem Entpacken und bei der Installation finden.

Haben andere Personen Zugang zu Ihrem Rechner, sollten Sie zum Schutz vor Viren folgende Regeln beachten:

- Stellen Sie einen Testrechner bereit, auf dem Sie Software-Downloads, Demoversionen und virenverdächtige Datenträger (Disketten, CD-R, CD-RW, Wechsellaufwerke) untersuchen können.
- Trennen Sie den Testrechner vom Netzwerk!
- Benennen Sie einen Datenschutzbeauftragten, der bei einer Virusinfektion für die Behandlung verantwortlich ist, und bestimmen Sie alle zur Beseitigung eines Virus notwendigen Schritte.
- Erstellen Sie einen Notfallplan. Ein solcher Plan kann Schäden/Verluste durch mutwillige Zerstörung, Diebstahl, Ausfall oder Veränderungen durch Inkompatibilitäten verhindern. Programme und Speichergeräte lassen sich ersetzen, nicht aber Daten, die für das wirtschaftliche Überleben eines Unternehmens notwendig sind.
- Erstellen Sie einen Schutz- und Wiederherstellungsplan für Ihre Daten.
- Sorgen Sie für ein einwandfrei konfiguriertes Netzwerk und weisen Sie Zugriffsrechte nach vernünftigen Gesichtspunkten zu.

  Mit diesen Maßnahmen sind Sie gegen Viren bestens geschützt.

Ausgabe Q2-2011

AVIRA

live free.™

Avira GmbH
Kaplaneiweg 1
88069 Tettnang
Germany

Telefon: +49 7542-500 0
Telefax: +49 7542-500 3000
www.avira.de