SOPHOS

Security made simple.

Sophos Anti-Virus für Linux

Konfigurationsanleitung

Produktversion: 9

Inhalt

1 Einleitung

Diese Anleitung beschreibt den Einsatz und die Konfiguration von Sophos Anti-Virus für Linux.

Informationen zur Installation erhalten Sie wie folgt:

Um Sophos Anti-Virus zur Verwaltung mit Sophos Central zu installieren, melden Sie sich bei Sophos Central an, gehen zur Seite „Downloads“ und folgen dort den Anweisungen.

Informationen zur Installation von Sophos Anti-Virus zur Verwaltung mit Sophos Enterprise Console entnehmen Sie bitte der Sophos Enterprise Console *Startup-Anleitung zu Linux und UNIX*.

Anweisungen zur Installation/Deinstallation von nicht-verwaltetem Sophos Anti-Virus auf Netzwerk- und Einzelplatzrechnern entnehmen Sie bitte der *Startup-Anleitung* zu Sophos Anti-Virus für Linux.

Begleitmaterial zu Sophos Software finden Sie hier:
http://www.sophos.com/de-de/support/documentation.aspx.

Wichtig: Die Konfigurationshinweise in dieser Anleitung gelten auch für Sophos Linux Security.

2 Informationen zu Sophos Anti-Virus für Linux

2.1 Funktionen von Sophos Anti-Virus

Sophos Anti-Virus erkennt und verarbeitet Viren (einschließlich Würmer und Trojaner) auf dem Linux-Computer. Es werden nicht nur Linux-Viren, sondern auch Viren anderer Betriebssysteme erkannt, die sich unter Umständen auf dem Linux-Computer befinden und auf Computer mit anderen Plattformen übertragen werden. Hierzu wird Ihr Computer überprüft.

2.2 Funktionsweise von Sophos Anti-Virus

Die On-Access-Überprüfung ist der Hauptmechanismus zum Schutz vor Viren und sonstigen Threats. Bei jedem Öffnen, Speichern oder Kopieren einer Datei überprüft Sophos Anti-Virus die Datei und erlaubt den Zugriff nur dann, wenn die Datei sicher ist.

Mit Sophos Anti-Virus können Sie auch eine *On-Demand-Überprüfung* ausführen, die weiteren Schutz bietet. On-Demand-Überprüfungen werden vom Benutzer eingeleitet. Sie können alle Objekte überprüfen, für die Sie Lesezugriff besitzen – der Überprüfungsumfang reicht von einzelnen Dateien bis hin zum gesamten Computer: Sie können On-Demand-Überprüfungen manuell durchführen oder zeitlich planen und automatisch ausführen lassen.

2.3 Benutzerschnittstelle von Sophos Anti-Virus

Sie führen sämtliche Aufgaben über die Befehlszeilenschnittstelle aus.

Zum Ausführen aller Befehle mit Ausnahme von **savscan**, dem Befehl für die On-Demand-Überprüfung, müssen Sie als root-Benutzer angemeldet sein.

In diesem Handbuch wird davon ausgegangen, dass Sophos Anti-Virus im Standardverzeichnis installiert wurde: `/opt/sophos-av`. Die Pfade der beschriebenen Befehle sind an diesem Verzeichnis orientiert.

2.4 Konfiguration von Sophos Anti-Virus

Die Methoden zur Konfiguration von Sophos Anti-Virus richten sich danach, ob Sie Sophos Verwaltungssoftware (Sophos Enterprise Console oder Sophos Central) nutzen oder nicht.

Über Enterprise Console oder Sophos Central verwaltete Computer

Wenn Ihre Linux-Computer über Enterprise Console oder Sophos Central verwaltet werden, konfigurieren Sie Sophos Anti-Virus wie folgt:

- Die **On-Access-Überprüfung, zeitgesteuerte Überprüfung, Benachrichtigungen und Alarme sowie die Protokolle und Updates** werden zentral über die Management-Konsole konfiguriert. Weitere Informationen entnehmen Sie bitte der Hilfe in der Management-Konsole.

Hinweis: Die Funktionen umfassen auch Parameter, die nicht zentral über die Management-Konsole festgelegt werden können. Sie können die Parameter lokal über die CLI von Sophos Anti-Virus auf allen Linux-Computern festlegen. Sie werden von der Management-Konsole ignoriert.

Hinweis: Falls Sie mit 64-Bit Linux-Servern arbeiten, die über Sophos Central verwaltet werden, lesen Sie in der Sophos Linux Security Startup-Anleitung nach.

- Konfigurieren Sie **On-Demand-Überprüfungen** von Sophos Anti-Virus lokal über die Befehlszeile auf allen Linux-Computern.

Netzwerkcomputer, die nicht über Enterprise Console oder Sophos Central verwaltetet werden

Wenn Sie über ein Netzwerk mit Linux-Computern verfügen, das *nicht* über Enterprise Console oder Sophos Central verwaltet wird, konfigurieren Sie Sophos Anti-Virus wie folgt:

- Sie können **On-Access-Überprüfungen, zeitgesteuerte Überprüfungen, Alarme, die Protokollfunktion sowie Updates** zentral konfigurieren, indem Sie die Konfigurationsdatei ändern, anhand derer die Computer Updates beziehen. Siehe Anhang: Konfiguration mit Extradateien (Seite 41).
- Konfigurieren Sie **On-Demand-Überprüfungen** von Sophos Anti-Virus lokal über die Befehlszeile auf allen Computern.

Hinweis: Greifen Sie nur auf die Konfiguration mit Extradateien zurück, wenn Ihnen der technische Support dazu rät oder wenn Ihnen keine Sophos Management-Konsole zur Verfügung steht. Die Konfiguration der Management-Konsole lässt sich nicht mit der Konfiguration mit Extradateien kombinieren.

Nicht über Enterprise Console oder Sophos Central verwalteter Einzelplatzcomputer

Wenn Sie über einen Einzelplatz-Linux-Computer verfügen, der *nicht* über Enterprise Console oder Sophos Central verwaltet wird, konfigurieren Sie alle Sophos Anti-Virus-Funktionen über die Befehlszeile.

3 On-Access-Scans

Die On-Access-Überprüfung ist der Hauptmechanismus zum Schutz vor Viren und sonstigen Threats. Bei jedem Öffnen, Speichern oder Kopieren einer Datei überprüft Sophos Anti-Virus die Datei und erlaubt den Zugriff nur dann, wenn die Datei sicher ist.

3.1 Prüfen, ob die On-Access-Überprüfung aktiv ist

- Geben Sie folgenden Befehl ein, um zu prüfen, ob die On-Access-Überprüfung aktiv ist:
  `/opt/sophos-av/bin/savdstatus`

3.2 Prüfen, ob beim Systemstart automatisch die On-Access-Überprüfung gestartet wird

Sie müssen sich auf dem Computer als „root“ anmelden, um das Verfahren durchführen zu können.

1. So überprüfen Sie, ob **`savd`** beim Systemstart automatisch gestartet wird:
   `chkconfig --list`

   Hinweis: Wenn der Befehl auf Ihrer Linux-Distribution nicht funktioniert, lassen Sie sich die beim Systemstart angezeigten Dienste mit einem passenden Tool anzeigen.

   Wenn die Liste einen Eintrag für sav-protect mit 2:on, 3:on, 4:on und 5:on enthält, so wird die On-Access-Überprüfung beim Systemstart automatisch ausgeführt.

   Geben Sie anderenfalls Folgendes ein:

   `/opt/sophos-av/bin/savdctl enableOnBoot savd`

2. Über folgenden Befehl können Sie prüfen, ob die automatisch die On-Access-Überprüfung mit **`savd`** gestartet wurde:
   `/opt/sophos-av/bin/savconfig query EnableOnStart`

   Wenn die Befehlsausgabe `true` lautet, wird die On-Access-Überprüfung beim Systemstart mit **`savd`** automatisch gestartet.

   Geben Sie anderenfalls Folgendes ein:

   `/opt/sophos-av/bin/savconfig set EnableOnStart true`

3.3 Starten der On-Access-Überprüfung

Sie können die On-Access-Überprüfung anhand einer der folgenden Methoden einleiten:

- Geben Sie Folgendes ein:
  `/opt/sophos-av/bin/savdctl enable`

- Starten Sie den installierten Dienst „sav-protect“ mit dem entsprechenden Tool. Beispiel:
  `/etc/init.d/sav-protect start`

  oder

```
service sav-protect start
```

3.4 Anhalten der On-Access-Überprüfung

Wichtig: Wenn Sie die On-Access-Überprüfung deaktivieren, sucht Sophos Anti-Virus in aufgerufenen Dateien nicht nach Bedrohungen. Dies setzt Ihren und die damit verbundenen Computer Risiken aus.

- Geben Sie zum Anhalten der On-Access-Überprüfung Folgendes ein:
  `/opt/sophos-av/bin/savdctl disable`

4 On-Demand-Scans

On-Demand-Überprüfungen werden vom Benutzer eingeleitet. Sie können alle Objekte überprüfen, für die Sie Lesezugriff besitzen – der Überprüfungsumfang reicht von einzelnen Dateien bis hin zum gesamten Computer: Sie können On-Demand-Überprüfungen manuell durchführen oder zeitlich planen und automatisch ausführen lassen.

Über den Befehl **`crontab`** können Sie einen Zeitplan für eine On-Demand-Überprüfung festlegen. Weitere Informationen entnehmen Sie bitte dem Sophos Support-Artikel 12176.

4.1 Ausführen einer On-Demand-Überprüfung

Der Befehl zur Einleitung einer On-Demand-Überprüfung lautet **`savscan`**.

4.1.1 Überprüfen des Computers

- Durch Eingabe des folgenden Befehls wird eine Überprüfung durchgeführt:
  `savscan /`

4.1.2 Überprüfen eines Verzeichnisses oder einer Datei

- Wenn Sie ein bestimmtes Verzeichnis oder eine Datei überprüfen möchten, geben Sie den entsprechenden Pfad an. Beispiel:
  `savscan /usr/Verzeichnis/Datei`

  Sie können mehrere Verzeichnisse oder Dateien hintereinander in die Befehlszeile eingeben.

4.1.3 Überprüfen eines Dateisystems

- Wenn ein Dateisystem überprüft werden soll, geben Sie den entsprechenden Namen ein. Beispiel:
  `savscan /home`

  Sie können mehrere Dateisysteme hintereinander in die Befehlszeile eingeben.

4.1.4 Überprüfen eines Boot-Sektors

Hinweis: Die Anweisungen beziehen sich ausschließlich auf Linux und FreeBSD.

Melden Sie sich zum Überprüfen eines Bootsektors als Superuser an. So erhalten Sie die erforderlichen Zugriffsrechte auf Laufwerke.

Sie können den Bootsektor logischer oder physischer Laufwerke überprüfen.

- Geben Sie zum Überprüfen des Bootsektors logischer Laufwerke Folgendes ein:
  `savscan -bs=`*`Laufwerk, Laufwerk, ...`*

  Dabei steht *Laufwerk* für einen Laufwerksnamen, wie etwa `/dev/fd0` oder `/dev/hda1`.

- Geben Sie zum Überprüfen des Bootsektors sämtlicher von Sophos Anti-Virus erkannter logischer Laufwerke Folgendes ein:
  `savscan -bs`

- Geben Sie zum Überprüfen des Master Boot Records aller festen physischen Laufwerke Folgendes ein:
  `savscan -mbr`

4.2 Konfigurieren von On-Demand-Überprüfungen

In diesem Abschnitt bezieht sich der Platzhalter *Pfad* hinter einem Befehl auf den zu überprüfenden Pfad.

Eine vollständige Liste der Optionen in Zusammenhang mit der On-Demand-Überprüfung erhalten Sie durch Eingabe von:

`man savscan`

4.2.1 Überprüfen aller Dateitypen

Standarmäßig überprüft Sophos Anti-Virus nur ausführbare Dateien. Eine vollständige Liste der von Sophos Anti-Virus standardmäßig überprüften Dateitypen erhalten Sie durch Eingabe von **`savscan -vv`**.

- Sollen alle Dateitypen überprüft werden, geben Sie die Option **-all** an. Geben Sie Folgendes ein:
  `savscan` *`Pfad`* **`-all`**

  Hinweis: Dies kann jedoch längere Überprüfungszeiten, eine Herabsetzung der Serverleistung sowie die Ausgabe falscher Virenreports zur Folge haben.

4.2.2 Überprüfen eines bestimmten Dateityps

Standarmäßig überprüft Sophos Anti-Virus nur ausführbare Dateien. Eine vollständige Liste der von Sophos Anti-Virus standardmäßig überprüften Dateitypen erhalten Sie durch Eingabe von **`savscan -vv`**.

- Sollen nur bestimmte Dateitypen überprüft werden, geben Sie die Option **-ext** mit der entsprechenden Dateinamenerweiterung ein. Wenn z.B. nur Dateien mit der Erweiterung `.txt` überprüft werden sollen, geben Sie Folgendes ein:
  `savscan` *`Pfad`* **`-ext=txt`**

- Sollen bestimmte Dateitypen nicht überprüft werden, geben Sie die Option **-next** mit der entsprechenden Dateinamenerweiterung ein.

Hinweis: Mehrere Dateitypen sind durch Komma abzutrennen.

4.2.3 Überprüfen aller Archivarten

Mit Sophos Anti-Virus lässt sich auch der Inhalt von Archiven überprüfen. Eine Liste der Archivtypen, die überprüft werden können, erhalten Sie durch Eingabe von **`savscan -vv`**.

Hinweis: Die Threat Detection Engine überprüft nur archivierte Dateien bis 8 GB (in dekomprimierter Form). Das liegt daran, dass die Engine das POSIX ustar-Archivformat unterstützt, das keine größeren Dateien verarbeiten kann.

- Sollen alle Archivtypen überprüft werden, geben Sie als Option **-archive** an. Geben Sie Folgendes ein:
  savscan *Pfad* **-archive**

  Archive, die in andere Archive eingebettet sind (z.B. ein TAR-Archiv in einem ZIP-Archiv), werden rekursiv überprüft.

  Wenn Sie über viele umfangreiche Archive verfügen, kann die Überprüfung mehr Zeit in Anspruch nehmen. Dies sollten Sie bei der Planung zeitgesteuerter Überprüfungen berücksichtigen.

4.2.4 Überprüfen bestimmter Archivarten

Sie können die Überprüfung mit Sophos Anti-Virus auch auf ganz bestimmte Archivtypen beschränken. Eine Liste der Archivtypen, die überprüft werden können, erhalten Sie durch Eingabe von **savscan -vv**.

Hinweis: Die Threat Detection Engine überprüft nur archivierte Dateien bis 8 GB (in dekomprimierter Form). Das liegt daran, dass die Engine das POSIX ustar-Archivformat unterstützt, das keine größeren Dateien verarbeiten kann.

- Soll ein bestimmter Archivtyp überprüft werden, geben Sie die in der Liste aufgeführte Option an. Durch folgende Eingabe werden z.B. nur TAR- und ZIP-Archive überprüft:
  savscan *Pfad* **-tar -zip**

  Archive, die in andere Archive eingebettet sind (z.B. ein TAR-Archiv in einem ZIP-Archiv), werden rekursiv überprüft.

  Wenn Sie über viele umfangreiche Archive verfügen, kann die Überprüfung mehr Zeit in Anspruch nehmen. Dies sollten Sie bei der Planung zeitgesteuerter Überprüfungen berücksichtigen.

4.2.5 Überprüfen von Remote-Computern

Sophos Anti-Virus überprüft in der Regel keine Objekte auf Remote-Computern (d.h. SAV durchquert keine Remote Mount Points).

- Zum Überprüfen von Remote-Computern verwenden Sie die Option **--no-stay-on-machine**. Geben Sie Folgendes ein:
  savscan *Pfad* **--no-stay-on-machine**

4.2.6 Deaktivieren der Überprüfung symbolisch verknüpfter Objekte

Standardmäßig überprüft Sophos Anti-Virus symbolisch verknüpfte Objekte.

- Wenn Sie die Überprüfung symbolisch verknüpfter Objekte deaktivieren möchten, verwenden Sie die Option **--no-follow-symlinks**. Geben Sie Folgendes ein:
  savscan *Pfad* **--no-follow-symlinks**

  Wenn Objekte nicht mehr als einmal überprüft werden sollen, verwenden Sie als Option **--backtrack-protection**.

4.2.7 Überprüfen des ursprünglichen Dateisystems

Sophos Anti-Virus kann so konfiguriert werden, dass nur das Dateisystem überprüft wird, in dem sich der angegebene Pfad befindet. So kann eine Überprüfung mehrerer Mount Points verhindert werden.

- Um nur das ursprüngliche Dateisystem zu überprüfen, verwenden Sie die Option **--stay-on-filesystem**. Geben Sie Folgendes ein:
  savscan *Pfad* **--stay-on-filesystem**

4.2.8 Auschluss von Objekten von der Überprüfung

Mit der Option **-exclude** können Sie in Sophos Anti-Virus bestimmte Objekte (Dateien, Verzeichnisse oder Dateisysteme) von der Überprüfung ausschließen. Sophos Anti-Virus schließt alle hinter der Option in der Befehlszeichenfolge angegebenen Objekte von der Überprüfung aus. Wenn z.B. die Objekte „`fred`“ und „`harry`“, nicht aber „`tom`“ und „`peter`“ überprüft werden sollen, geben Sie Folgendes ein:

```
savscan fred harry -exclude tom peter
```

Sie können auch Verzeichnisse und Dateien von der Überprüfung ausschließen, die einem Verzeichnis *untergeordnet* sind. Wenn z.B. Freds gesamtes „home“-Verzeichnis überprüft werden soll, nicht aber das Verzeichnis „`games`“ (inklusive aller untergeordneten Verzeichnisse und Dateien), geben Sie Folgendes ein:

```
savscan /home/fred -exclude /home/fred/games
```

Außerdem können Sie Sophos Anti-Virus mit der Option **-include** mitteilen, dass die aufgezählten Objekte in die Überprüfung *eingeschlossen* werden sollen. Wenn z.B. die Objekte „`fred`“, „`harry`“ und „`bill`“, nicht aber „`tom`“ und „`peter`“ überprüft werden sollen, geben Sie Folgendes ein:

```
savscan fred harry -exclude tom peter -include bill
```

4.2.9 Überprüfen ausführbarer UNIX-Dateien

Normalerweise überprüft Sophos Anti-Virus keine Dateien, die UNIX als ausführbar betrachtet.

- Sollen Dateien überprüft werden, die UNIX als ausführbar betrachtet, verwenden Sie die Option **--examine-x-bit**. Geben Sie Folgendes ein:
  savscan *Pfad* **--examine-x-bit**

  Sophos Anti-Virus überprüft weiterhin auch alle Dateitypen, die standardmäßig dafür festgelegt sind. Eine Liste der Erweiterungen, die überprüft werden können, erhalten Sie durch Eingabe von **savscan -vv**.

5 Was passiert, wenn ein Virus erkannt wird?

Wenn bei der On-Access-Überprüfung oder On-Demand-Überprüfung Viren erkannt werden, werden standardmäßig folgende Maßnahmen von Sophos Anti-Virus vorgenommen:

- Festhalten des Ereignisses im Systemprotokoll und im Sophos Anti-Virus-Protokoll (nähere Informationen entnehmen Sie bitte dem Abschnitt Aufrufen des Protokolls von Sophos Anti-Virus (Seite 19)).
- Versenden eines Alarms an Enterprise Console (bei Verwaltung mit Enterprise Console).
- Versenden einer E-Mail-Benachrichtigung an „root@localhost“.

Standardmäßig gibt Sophos Anti-Virus zudem Alerts aus, aus denen hervorgeht, ob die Viren von der On-Access-Überprüfung oder On-Demand-Überprüfung erkannt wurden (siehe unten).

On-Access-Überprüfung

Wenn ein Virus bei der On-Access-Überprüfung erkannt wird, verweigert Sophos Anti-Virus den Zugriff auf die Datei. Standardmäßig wird zudem ein Pop-up-Alarme auf dem Desktop (wie unten abgebildet) angezeigt.

Wenn kein Pop-up-Alarme auf dem Desktop angezeigt werden kann, wird eine Befehlszeilenbenachrichtigung angezeigt.

Informationen zur Beseitigung von Viren finden Sie unter Bereinigen von Viren (Seite 16).

On-Demand-Überprüfungen

Wenn bei der On-Demand-Überprüfung ein Virus erkannt wird, zeigt Sophos Anti-Virus standardmäßig eine Befehlszeilenbenachrichtigung an. Der Virus wird in der Zeile gemeldet, die mit>>>, gefolgt von `Virus` oder `Virus Fragment`, beginnt:

```
SAVScan virus detection utility
Version 4.69.0 [Linux/Intel]
Virus data version 4.69
Includes detection for 2871136 viruses, Trojans and worms
Copyright (c) 1989-2012 Sophos Limited. All rights reserved.
System time 13:43:32, System date 22 September 2012
IDE directory is: /opt/sophos-av/lib/sav
 Using IDE file nyrate-d.ide
. . . . . .
Using IDE file injec-lz.ide
Quick Scanning
>>> Virus 'EICAR-AV-Test' found in file /usr/mydirectory/eicar.src
33 files scanned in 2 seconds.
1 virus was discovered.
1 file out of 33 was infected.
Please send infected samples to Sophos for analysis.
For advice consult www.sophos.com/de-de or email support@sophos.de
End of Scan.
```

Informationen zur Beseitigung von Viren finden Sie unter Bereinigen von Viren (Seite 16).

6 Bereinigen von Viren

6.1 Bereinigungs-Details

Auf der Sophos Website erhalten Sie weitere Informationen und Bereinigungshinweise zu Viren.

So rufen Sie die Bereinigungs-Details ab:

1. Rufen Sie die Seite mit den Sicherheitsanalysen auf: (http://www.sophos.com/de-de/threat-center/threat-analyses/viruses-and-spyware.aspx).
2. Suchen Sie die Analyse des Virus anhand des von Sophos Anti-Virus gemeldeten Namens.

6.2 Isolieren infizierter Dateien

Sie können On-Demand-Überprüfungen so konfigurieren, dass infizierte Dateien in Quarantäne verschoben und so von jeglichen Zugriffen isoliert werden. Dies wird durch Änderung der Besitz- und Zugriffsrechte der infizierten Dateien erreicht.

Hinweis: Wenn Sie sowohl Desinfektion (siehe Bereinigen infizierter Dateien (Seite 17)) als auch Quarantäne auswählen, versucht Sophos Anti-Virus zunächst, die infizierten Objekte zu desinfizieren. Wenn dies nicht gelingt, werden die Dateien in Quarantäne verschoben und somit isoliert.

In diesem Abschnitt bezieht sich der Platzhalter *Pfad* hinter einem Befehl auf den zu überprüfenden Pfad.

6.2.1 Angabe der Parameter für Quarantäne

- Der Befehlszeilenparameter zum Isolieren von Dateien lautet **--quarantine**. Geben Sie Folgendes ein:
  savscan *Pfad* **--quarantine**

6.2.2 Parameter für Besitz- und Zugriffsrechte

Standardmäßig führt Sophos Anti-Virus Folgendes durch:

- Der Benutzer, der Sophos Anti-Virus ausführt, wird zum Eigentümer der infizierten Datei.
- Die Gruppe, der der Benutzer angehört, erhält das Besitzrecht an der Datei.
- Die Zugriffsrechte auf die Datei werden in **-r-------- (0400**) geändert.

Sie können den Eigentümer, das Gruppenbesitzrecht und die Zugriffsrechte, die infizierten Dateien von Sophos Anti-Virus automatisch zugewiesen werden, jedoch selbst angeben. Dazu gibt es folgende Parameter:

```
uid=nnn
user=Benutzername
gid=nnn
group=Gruppenname
mode=ppp
```

Zum Festlegen des Eigentümers oder des Gruppenbesitzes dürfen Sie nicht mehr als einen Parameter angeben. Zum Beispiel ist es nicht möglich, den Parameter **uid** *und* den Parameter **user** anzugeben.

Für alle nicht von Ihnen verwendeten Parameter wird der Vorgabewert (siehe oben) übernommen.

Beispiel:

```
savscan fred --quarantine:user=virus,group=virus,mode=0400
```

Dieser Befehl weist einer infizierten Datei den Eigentümer „virus“, die Gruppe „virus“ und die Zugriffsberechtigung *-r--------* zu. Die Datei gehört folglich dem Benutzer „virus“ und der Gruppe „virus“ an, doch nur der Benutzer namens „virus“ erhält (Lese-)Zugriff auf die Datei. Nur der Benutzer „root“ kann Änderungen an der Datei vornehmen.

Als Voraussetzung zum Ändern der Besitz- und Zugriffsrechte kann die Anmeldung mit besonderen Rechten erforderlich sein (z.B. als „superuser“).

6.3 Bereinigen infizierter Dateien

Sie können infizierte Dateien bei einer On-Demand-Überprüfung bereinigen (desinfizieren oder löschen). Alle von Sophos Anti-Virus gegen infizierte Dateien ergriffenen Maßnahmen sind in einer Zusammenfassung und im Sophos Anti-Virus-Protokoll aufgeführt. Standardmäßig ist die Bereinigung deaktiviert.

In diesem Abschnitt bezieht sich der Platzhalter *Pfad* hinter einem Befehl auf den zu überprüfenden Pfad.

6.3.1 Löschen einer bestimmten infizierten Datei

- Zum Desinfizieren einer infizierten Datei geben Sie den Parameter **-di** an. Geben Sie Folgendes ein:
  savscan *Pfad* **-di**

  Sie müssen Ihre Eingabe bestätigen, bevor Sophos Anti-Virus die Datei desinfiziert.

  Hinweis: Durch die Desinfizierung von infizierten Dokumenten werden keine von dem Virus vorgenommenen Änderungen rückgängig gemacht. Unter Bereinigungs-Details (Seite 16) erfahren Sie, wie Sie sich auf der Sophos Website über die Folgeerscheinungen eines bestimmten Virus informieren.

6.3.2 Löschen aller infizierten Dateien auf einem Computer

- Zum Bereinigen aller infizierten Dateien auf einem Computer geben Sie folgenden Befehl ein:
  savscan / -di

  Sie müssen Ihre Eingabe bestätigen, bevor Sophos Anti-Virus die Datei desinfiziert.

  Hinweis: Durch die Desinfizierung von infizierten Dokumenten werden keine von dem Virus vorgenommenen Änderungen rückgängig gemacht. Unter Bereinigungs-Details (Seite 16) erfahren Sie, wie Sie sich auf der Sophos Website über die Folgeerscheinungen eines bestimmten Virus informieren.

6.3.3 Löschen einer bestimmten infizierten Datei

- Zum Desinfizieren einer bestimmten infizierten Datei geben Sie den Parameter **-remove** an. Geben Sie Folgendes ein:
  savscan *Pfad* **-remove**

  Sie müssen Ihre Eingabe bestätigen, bevor Sophos Anti-Virus die Datei löscht.

6.3.4 Löschen aller infizierten Dateien auf einem Computer

- Zum Löschen aller infizierten Dateien auf einem Computer geben Sie folgenden Befehl ein:
  savscan / -remove

  Sie müssen Ihre Eingabe bestätigen, bevor Sophos Anti-Virus die Datei löscht.

6.3.5 Desinfizieren eines infizierten Bootsektors

Hinweis: Die Anweisungen beziehen sich ausschließlich auf Linux und FreeBSD.

- Sie können infizierte Bootsektoren über die Option **-di** und **-bs** desinfizieren. Beispiel:
  savscan -bs=/dev/fd0 -di

  Dabei steht **/dev/fd0** für den Namen des Laufwerks mit dem infizierten Bootsektor.

  Sie müssen Ihre Eingabe bestätigen, bevor Sophos Anti-Virus die Datei desinfiziert.

6.4 Beheben von Virenschäden

Das Vorgehen zum Beheben eines virenbedingten Schadens richtet sich danach, auf welche Weise der Computer infiziert wurde. Einige Viren hinterlassen keine Schäden, während andere Viren einen so großen Schaden verursachen, dass die gesamte Festplatte davon betroffen sein kann.

Einige Viren nehmen nach und nach geringfügige Änderungen an Daten vor. Diese Art der Schädigung ist besonders schwer zu erkennen. Daher raten wir Ihnen, die Sicherheitsanalysen auf der Sophos Website zu lesen und betroffene Dokumente nach der Desinfizierung sorgfältig zu überprüfen.

Sicherungskopien sind unerlässlich. Falls Sie vor einer Infizierung noch keine Sicherungskopien angelegt hatten, sollten Sie nach der Bereinigung und Desinfizierung damit anfangen, damit Sie in Zukunft besser vorbereitet sind.

Manchmal lassen sich jedoch noch Daten auf von Viren beschädigten Festplatten retten. Sophos verfügt über Tools zur Behebung bestimmter Virenschäden. Der technische Support kann Ihnen bei der Problembehebung behilflich sein.

7 Aufrufen des Protokolls von Sophos Anti-Virus

Sophos Anti-Virus schreibt alle Überprüfungsvorgänge in das Sophos Anti-Virus-Protokoll und in das syslog-Protokoll. Des Weiteren werden Viren- und Fehlerereignisse im Protokoll von Sophos Anti-Virus verzeichnet.

- Zum Abrufen des Sophos Anti-Virus-Protokolls geben Sie den Befehl **`savlog`** ein. Durch die Verwendung von Optionen kann die Ausgabe auf bestimmte Meldungen beschränkt werden. Außerdem lässt sich die Darstellungsweise bestimmen.

  Wenn Sie z.B. alle Meldungen abrufen möchten, die in den letzten 24 Stunden im Sophos Anti-Virus-Protokoll festgehalten wurden, und das Datum sowie die Uhrzeit gemäß der ISO-Norm 8601 im UTC-Format angegeben werden sollen, lautet der Befehl wie folgt:

  ```
  /opt/sophos-av/bin/savlog --today --utc
  ```

- Eine vollständige Liste der Optionen in Zusammenhang mit **`savlog`** erhalten Sie durch Eingabe von:

  ```
  man savlog
  ```

8 Sofort-Update von Sophos Anti-Virus

Wenn Auto-Updates aktiviert sind, wird Sophos Anti-Virus automatisch auf den neuesten Stand gebracht. Sie können Sophos Anti-Virus ein Update auch sofort durchführen lassen, so dass Sie nicht auf das nächste automatische Update warten müssen.

- Geben Sie auf dem Computer, auf dem Sie das Update von Sophos Anti-Virus durchführen möchten, Folgendes ein:
  `/opt/sophos-av/bin/savupdate`

Hinweis: Sofort-Updates sind auch über Sophos Enterprise Console möglich.

9 Kernel-Unterstützung

Hinweis: Der Abschnitt ist nur relevant, wenn Talpa als Interception-Methode für On-Access-Überprüfungen festgelegt wurde. Nähere Informationen entnehmen Sie bitte dem Abschnitt Ändern der Bedingungen für On-Access-Überprüfungen (Seite 37).

9.1 Unterstützung neuer Kernel-Versionen

Wenn einer der von Sophos Anti-Virus unterstützten Linux-Hersteller ein Update des Linux Kernel herausgibt, gibt Sophos ein Update des Sophos Kernel-Oberflächenmoduls heraus, um das Update zu unterstützen. Wenn Sie das Update eines Linux Kernels vor dem Update des entsprechenden Talpa-Updates installieren, initiiert Sophos Anti-Virus eine lokale Talpa-Kompilierung. Wenn dies nicht erfolgreich ist, verwendet Sophos Anti-Virus Fanotify als Interception-Methode. Wenn Fanotify ebenfalls nicht verfügbar ist, wird die On-Acces-Überprüfung abgebrochen, und es wird ein Fehler ausgegeben.

Sie können das Problem umgehen, indem Sie sicherstellen, dass das passende Talpa-Update vor der Übertragung des Linux Kernel-Updates veröffentlicht wurde. Eine Liste unterstützter Linux-Versionen und -Updates finden Sie im Sophos Support-Artikel 14377 (http://www.sophos.com/de-de/support/knowledgebase/14377.aspx). Wenn das erforderliche Talpa-Update aufgeführt wird, steht es zum Download bereit. Wenn Auto-Updates aktiviert sind, lädt Sophos Anti-Virus das Update automatisch herunter. Sie können Sophos Anti-Virus ein Update auch sofort durchführen lassen, so dass Sie nicht auf das nächste automatische Update warten müssen. Geben Sie hierzu Folgendes ein:

```
/opt/sophos-av/bin/savupdate
```

Danach können Sie das Update des Linux Kernels übertragen.

9.2 Unterstützung kundenspezifischer Kernel

Dieses Handbuch beschreibt die Konfiguration von Updates zur Unterstützung kundenspezifischer Linux Kernel nicht. Details hierzu finden Sie im Support-Artikel 13503 (http://www.sophos.com/de-de/support/knowledgebase/13503.aspx).

10 Konfigurieren von zeitgesteuerten Überprüfungen

Sophos Anti-Virus kann Definitionen mehrerer zeitgesteuerter Überprüfungen speichern.

Hinweis: Die Namen von über Enterprise Console erstellten Überprüfungen beginnen mit „SEC:“ und können nur in Enterprise Console geändert oder entfernt werden.

10.1 Laden einer zeitgesteuerten Überprüfung aus einer Datei

1. Um eine Vorlagen-Überprüfungsdefinition als Startpunkt zu verwenden, öffnen Sie `/opt/sophos-av/doc/namedscan.example.en`.

   Um eine neue Überprüfungsdefinition zu erstellen, öffnen Sie eine neue Textdatei.
2. Bestimmen Sie die Objekte und die Zeitpunkte für die Überprüfung, und legen Sie anhand der Parameter in der Vorlage sonstige Optionen fest.

   Zur Planung der Überprüfung müssen zumindest ein Tag und eine Uhrzeit eingestellt werden.
3. Speichern Sie die Datei in einem beliebigen Verzeichnis. Achten Sie jedoch darauf, dass die Vorlage nicht überschrieben wird.
4. Weisen Sie die über den Befehl **`savconfig`** gefolgt vom Vorgang **add** und dem Parameter **NamedScans** die zeitgesteuerte Überprüfung Sophos Anti-Virus zu. Geben Sie den Namen der Überprüfung und den Pfad der Überprüfungsdefinitionsdatei an.

   Um z.B. eine Überprüfung namens „Daily“ zu laden, die sich unter dem Pfad `/home/fred/DailyScan` befindet, geben Sie ein:

   ```
   /opt/sophos-av/bin/savconfig add NamedScans Daily
   /home/fred/DailyScan
   ```

10.2 Einrichten einer zeitgesteuerten Überprüfung über Tastatureingabe

1. Weisen Sie die über den Befehl **`savconfig`** gefolgt vom Vorgang **add** und dem Parameter **NamedScans** die zeitgesteuerte Überprüfung Sophos Anti-Virus zu. Geben Sie den Namen der Überprüfung gefolgt von einem Bindestrich ein. Somit geben Sie an, dass die Definition über die Tastatur eingelesen werden soll.

   Um zum Beispiel eine Überprüfung namens „Daily“ einzurichten, geben Sie Folgendes ein:

   ```
   /opt/sophos-av/bin/savconfig add NamedScans Daily -
   ```

   Wenn Sie die Eingabetaste drücken, wartet Sophos Anti-Virus auf Ihre Eingabe der Definition für die zeitgesteuerte Überprüfung.

2. Bestimmen Sie die Objekte und die Zeitpunkte für die Überprüfung, und legen Sie anhand der Parameter in der Vorlagen-Überprüfungsdefinition sonstige Optionen fest: `/opt/sophos-av/doc/namedscan.example.en`. Drücken Sie nach Eingabe jedes Parameters und des Werts jeweils die Eingabetaste.

   Zur Planung der Überprüfung müssen zumindest ein Tag und eine Uhrzeit eingestellt werden.

3. Wenn Sie mit der Definition fertig sind, drücken Sie STRG+D.

10.3 Exportieren einer zeitgesteuerten Überprüfung in eine Datei

- Wenn Sie eine zeitgesteuerte Überprüfung von Sophos Anti-Virus in eine Datei exportieren möchten, geben Sie den Befehl **`savconfig`** gefolgt vom Vorgang **query** und dem Parameter **NamedScans** ein. Geben Sie den Namen der Überprüfung und den Pfad der Datei ein, in die Sie die Überprüfung exportieren möchten.

  Um z.B. eine Überprüfung namens „Daily“ in die Datei `/home/fred/DailyScan` zu exportieren, geben Sie ein:

  `/opt/sophos-av/bin/savconfig query NamedScans Daily > /home/fred/DailyScan`

10.4 Exportieren aller zeitgesteuerten Überprüfungen in eine Datei

- Wenn alle zeitgesteuerten Überprüfungen (einschl. der mit Enterprise Console erstellten Überprüfungen) von Sophos Anti-Virus in eine Datei exportiert werden sollen, geben Sie den Befehl **`savconfig`** gefolgt vom Vorgang **query** und dem Parameter **NamedScans** ein. Geben Sie den Pfad der Datei an, in die die Überprüfungen exportiert werden sollen.

  Um z.B. die Namen aller zeitgesteuerten Überprüfungen in die Datei `/home/fred/AllScans` zu exportieren, geben Sie ein:

  `/opt/sophos-av/bin/savconfig query NamedScans > /home/fred/AllScans`

  Hinweis: Die Überprüfung `SEC:FullSystemScan` ist immer definiert, wenn der Computer von Enterprise Console verwaltet wird.

10.5 Senden einer zeitgesteuerten Überprüfung an die Standardausgabe

- Wenn Sie eine zeitgesteuerte Überprüfung von Sophos Anti-Virus an die Standardausgabe senden möchten, geben Sie den Befehl **`savconfig`** gefolgt vom Vorgang **query** und dem Parameter **NamedScans** ein. Geben Sie den Namen der Überprüfung ein.

  Um zum Beispiel die Definition der Überprüfung „Daily“ an die Standardausgabe zu senden, geben Sie ein:

  `/opt/sophos-av/bin/savconfig query NamedScans Daily`

10.6 Exportieren der Namen aller zeitgesteuerten Überprüfungen in die Standardausgabe

- Wenn alle zeitgesteuerten Überprüfungen (einschl. der mit Enterprise Console erstellten Überprüfungen) von Sophos Anti-Virus an die Standardausgabe gesendet werden sollen, geben Sie den Befehl **`savconfig`** gefolgt vom Vorgang **query** und dem Parameter **NamedScans** ein.

  Um die Namen aller zeitgesteuerten Überprüfungen an die Standardausgabe zu senden, geben Sie Folgendes ein:

  `/opt/sophos-av/bin/savconfig query NamedScans`

  Hinweis: Die Überprüfung `SEC:FullSystemScan` ist immer definiert, wenn der Computer von Enterprise Console verwaltet wird.

10.7 Ändern einer zeitgesteuerten Überprüfung, die aus einer Datei geladen wurde

Hinweis: Sie können keine zeitgesteuerten Überprüfungen ändern, die mit Enterprise Console erstellt wurden.

1. Öffnen Sie die Datei, in der die zeitgesteuerte Überprüfung definiert ist, die geändert werden soll.

   Wenn die Überprüfung nicht bereits in einer Datei definiert wurde, können Sie die Überprüfung in eine Datei exportieren. Lesen Sie dazu den Abschnitt Exportieren einer zeitgesteuerten Überprüfung in eine Datei (Seite 23).

2. Passen Sie die Definition ggf. an. Verwenden Sie dabei nur Parameter, die in der Vorlagen-Überprüfungsdefinition aufgeführt sind: `/opt/sophos-av/doc/namedscan.example.en`. Die Überprüfung muss vollständig definiert werden, d.h. Sie dürfen nicht nur die Bereiche angeben, die geändert werden sollen.
3. Speichern Sie die Datei.
4. Ändern Sie die zeitgesteuerte Überprüfung in Sophos Anti-Virus über den Befehl **`savconfig`** gefolgt vom Vorgang **update** und dem Parameter **NamedScans**. Geben Sie den Namen der Überprüfung und den Pfad der Überprüfungsdefinitionsdatei an.

   Um z.B. eine Überprüfung namens „Daily“ zu ändern, die sich unter dem Pfad `/home/fred/DailyScan` befindet, geben Sie ein:

   `/opt/sophos-av/bin/savconfig update NamedScans Daily /home/fred/DailyScan`

10.8 Ändern einer zeitgesteuerten Überprüfung über Tastatureingabe

Hinweis: Sie können keine zeitgesteuerten Überprüfungen ändern, die mit Enterprise Console erstellt wurden.

1. Ändern Sie die zeitgesteuerte Überprüfung in Sophos Anti-Virus über den Befehl **`savconfig`** gefolgt vom Vorgang **update** und dem Parameter **NamedScans**. Geben Sie den Namen der Überprüfung gefolgt von einem Bindestrich ein. Somit geben Sie an, dass die Definition über die Tastatur eingelesen werden soll.

   Um zum Beispiel eine Überprüfung namens „Daily“ zu ändern, geben Sie ein:

   ```
   /opt/sophos-av/bin/savconfig update NamedScans Daily -
   ```

   Wenn Sie die Eingabetaste drücken, wartet Sophos Anti-Virus auf Ihre Eingabe der Definition für die zeitgesteuerte Überprüfung.

2. Bestimmen Sie die Objekte und die Zeitpunkte für die Überprüfung, und legen Sie anhand der Parameter in der Vorlagen-Überprüfungsdefinition sonstige Optionen fest: `/opt/sophos-av/doc/namedscan.example.en`. Drücken Sie nach Eingabe jedes Parameters und des Werts jeweils die Eingabetaste. Die Überprüfung muss vollständig definiert werden, d.h. Sie dürfen nicht nur die Bereiche angeben, die geändert werden sollen.

   Zur Planung der Überprüfung müssen zumindest ein Tag und eine Uhrzeit eingestellt werden.

3. Wenn Sie mit der Definition fertig sind, drücken Sie STRG+D.

10.9 Aufrufen eines Protokolls einer zeitgesteuerten Überprüfung

- Sie können das Protokoll der zeitgesteuerten Überprüfung über den Befehl **`savlog`** und die Option **namedscan** festlegen. Geben Sie den Namen der Überprüfung ein.

  Um z.B. dedas Protokoll der täglichen Überprüfung abzurufen, geben Sie Folgendes ein:

  ```
  /opt/sophos-av/bin/savlog --namedscan=Daily
  ```

10.10 Löschen einer zeitgesteuerten Überprüfung

Hinweis: Sie können keine zeitgesteuerten Überprüfungen löschen, die mit Enterprise Console erstellt wurden.

- Wenn Sie eine zeitgesteuerte Überprüfung aus Sophos Anti-Virus löschen möchten, geben Sie den Befehl **`savconfig`** gefolgt vom Vorgang **remove** und dem Parameter **NamedScans** ein. Geben Sie den Namen der Überprüfung ein.

  Um zum Beispiel eine Überprüfung namens „Daily“ zu löschen, geben Sie ein:

  ```
  /opt/sophos-av/bin/savconfig remove NamedScans Daily
  ```

10.11 Löschen aller zeitgesteuerten Überprüfungen

Hinweis: Sie können keine zeitgesteuerten Überprüfungen löschen, die mit Enterprise Console erstellt wurden.

- Geben Sie folgenden Befehl ein, wenn Sie alle zeitgesteuerten Überprüfungen aus Sophos Anti-Virus löschen möchten:
  `/opt/sophos-av/bin/savconfig delete NamedScans`

11 Konfigurieren von Alerts

Hinweis: Wenn Sie einen einzigen Computer im Netzwerk konfigurieren, könnte die Konfiguration beim Download einer neuen Konfiguration (über Enterprise Console oder Konfiguration mit Extradateien) auf diesem Computer überschrieben werden.

Sie können Sophos Anti-Virus so konfigurieren, dass bei Virenerkennung, Überprüfungsfehlern oder sonstigen Fehlern eine Benachrichtigung versendet wird. Solche Alarme können in der folgenden Form vorliegen:

- Popup-Benachrichtigungen auf dem Desktop (nur On-Access-Überprüfung)
- Befehlszeile (nur On-Demand-Überprüfung)
- E-Mail (On-Access-Überprüfung und On-Demand-Überprüfung).

Popup-Benachrichtigungen auf dem Desktop und Befehlszeilenbenachrichtigungen werden in der Sprache des Computers, auf dem das Problem auftritt, angezeigt.
E-Mail-Benachrichtigungen können auf Englisch und Japanisch verfasst werden.

11.1 Konfigurieren von Popup-Benachrichtigungen auf dem Desktop

11.1.1 Deaktivieren von Popup-Benachrichtigungen auf dem Desktop

Standardmäßig sind Popup-Benachrichtigungen auf dem Desktop aktiviert.

- Geben Sie zum Deaktivieren der Popup-Benachrichtigungen auf dem Desktop folgenden Befehl ein:
  `/opt/sophos-av/bin/savconfig set UIpopupNotification disabled`

- Wenn Sie sowohl Popup-Benachrichtigungen auf dem Desktop als auch Befehlszeilenbenachrichtigungen deaktivieren möchten, geben Sie Folgendes ein:
  `/opt/sophos-av/bin/savconfig set UINotifier disabled`

11.1.2 Angeben einer benutzerdefinierten Meldung

Sie können eine benutzerdefinierte Meldung festlegen, die zu allen Befehlszeilenbenachrichtigungen und Popup-Benachrichtigungen auf dem Desktop hinzugefügt wird.

👉 **Merke!:** Die Hauptnachricht wird in verschiedenen Sprachen angezeigt (je nach Systemeinstellungen), aber der angepasste Text bleibt in der Sprache, die Sie bei dessen Festlegung verwendet haben.

- Sie können die Meldung über den Parameter **UIContactMessage** angeben. Beispiel:
  `/opt/sophos-av/bin/savconfig set UIContactMessage 'Contact IT'`

11.2 Konfigurieren von Befehlszeilenbenachrichtigungen

11.2.1 Deaktivieren von Befehlszeilenbenachrichtigungen

Standardmäßig sind Befehlszeilenbenachrichtigung aktiviert.

- Geben Sie zum Deaktivieren von Befehlszeilenbenachrichtigungen folgenden Befehl ein:
  `/opt/sophos-av/bin/savconfig set UIttyNotification disabled`

- Wenn Sie sowohl Popup-Benachrichtigungen auf dem Desktop als auch Befehlszeilenbenachrichtigungen deaktivieren möchten, geben Sie Folgendes ein:
  `/opt/sophos-av/bin/savconfig set UINotifier disabled`

11.2.2 Angeben einer benutzerdefinierten Meldung

Sie können eine benutzerdefinierte Meldung festlegen, die zu allen Befehlszeilenbenachrichtigungen und Popup-Benachrichtigungen auf dem Desktop hinzugefügt wird.

👉 **Merke!:** Die Hauptnachricht wird in verschiedenen Sprachen angezeigt (je nach Systemeinstellungen), aber der angepasste Text bleibt in der Sprache, die Sie bei dessen Festlegung verwendet haben.

- Sie können die Meldung über den Parameter **UIContactMessage** angeben. Beispiel:
  `/opt/sophos-av/bin/savconfig set UIContactMessage 'Contact IT'`

11.3 Konfigurieren von E-Mail-Benachrichtigungen

11.3.1 Deaktivieren von E-Mail-Benachrichtigungen

Standardmäßig sind E-Mail-Benachrichtigungen aktiviert.

- Geben Sie zum Deaktivieren der Benachrichtigungen folgenden Befehl ein:
  `/opt/sophos-av/bin/savconfig set EmailNotifier disabled`

11.3.2 Angabe von SMTP-Server-Hostnamen oder IP-Adresse

Standardmäßig lauten Hostname und Port des SMTP-Servers „localhost:25“.

- Über den Parameter **EmailServer** geben Sie den Hostnamen bzw. die IP-Adresse des SMTP-Servers ein. Beispiel:
  `/opt/sophos-av/bin/savconfig set EmailServer 171.17.31.184`

11.3.3 Sprachauswahl

Standardmäßig werden Alarme auf Englisch ausgegeben.

- Über den Parameter **EmailLanguage** geben Sie die Sprache an, in der der Text des Alarms verfasst werden soll. Zurzeit können Sie zwischen den Werten „**English**“ und „**Japanese**“ auswählen. Beispiel:
  /opt/sophos-av/bin/savconfig set EmailLanguage Japanese

  Hinweis: Die Sprachauswahl bezieht sich nur auf den Alert selbst, nicht die benutzerdefinierte Nachricht, die an den Alert angehängt wird.

11.3.4 Angeben der E-Mail-Empfänger

Standardmäßig werden E-Mail-Benachrichtigungen an „root@localhost“ gesendet.

- Über den Parameter **Email** und den Vorgang **add** können Sie Adressen in die E-Mail-Empfängerliste aufnehmen. Beispiel:
  /opt/sophos-av/bin/savconfig add Email admin@localhost

  Hinweis: Sie können mehrere Empfänger hintereinander in die Befehlszeile eingeben. Mehrere Empfänger trennen Sie durch ein Leerzeichen voneinander ab.

- Über den Parameter **Email** und den Vorgang **remove** können Sie eine Adresse aus der Liste entfernen. Beispiel:
  /opt/sophos-av/bin/savconfig remove Email admin@localhost

  Wichtig: Sie können **root@localhost** nicht mit diesem Befehl entfernen. Hierzu müssen Sie die Liste vollständig mit folgendem Befehl überschreiben:
  /opt/sophos-av/bin/savconfig set Email <email addresses>

11.3.5 Festlegen der E-Mail-Absenderadresse

Standardmäßig werden E-Mail-Benachrichtigungen von „root@localhost“ gesendet.

- Die E-Mail-Absenderadresse geben Sie über den Parameter **EmailSender** an. Beispiel:
  /opt/sophos-av/bin/savconfig set EmailSender admin@localhost

11.3.6 Festlegen der E-Mail-Antwortadresse

- Die E-Mail-Antwortadresse geben Sie über den Parameter **EmailReplyTo** an. Beispiel:
  /opt/sophos-av/bin/savconfig set EmailReplyTo admin@localhost

11.3.7 Was passiert, wenn ein Virus von der On-Access-Überprüfung erkannt wird?

Standardmäßig gibt Sophos Anti-Virus eine E-Mail-Benachrichtigung aus, wenn bei der On-Access-Überprüfung Viren erkannt. Neben dem eigentlichen Benachrichtigungstext enthalten die Nachrichten eine anpassbare Meldung in englischer Sprache.Sie können den Wortlaut dieser Meldung ändern. Eine Übersetzung erfolgt jedoch nicht.

- Geben Sie zum Deaktivieren von E-Mail-Benachrichtigungen bei von der On-Access-Überprüfung erkannten Viren Folgendes ein:

```
/opt/sophos-av/bin/savconfig set SendThreatEmail disabled
```

- Sie können die Meldung über den Parameter **ThreatMessage** anpassen. Beispiel:
  `/opt/sophos-av/bin/savconfig set ThreatMessage 'Contact IT'`

11.3.8 Festlegen der Vorgehensweise bei On-Access-Überprüfungs-Fehlern

Standardmäßig versendet Sophos Anti-Virus E-Mail-Benachrichtigungen zu On-Access-Überprüfungs-Fehlern. Neben dem eigentlichen Benachrichtigungstext enthalten die Nachrichten eine anpassbare Meldung in englischer Sprache.Sie können den Wortlaut dieser Meldung ändern. Eine Übersetzung erfolgt jedoch nicht.

- Geben Sie zum Deaktivieren von E-Mail-Benachrichtigungen bei Fehlern der On-Access-Überprüfung Folgendes ein:

  ```
  /opt/sophos-av/bin/savconfig set SendErrorEmail disabled
  ```

- Sie können die Meldung über den Parameter **ScanErrorMessage** angeben. Beispiel:
  `/opt/sophos-av/bin/savconfig set ScanErrorMessage 'Contact IT'`

11.3.9 Deaktivieren von E-Mail-Benachrichtigungen

Standardmäßig versendet Sophos Anti-Virus nur dann eine Zusammenfassung zu On-Demand-Überprüfungen, wenn Viren erkannt werden.

- Wenn Sie solche E-Mails nicht erhalten möchten, geben Sie Folgendes ein:
  `/opt/sophos-av/bin/savconfig set EmailDemandSummaryIfThreat disabled`

11.3.10 Ändern der Protokollmeldung

Standardmäßig sendet Sophos Anti-Virus eine E-Mail-Benachrichtigung mit einer voreingestellten Protokollmeldung, wenn im Sophos Anti-Virus-Protokoll ein Ereignis festgehalten wird. Neben dem eigentlichen Alarmtext umfassen Alarme umfassen eine anpassbare Meldung in englischer Sprache. Sie können den Wortlaut der Meldung ändern. Eine Übersetzung erfolgt jedoch nicht.

- Sie können die Meldung über den Parameter **LogMessage** angeben. Beispiel:
  `/opt/sophos-av/bin/savconfig set LogMessage 'Contact IT'`

12 Konfigurieren der Protokollierung

Hinweis: Wenn Sie einen einzigen Computer im Netzwerk konfigurieren, könnte die Konfiguration beim Download einer neuen Konfiguration (über Enterprise Console oder Konfiguration mit Extradateien) auf diesem Computer überschrieben werden.

Standardmäßig werden die Überprüfungsvorgänge im Sophos Anti-Virus-Protokoll festgehalten: `/opt/sophos-av/log/savd.log`. Wenn ein Protokoll auf 1 MB anwächst, werden im gleichen Verzeichnis automatisch eine Sicherungskopie und ein neues Protokoll wird angelegt.

- Wenn Sie wissen möchten, wie viele Protokolle standardmäßig angelegt werden können, geben Sie ein:
  `/opt/sophos-av/bin/savconfig -s query LogMaxSizeMB`

- Über den Parameter **LogMaxSizeMB** legen Sie die maximale Anzahl an Protokollen fest. Wenn die Höchstanzahl der Protokolle etwa 50 betragen soll, geben Sie Folgendes ein:
  `/opt/sophos-av/bin/savconfig set LogMaxSizeMB 50`

13 Konfigurieren der Updates

Wichtig: Wenn Sie Sophos Anti-Virus mit Sophos Enterprise Console verwalten, müssen Sie Updates mit Enterprise Console konfigurieren. In der Hilfe zu Enterprise Console finden Sie nähere Anweisungen hierzu.

13.1 Grundbegriffe

Update-Server

Unter *Update-Server* ist ein Computer mit Sophos Anti-Virus für Linux zu verstehen, der anderen Computern als Update-Quelle dient. Die anderen Computer können entweder Update-Server oder Update-Clients sein. Dies richtet sich danach, auf welche Weise Sophos Anti-Virus im Netzwerk eingesetzt wird.

Update-Client

Unter *Update*-Client ist ein Computer mit Sophos Anti-Virus zu verstehen, der anderen Computern nicht als Update-Quelle dient.

Primäre Update-Quelle

Bei der *primären Update-Quelle* handelt es sich um den Pfad, über den Computer gewöhnlich ihre Updates beziehen. Zum Zugriff auf diesen Pfad sind u.U. Zugangsdaten erforderlich.

Sekundäre Update-Quelle

Bei der *sekundären Update-Quelle* handelt es sich um den Pfad, über den Computer ihre Updates beziehen, wenn die primäre Update-Quelle nicht verfügbar ist. Zum Zugriff auf diesen Pfad sind u.U. Zugangsdaten erforderlich.

13.2 Konfiguration mit „savsetup“

Mit dem Befehl **`savsetup`** können Sie Updates konfigurieren. Sie sollten ihn nur für die im Folgenden ausgeführten Aufgaben verwenden.

Im Vergleich zur Konfiguration mit **`savconfig`** erhalten Sie nur Zugriff auf einige Parameter, doch der Umgang mit diesem Befehl ist einfacher. Sie werden zur Eingabe von Parameterwerten aufgefordert. Sie brauchen die Werte also nur einzugeben oder auszuwählen. Durch folgende Eingabe starten Sie **`savsetup`**:

```
/opt/sophos-av/bin/savsetup
```

13.3 Anzeigen der Auto-Update-Konfiguration auf einem Computer

1. Geben Sie folgenden Befehl auf dem Computer ein, den Sie überprüfen möchten:
   `/opt/sophos-av/bin/savsetup`

   Nun fordert **„`savsetup`“** Sie zur Auswahl einer Aktion auf.

2. Wählen Sie **Auto-updating configuration**.

   Nun fordert **„`savsetup`“** Sie zur Auswahl einer Aktion auf.

3. Wählen Sie **Display update configuration**, um die aktuelle Konfiguration anzuzeigen.

13.4 Konfigurieren eines Update-Servers

Sie können jede beliebige Standalone Sophos Anti-Virus für Liux-Installation als Update-Server für andere Netzwerkcomputer verwenden.

1. Geben Sie am Update-Server Folgendes ein:
   `/opt/sophos-av/bin/savsetup`

   Nun fordert **„`savsetup`“** Sie zur Auswahl einer Aktion auf.

2. Wählen Sie eine Option aus und befolgen Sie die Anweisungen auf dem Bildschirm zu Konfiguration des Update-Servers.

   Wenn Sie Updates von Sophos beziehen, geben Sie bei der Konfiguration von Updates die Zugangsdaten aus Ihrer Lizenz ein. Wenn Sie Updates von einem Update-Server beziehen, können Sie entweder eine HTTP-Adresse oder einen UNC-Pfad angeben, je nachdem, wie Sie den Update-Server eingerichtet haben.

3. Verfahren Sie zum Hosten von Updates für andere Sophos Anti-Virus Clients wie folgt:

   a) Konfigurieren Sie den Update-Server so, dass die zusätzlichen Dateien, die eventuell zur Aktualisierung der Clients benötigt werden, heruntergeladen werden. Geben Sie am Update-Server Folgendes ein:
   `/opt/sophos-av/bin/savconfig set PrimaryUpdateAllDistros true`

   b) Zwingen Sie den Update-Server zur Aktualisierung, um sicherzustellen, dass die zusätzlichen Dateien heruntergeladen werden. Geben Sie am Update-Server Folgendes ein:
   `/opt/sophos-av/bin/savupdate --force`

   c) Kopieren Sie das lokale Cache-Verzeichnis (/opt/sophos-av/update/cache/) in ein anderes Verzeichnis im Dateisystem.

   Dieser Vorgang lässt sich mit einem Skript automatisieren.

   d) Veröffentlichen Sie das Verzeichnis für andere Computer im Netzwerk per HTTP, SMB, NFS oder eine andere Methode.

   Bei dem Verzeichnis handelt es sich um das zentrale Installationsverzeichnis (CID), von dem die Clients Updates herunterladen.

13.5 Konfigurieren von Updates für mehrere Clients

In diesem Abschnitt wird die Aktualisierung der Update-Parameter in der Konfiguration mit Extradateien erläutert. Die Konfiguration wird beim nächsten Update von den Update-Clients heruntergeladen.

In diesem Abschnitt wird davon ausgegangen, dass Sie bereits eine Konfiguration mit Extradateien erstellt haben. Wenn die Konfiguration nicht erstellt wurde, finden Sie nähere Anweisungen im Anhang: Konfiguration mit Extradateien (Seite 41).

Hinweis: In diesem Abschnitt wird beschrieben, wie Sie mehrere Update-Clients so konfigurieren können, dass sie von der *primären* Update-Quelle Updates beziehen. Mit diesem Verfahren können Sie auch die *sekundäre* Update-Quelle konfigurieren, indem Sie *Primary* durch *Secondary* ersetzen. Beispiel: **PrimaryUpdateSourcePath** anstelle von **SecondaryUpdateSourcePath**.

So konfigurieren Sie Updates für mehrere Clients:

1. Legen Sie auf dem Computer, auf dem die Konfiguration mit Extradateien gespeichert wurde, als Adresse der Update-Quelle entweder **`sophos:`** oder das Verzeichnis des zentralen Installationsverzeichnisses (CID) fest. Verwenden Sie hierzu den Parameter **PrimaryUpdateSourcePath**.

   Um Updates vom CID zu beziehen, können Sie entweder eine HTTP-Adresse oder einen UNC-Pfad angeben, je nachdem, wie Sie den Update-Server eingerichtet haben. Beispiel:

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path -c set
   PrimaryUpdateSourcePath 'http://www.mywebcid.com/cid'
   ```

   Geben Sie Folgendes ein, um Updates von **`sophos:`** zu beziehen:

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path -c set
   PrimaryUpdateSourcePath 'sophos:'
   ```

2. Falls für den Zugriff auf die Update-Quelle eine Anmeldung erforderlich ist, legen Sie über die Parameter **PrimaryUpdateUsername** und **PrimaryUpdatePassword** jeweils einen Benutzernamen und ein Kennwort fest. Beispiel:

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path -c set
   PrimaryUpdateUsername 'fred'
   ```

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path -c set
   PrimaryUpdatePassword 'j23rjjfwj'
   ```

3. Wenn Sie die Verbindung zur Update-Quelle über einen Proxyserver herstellen, legen Sie über die Parameter **PrimaryUpdateProxyAddress**, **PrimaryUpdateProxyUsername** und **PrimaryUpdateProxyPassword** jeweils die Adresse, den Benutzernamen und das Kennwort fest. Beispiel:

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path -c set
   PrimaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'
   ```

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path-c set
   PrimaryUpdateProxyUsername 'penelope'
   ```

   ```
   /opt/sophos-av/bin/savconfig -f offline-config-file-path -c set
   PrimaryUpdateProxyPassword 'fj202jrjf'
   ```

4. Wenn Sie Parameter in der Offline-Konfigurationsdatei festgelegt haben, aktualisieren Sie die Live-Konfigurationsdatei über den Befehl **addextra**. Es gilt folgende Syntax:

   /opt/sophos-av/update/addextra
   offline-config-file-pathlive-config-file-path
   --signing-key=*signing-key-file-path*
   --signing-certificate=*signing-certificate-file-path*

   Beispiel:

   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /var/www/extrafiles/ --signing-key= /root/certificates/extrafiles-signing.key --signing-certificate=/root/certificates/extrafiles-signing.crt

Die neue Konfiguration steht den Update-Clients beim nächsten Update zum Download bereit.

13.6 Konfigurieren von Updates von Sophos für einen Client

1. Geben Sie folgenden Befehl auf dem Computer ein, den Sie konfigurieren möchten: **/opt/sophos-av/bin/savsetup**

   Nun fordert **„savsetup“** Sie zur Auswahl einer Aktion auf.

2. Wählen Sie eine Option aus und befolgen Sie die Anweisungen auf dem Bildschirm zu Konfiguration des Update-Clients.

   Wenn Sie Updates von Sophos beziehen, geben Sie bei der Konfiguration von Updates die Zugangsdaten aus Ihrer Lizenz ein. Wenn Sie Updates von einem CID beziehen, können Sie entweder eine HTTP-Adresse oder einen UNC-Pfad angeben, je nachdem, wie Sie den Update-Server eingerichtet haben.

14 Konfigurieren von Sophos Live-Schutz

Hinweis: Wenn Sie einen einzigen Computer im Netzwerk konfigurieren, könnte die Konfiguration beim Download einer neuen Konfiguration (über Enterprise Console oder Konfiguration mit Extradateien) auf diesem Computer überschrieben werden.

Sophos Live-Schutz stellt fest, ob eine verdächtige Datei einen Threat darstellt. Handelt es sich um einen Threat, werden umgehend die in der Bereinigungskonfiguration von Sophos Anti-Virus festgelegten Maßnahmen ergriffen.

Die Malware-Erkennung wird durch den Live-Schutz erheblich verbessert, und es kommt nicht zu unerwünschten Erkennungen. Das Verfahren basiert auf einem Sofortabgleich mit aktueller Malware. Wenn neue Malware erkannt wird, kann Sophos binnen Sekunden Updates bereitstellen.

Wenn eine Datei von einem Antiviren-Scan auf einem Endpoint als verdächtig eingestuft wurde, anhand der Threatkennungsdateien (IDEs) auf dem Computer jedoch nicht festgestellt kann, ob die Datei virenfrei ist, werden bestimmte Dateidaten (z.B. die Prüfsumme der Datei und weitere Attribute) zur weiteren Analyse an Sophos übermittelt.

Bei der „In-the-Cloud“-Prüfung wird durch Abgleich mit der Datenbank der SophosLabs festgestellt, ob es sich um eine verdächtige Datei handelt. Die Datei wird als virenfrei oder von Malware betroffen eingestuft. Das Ergebnis der Prüfung wird an den Computer übertragen, und der Status der Datei wird automatisch aktualisiert.

14.1 Überprüfen der Einstellungen des Sophos Live-Schutz

Bei der Erstinstallation von Sophos Anti-Virus ist der Live-Schutz von Sophos standardmäßig aktiviert. Bei einem Upgrade von einer älteren Version von Sophos Anti-Virus ist die Option deaktiviert.

- Geben Sie zum Überprüfen der Live-Schutz-Einstellung Folgendes ein:
  `/opt/sophos-av/bin/savconfig query LiveProtection`

14.2 Aktivieren/Deaktivieren von Sophos Live-Schutz

- Geben Sie zum Deaktivieren von Sophos Live-Schutz Folgendes ein:

  `/opt/sophos-av/bin/savconfig set LiveProtection true`

- Geben Sie zum Aktivieren von Sophos Live-Schutz Folgendes ein:

  `/opt/sophos-av/bin/savconfig set LiveProtection false`

15 Konfigurieren von On-Access-Scans

Hinweis: Wenn Sie einen einzigen Computer im Netzwerk konfigurieren, könnte die Konfiguration beim Download einer neuen Konfiguration (über Enterprise Console oder Konfiguration mit Extradateien) auf diesem Computer überschrieben werden.

15.1 Ändern der Interception-Methode zur On-Access-Überprüfung

Wenn Sie ein Upgrade auf eine Version des Linuxkernels durchführen, bei der Talpa nicht unterstützt wird, können Sie Fanotify als Interception-Methode zur On-Access-Überprüfung verwenden.

Wichtig: Die Verwendung von Fanotify in Sophos Anti-Virus befindet sich noch in der Betaphase und wird nicht vollständig unterstützt.

- Geben Sie zum Festlegen von Fanotify als Interception-Methode zur On-Access-Überprüfung Folgendes ein.
  `/opt/sophos-av/bin/savconfig set DisableFanotify false`

15.2 Ausschließen von Dateien und Verzeichnissen von der Überprüfung

Sie können Dateien und Verzeichnisse auf verschiedene Weise von der Überprüfung ausschließen:

- über Datei- oder Verzeichnisnamen
- über Platzhalter

Wenn Sie Dateien und Verzeichnisse ausschließen möchten, deren Namen nicht mit UTF-8 verschlüsselt sind, finden Sie im Abschnitt Festlegen der Zeichenverschlüsselung von Verzeichnisnamen und Dateinamen (Seite 38) nähere Anweisungen.

15.2.1 Über Datei- oder Verzeichnisnamen

Hinweis: Wenn Sie einen einzigen Computer im Netzwerk konfigurieren, könnte die Konfiguration beim Download einer neuen Konfiguration (über Enterprise Console oder Konfiguration mit Extradateien) auf diesem Computer überschrieben werden.

- Über den Parameter **ExcludeFilePaths** und den Vorgang **add** können Sie eine bestimmte Datei oder ein bestimmtes Verzeichnis ausschließen. Setzen Sie ans Ende eines Verzeichnisses einen Schrägstrich. Wenn Sie beispielsweise die Datei `/tmp/report` in die Liste mit den auszuschließenden Dateien und Verzeichnissen aufnehmen möchten, geben Sie Folgendes ein:
  `/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/report`

  Wenn Sie das Verzeichnis `/tmp/report/` in die Liste mit den auszuschließenden Dateien und Verzeichnissen aufnehmen möchten, geben Sie Folgendes ein:

  `/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/report/`

- Über den Parameter **ExcludeFilePaths** und den Vorgang **remove** können Sie den Ausschluss aus der Liste entfernen. Beispiel:

  ```
  /opt/sophos-av/bin/savconfig remove ExcludeFilePaths /tmp/report
  ```

15.2.2 Platzhalter

Hinweis: Wenn Sie einen einzigen Computer im Netzwerk konfigurieren, könnte die Konfiguration beim Download einer neuen Konfiguration (über Enterprise Console oder Konfiguration mit Extradateien) auf diesem Computer überschrieben werden.

- Über den Parameter **ExcludeFileOnGlob** und den Vorgang **add** können Sie Dateien oder ein Verzeichnisse mit Platzhaltern ausschließen. Sie können die Platzhalter ***** (entspricht einer beliebigen Anzahl an beliebigen Zeichen) und **?** (entspricht einem beliebigen Zeichen) verwenden. Wenn Sie beispielsweise alle Textdateien im Verzeichnis `/tmp` in die Liste mit den auszuschließenden Dateien und Verzeichnissen aufnehmen möchten, geben Sie Folgendes ein:
  ```
  /opt/sophos-av/bin/savconfig add ExcludeFileOnGlob '/tmp/*.txt'
  ```

  Hinweis: Wenn Sie **ExcludeFileOnGlob** verwenden, um **ein Verzeichnis** auszuschließen, müssen Sie am Ende des Pfads den Platzhalter * hinzufügen. Beispiel:

  ```
  /opt/sophos-av/bin/savconfig add ExcludeFileOnGlob '/tmp/report/*'
  ```

- Wenn Sie den Ausdruck nicht mit Anführungszeichen schließen, erweitert Linux den Ausdruck und überträgt die Dateiliste an Sophos Anti-Virus. Dies ist zum Ausschließen bereits vorhandener Dateien hilfreich sowie zum Aktivieren der Überprüfung von Dateien, die später erstellt werden sollen. Wenn Sie beispielsweise alle Textdateien, die bereits im Verzeichnis `/tmp` vorhanden sind, in die Liste mit den auszuschließenden Dateien und Verzeichnissen aufnehmen möchten, geben Sie Folgendes ein:
  ```
  /opt/sophos-av/bin/savconfig add ExcludeFileOnGlob /tmp/*.txt
  ```

- Über den Parameter **ExcludeFileOnGlob** und den Vorgang **remove** können Sie den Ausschluss aus der Liste entfernen. Beispiel:
  ```
  /opt/sophos-av/bin/savconfig remove ExcludeFileOnGlob
  '/tmp/notes.txt'
  ```

15.2.3 Festlegen der Zeichenverschlüsselung von Verzeichnisnamen und Dateinamen

Mit Linux können Sie Verzeichnisse und Dateien mit beliebiger Zeichenverschlüsselung angeben (z.B. UTF-8, EUC_jp). Sophos Anti-Virus speichert Ausschlüsse jedoch nur in UTF-8. Wenn Sie also Verzeichnisse und Dateien von der Überprüfung ausschließen möchten, deren Namen nicht mit UTF-8 verschlüsselt sind, geben Sie die Ausschlüsse in UTF-8 und die Verschlüsselungen mit dem Parameter **ExclusionEncodings** an. So werden die Namen aller Verzeichnisse und Dateien, die Sie ausschließen, in allen angegebenen Verschlüsselungen getestet und alle übereinstimmenden Verzeichnisse und Dateien werden ausgeschlossen. Dies trifft für Ausschlüsse zu, die mit den Parametern **ExcludeFilePaths** und **ExcludeFileOnGlob** angegeben wurden. Standardmäßig werden UTF-8, EUC_jp und ISO-8859-1 (Latin-1) angegeben.

Wenn Sie beispielsweise Verzeichnisse und Dateien ausschließen wollen, deren Namen in EUC_cn verschlüsselt sind, geben Sie die Namen der Verzeichnisse und Dateien mit dem Parameter **ExcludeFilePaths** und/oder **ExcludeFileOnGlob** an. Fügen Sie „EUC_cn“ anschließend zur Verschlüsselungsliste hinzu:

`/opt/sophos-av/bin/savconfig add ExclusionEncodings EUC_cn`

Danach testet Sophos Anti-Virus alle Verzeichnisnamen und Dateinamen, die Sie angegeben haben, in „UTF-8“, „EUC_jp“, „ISO-8859-1 (Latin-1)“ und „EUC_cn“. Alle Verzeichnisse und Dateien, deren Namen übereinstimmen, werden ausgeschlossen.

15.3 Ausschließen von Dateisystemtypen von der Überprüfung

Standardmäßig werden alle Dateisystemtypen überprüft.

- Über den Parameter **ExcludeFilesystems** und den Vorgang **add** können Sie einen Dateisystemtyp ausschließen. Gültige Dateisystemtypen werden in der Datei **/proc/filesystems** aufgelistet. Wenn Sie beispielsweise „nfs“ in die Liste mit den Dateisystemtypen aufnehmen möchten, geben Sie Folgendes ein:
  `/opt/sophos-av/bin/savconfig add ExcludeFilesystems nfs`

- Über den Parameter **ExcludeFilesystems** und den Vorgang **remove** können Sie den Ausschluss aus der Liste entfernen. Beispiel:
  `/opt/sophos-av/bin/savconfig remove ExcludeFilesystems nfs`

15.4 Überprüfen von Archivdateien

Die On-Access-Überprüfung von Archivdateien ist standardmäßig deaktiviert. Wenn Sie jedoch mehrere Dateien gleichzeitig bearbeiten, ist die Gefahr, dass ein Virus nicht erkannt wird, groß. Dann bietet sich an, die Option zu aktivieren. Dies kann etwa der Fall sein, wenn Sie Archive an einen wichtigen Kunden schicken.

Hinweis: Aus folgenden Gründen empfiehlt sich die Auswahl dieser Option nicht:

- Die Überprüfung von in Archivdateien ist äußerst zeitaufwändig.
- Auch wenn diese Option nicht aktiviert ist, wird eine aus einem Archiv extrahierte Datei beim Öffnen überprüft.

Hinweis: Die Threat Detection Engine überprüft nur archivierte Dateien bis 8 GB (in dekomprimierter Form). Das liegt daran, dass die Engine das POSIX ustar-Archivformat unterstützt, das keine größeren Dateien verarbeiten kann.

- Geben Sie zum *Aktivieren* der Überprüfung von Archivdateien folgenden Befehl ein:
  `/opt/sophos-av/bin/savconfig set ScanArchives enabled`

- Geben Sie zum *Deaktivieren* der Überprüfung von Archivdateien folgenden Befehl ein:
  `/opt/sophos-av/bin/savconfig set ScanArchives disabled`

15.5 Bereinigen infizierter Dateien

Sie können infizierte Dateien bei einer On-Access-Überprüfung bereinigen (desinfizieren oder löschen). Standardmäßig ist die Bereinigung deaktiviert.

Alle von Sophos Anti-Virus gegen infizierte Dateien ergriffenen Maßnahmen werden im Sophos Anti-Virus-Protokoll aufgezeichnet.

Hinweis: Sie können sowohl Desinfektion als auch Löschen aktivieren; wir raten jedoch davon ab. Bei Wahl dieser Einstellungen versucht Sophos Anti-Virus zunächst, die Datei zu desinfizieren. Schlägt die Desinfektion fehl, wird die Datei gelöscht.

Hinweis: Sophos Anti-Virus kann Dateien desinfizieren oder löschen, wenn die Überprüfung „beim Öffnen“ (d. h. wenn Dateien kopiert, verschoben oder geöffnet werden) erfolgt. Bei einer Überprüfung „beim Schließen“ (d. h. wenn Dateien gespeichert oder erstellt werden) ist dies nicht möglich. Bei normaler Nutzung stellt dies kein Problem dar, weil eine Überprüfung „beim Öffnen“ auf Linux-Computern nicht zentral deaktiviert werden kann und Dateien beim nächsten Zugriff desinfiziert oder gelöscht werden.

15.5.1 Desinfektion infizierter Dateien und Bootsektoren

- Geben Sie zum *Deaktivieren* der Desinfektion infizierter Dateien bei Zugriff Folgendes ein:
  `/opt/sophos-av/bin/savconfig add AutomaticAction disinfect`

  Wichtig: Sie müssen Ihre Eingabe nicht bestätigen, bevor Sophos Anti-Virus die Datei desinfiziert.

  Hinweis: Durch die Desinfizierung von infizierten Dokumenten werden keine von dem Virus vorgenommenen Änderungen rückgängig gemacht. Unter Bereinigungs-Details (Seite 16) erfahren Sie, wie Sie sich auf der Sophos Website über die Folgeerscheinungen eines bestimmten Virus informieren.

- Geben Sie zum *Deaktivieren* der Desinfektion infizierter Dateien und Bootsektoren Folgendes ein:
  `/opt/sophos-av/bin/savconfig remove AutomaticAction disinfect`

15.5.2 Löschen infizierter Dateien

Wichtig: Diese Option sollten Sie nur nach Rücksprache mit dem technischen Support von Sophos verwenden. Wenn sich eine infizierte Datei im Posteingang befinden, löscht Sophos Anti-Virus unter Umständen den gesamten Posteingang.

- Geben Sie zum *Aktivieren* des Löschens infizierter Dateien bei Zugriff Folgendes ein:
  `/opt/sophos-av/bin/savconfig add AutomaticAction delete`

  Wichtig: Sie müssen Ihre Eingabe nicht bestätigen, bevor Sophos Anti-Virus die Datei löscht.

- Geben Sie zum *Deaktivieren* des Löschens infizierter Dateien bei Zugriff Folgendes ein:
  `/opt/sophos-av/bin/savconfig remove AutomaticAction delete`

16 Konfiguration mit Extradateien

In diesem Abschnitt wird beschrieben, wie Sie Sophos Anti-Virus mit der Methode „Konfiguration mit Extradateien“ konfigurieren.

16.1 Die Konfiguration mit Extradateien

Dieser Abschnitt enthält einen Überblick über die Konfiguration mit Extradateien.

16.1.1 Was bedeutet Konfiguration mit Extradateien?

Die Konfiguration mit Extradateien ist eine Methode, um Sophos Anti-Virus für Linux zu konfigurieren, und stellt eine Alternative zur Konfiguration über Sophos Enterprise Console dar, bei der kein Windows-Computer erforderlich ist.

Sie sollten diese Methode nur anwenden, wenn Sie Enterprise Console nicht verwenden können.

Hinweis: Die Konfiguration von Enterprise Console lässt sich nicht mit der Konfiguration mit Extradateien kombinieren.

Mit dieser Methode können Sie sämtliche Funktionen von Sophos Anti-Virus mit Ausnahme der On-Demand-Überprüfung (Anweisungen zu letzterer entnehmen Sie bitte dem Abschnitt Konfigurieren von On-Demand-Überprüfungen (Seite 11)) konfigurieren.

16.1.2 Wie verwendet man die Konfiguration mit Extradateien?

Sie erstellen eine Datei, die die Einstellungen für die Konfiguration mit Extradateien enthält. Diese Datei ist offline, so dass andere Computer nicht darauf zugreifen können.

Sobald Sie Ihre Computer konfigurieren möchten, kopieren Sie die Offline-Datei in eine Live-Konfigurationsdatei, die an einem Ort gespeichert ist, auf die Endpoint-Computer zugreifen können. Sie können alle Endpoint-Computer so konfigurieren, dass sie ihre Konfiguration von der Live-Konfigurationsdatei abrufen, wenn der betreffende Computer ein Update durchführt.

Um Endpoint-Computer neu zu konfigurieren, aktualisieren Sie die Offline-Konfigurationsdatei und kopieren sie erneut in die Live-Konfigurationsdatei.

Hinweise:

- Um sicherzustellen, dass die Konfigurationsdatei sicher ist, müssen Sie Sicherheitszertifikate erstellen und verwenden, wie in den folgenden Abschnitten beschrieben.
- Sie können Teile der bzw. die gesamte Konfiguration sperren, damit einzelne Benutzer sie auf ihrem Computer nicht ändern können.

In den folgenden Abschnitten erfahren Sie, wie Sie Dateien für die Konfiguration mit Extradateien erstellen und verwenden.

16.2 Verwenden der Konfiguration mit Extradateien

Für die Verwendung von Extradateien gehen Sie wie folgt vor:

- Erstellen Sie Sicherheitszertifikate auf dem Server.
- Erstellen Sie eine Konfiguration mit Extradateien.
- Installieren Sie das Stammzertifikat auf den Endpoint-Computern.
- Richten Sie die Endpoint-Computer so ein, dass die Konfiguration mit Extradateien verwendet wird.

16.2.1 Erstellen von Sicherheitszertifikaten auf dem Server

So erstellen Sie die Sicherheitszertifikate:

Hinweis: Wenn Sie OpenSSL verwenden, um Zertifikate zu erstellen, müssen Sie OpenSSL 0.9.8 oder höher ausführen.

1. Holen Sie das Skript, das Sie zum Erstellen der Zertifikate verwenden möchten. Das Skript finden Sie im Sophos Support-Artikel 119602.
2. Führen Sie das Skript zum Erstellen der Zertifikate aus. Beispiel:

   ```
   ./create_certificates.sh /root/certificates
   ```

   Sie können ein anderes Verzeichnis angeben, in dem die Zertifikate abgelegt werden. Sie müssen jedoch sicherstellen, dass die Zertifikate an einem sicheren Ort gespeichert werden.
3. Wenn Sie dazu aufgefordert werden, geben Sie das Root-Schlüssel-Kennwort ein.
4. Wenn Sie dazu aufgefordert werden, geben Sie das Signaturschlüssel-Kennwort ein.
5. Stellen Sie sicher, dass sich die Zertifikate in dem Verzeichnis befinden. Geben Sie Folgendes ein:

   ```
   ls /root/certificates/
   ```

   Sie sollten folgende Dateien sehen:

   ```
   extrafiles-root-ca.crt extrafiles-root-ca.key extrafiles-signing.cnf
   extrafiles-signing.crt extrafiles-signing.key
   ```

16.2.2 Erstellen einer Konfiguration mit Extradateien

1. Führen Sie auf dem Computer, auf dem die Konfiguration mit Extradateien speichern möchten, den Befehl **savconfig** aus, um die Offline-Konfigurationsdatei zu erstellen und die Parameterwerte der Datei festzulegen.

   Es gilt folgende Syntax:

   /opt/sophos-av/bin/savconfig -f *offline-config-file-path* **-c** *operation parameter value*

   Hierbei gilt:

   - -f *offline-config-file-path* legt den Pfad der Offline-Konfigurationsdatei einschließlich Dateiname fest. Die Datei wird von **savconfig** erstellt.
   - **-c** kündigt an, dass auf die Corporate-Ebene der Offline-Datei zugegriffen werden soll. (Näheres über Ebenen erfahren Sie im Abschnitt Konfigurationsebenen (Seite 45).)
   - *Vorgang*: entweder **set** (setzen), **update** (aktualisieren), **add** (hinzufügen), **remove** (entfernen) oder **delete** (löschen).
   - *Parameter* ist der Parameter, der geändert werden soll.
   - *Wert* ist der Wert, den der Parameter erhalten soll.

   Durch den folgenden Befehl wird beispielsweise im Verzeichnis `/rootconfig/` eine Datei namens „`OfflineConfig.cfg`“ angelegt und E-Mail-Benachrichtigungen werden deaktiviert:

   /opt/sophos-av/bin/savconfig -f /root/config/OfflineConfig.cfg -c set EmailNotifier Disabled

   Weitere Informationen zu **savconfig** entnehmen Sie bitte dem Abschnitt Konfiguration mit „savconfig“ (Seite 46).

2. Zum Anzeigen der Parameterwerte geben Sie als Vorgang **query** an. Es lassen sich sowohl der Wert eines einzelnen Parameters als auch die Werte aller Parameter anzeigen. Um z.B. die Werte aller festgelegten Parameter anzuzeigen, geben Sie Folgendes ein: **/opt/sophos-av/bin/savconfig -f /root/config/OfflineConfig.cfg -c query**

3. Wenn Sie alle Parameter in der Offline-Konfigurationsdatei festgelegt haben, erstellen Sie eine Web-Freigabe oder eine Freigabe zum Speichern der Live-Konfigurationsdatei.
4. Erstellen Sie die Live-Konfigurationsdatei über den Befehl **addextra**. Es gilt folgende Syntax:

   /opt/sophos-av/update/addextra
   offline-config-file-pathlive-config-file-path
   --signing-key=*signing-key-file-path*
   --signing-certificate=*signing-certificate-file-path*

   Beispiel:

   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /var/www/extrafiles/ --signing-key= /root/certificates/extrafiles-signing.key --signing-certificate=/root/certificates/extrafiles-signing.crt

16.2.3 Installation des Stammzertifikats auf Endpoint-Computern

Sie müssen das Stammzertifikat auf allen Endpoint-Computern installieren.

1. Erstellen Sie auf dem Computer, auf dem Sie die Zertifikate erstellt haben (oder auf dem Computer, auf den Sie diese kopiert haben), ein neues Verzeichnis für das Stammzertifikat. Geben Sie Folgendes ein:

   ```
   mkdir rootcert
   cd rootcert/
   ```

2. Kopieren Sie das Stammzertifikat in das neue Verzeichnis. Geben Sie Folgendes ein:

   ```
   cp /root/certificates/extrafiles-root-ca.crt .
   ```

3. Kopieren Sie das neue Verzeichnis in eine Freigabe.
4. Mounten Sie auf allen Endpoint-Computern die Freigabe.
5. Installieren Sie das Zertifikat. Es gilt folgende Syntax:

   /opt/sophos-av/update/addextra_certs --install= *shared-rootcert-directory*

   Beispiel:

   ```
   /opt/sophos-av/update/addextra_certs --install=
   shared-rootcert-directory
   ```

16.2.4 Endpoint-Computer so einrichten, dass die Konfiguration mit Extradateien verwendet wird

Um die Endpoint-Computer so einzurichten, dass sie die Konfiguration herunterladen und verwenden, gehen Sie wie folgt vor:

1. Wenn sich die Live-Konfigurationsdatei in einer Freigabe befindet, mounten Sie das Verzeichnis auf allen Clients.
2. Geben Sie auf allen Endpoint-Computern den Pfad der Live-Konfigurationsdatei an. Beispiel:

   ```
   /opt/sophos-av/bin/savconfig set ExtraFilesSourcePath
   http://www.example.com/extrafiles
   ```

   Die neue Konfiguration steht Computern beim nächsten Update zum Download bereit.

3. Um jetzt ein Update auszuführen, geben Sie Folgendes ein:

   ```
   /opt/sophos-av/bin/savupdate
   ```

16.3 Aktualisieren der Konfiguration mit Extradateien

1. Führen Sie auf dem Computer, auf dem die Konfiguration mit Extradateien gespeichert wurde, den Befehl **savconfig** aus, um die Offline-Konfigurationsdatei zu aktualisieren und die Parameterwerte der Datei festzulegen.

   Sie können die gleiche Syntax wie bei der Erstellung der Offline-Konfigurationsdatei verwenden.

   Durch den folgenden Befehl wird beispielsweise im Verzeichnis `/opt/sophos-av` eine Datei namens `OfflineConfig.cfg` aktualisiert und E-Mail-Benachrichtigungen werden aktiviert:

   ```
   /opt/sophos-av/bin/savconfig -f /opt/sophos-av/OfflineConfig.cfg
   -c set EmailNotifier Enabled
   ```

2. Zum Anzeigen der Parameterwerte geben Sie als Vorgang **query** an. Es lassen sich sowohl der Wert eines einzelnen Parameters als auch die Werte aller Parameter anzeigen. Um z.B. die Werte aller festgelegten Parameter anzuzeigen, geben Sie Folgendes ein:
   ```
   /opt/sophos-av/bin/savconfig -f /opt/sophos-av/OfflineConfig.cfg
   -c query
   ```

3. Wenn Sie Parameter in der Offline-Konfigurationsdatei festgelegt haben, aktualisieren Sie die Live-Konfigurationsdatei über den Befehl **addextra**. Es gilt folgende Syntax:

   ```
   /opt/sophos-av/update/addextra
   offline-config-file-pathlive-config-file-path
   --signing-key=signing-key-file-path
   --signing-certificate=signing-certificate-file-path
   ```

   Beispiel:

   ```
   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg
   /var/www/extrafiles/ --signing-key=
   /root/certificates/extrafiles-signing.key
   --signing-certificate=/root/certificates/extrafiles-signing.crt
   ```

   Die neue Konfiguration steht Computern beim nächsten Update zum Download bereit.

4. Um jetzt ein Update auszuführen, geben Sie Folgendes ein:

   ```
   /opt/sophos-av/bin/savupdate
   ```

16.4 Konfigurationsebenen

Mit jeder Installation von Sophos Anti-Virus wird eine lokale Konfigurationsdatei angelegt, die Einstellungen für alle Komponenten von Sophos Anti-Virus mit Ausnahme der On-Demand-Überprüfung enthält.

Eine lokale Konfigurationsdatei kann aus mehreren Ebenen aufgebaut sein:

- Sophos: Diese Ebene ist immer in der Datei vorhanden. In ihr sind werkseitige Voreinstellungen enthalten, die nur von Sophos geändert werden.
- Corporate: Diese Ebene ist vorhanden, wenn Sophos Anti-Virus über die Konfiguration mit Extradateien konfiguriert wird.
- User: Diese Ebene ist vorhanden, wenn Sophos Anti-Virus lokal konfiguriert wird. Sie enthält Einstellungen, die nur für Sophos Anti-Virus auf dem lokalen Computer gelten.

Jede Ebene enthält die gleichen Parameter. So lässt sich ein Parameter für mehrere Ebenen festlegen. Beim Abrufen eines Parameterwerts folgt Sophos Anti-Virus jedoch einer Hierarchie:

- Standardmäßig hat die Corporate-Ebene eine höhere Priorität als die User-Ebene.
- Die Corporate-Ebene und die User-Ebene haben Vorrang vor der Sophos-Ebene.

Wenn z.B. ein bestimmter Parameter sowohl in der User-Ebene als auch in der Corporate-Ebene gesetzt ist, gilt der Wert der Corporate-Ebene. Die Werte einzelner Parameter in der Corporate-Ebene lassen sich jedoch entsperren und so durch die jeweiligen Parameterwerte einer anderen Ebene überschreiben.

Beim Aktualisieren der lokalen Konfigurationsdatei über die Konfigurationsdatei mit Extradateien wird die Corporate-Ebene in der lokalen Datei durch die Konfigurationsdatei mit Extradateien ersetzt.

16.5 Konfiguration mit „savconfig“

Mit dem Befehl **`savconfig`** können Sie auf sämtliche Funktionen von Sophos Anti-Virus mit Ausnahme der On-Demand-Überprüfung zugreifen. Der Pfad zu diesem Programm bzw. Befehl lautet `/opt/sophos-av/bin`. Die Konfiguration bestimmter Funktionen von Sophos Anti-Virus anhand dieses Befehls wird nach und nach in diesem Handbuch erläutert. In diesem Unterabschnitt wird lediglich die Syntax erläutert.

Folgende Syntax gilt für den Befehl **`savconfig`**:

`savconfig [`*`Option`***`] ... `***`Vorgang`***`] [`***`Parameter`***`] [`***`Wert`***`] ...`**

Eine vollständige Liste der Optionen, Vorgänge und Parameter erhalten Sie durch Eingabe von:

```
man savconfig
```

16.5.1 *Option*

Sie können eine oder mehrere Optionen angeben. Die Optionen beziehen sich größtenteils auf die *Ebenen* in der lokalen Konfigurationsdatei einer Installation. Standardmäßig adressiert der Befehl die User-Ebene. Wenn die Corporate-Ebene adressiert werden soll, verwenden Sie die Option **-c** oder **--corporate**.

Normalerweise sind die Parameterwerte in der Corporate-Ebene gesperrt und deaktivieren somit die Werte in der User-Ebene. Wenn eine Corporate-Einstellung von Benutzern überschrieben werden soll, entsperren Sie sie über die Option **--nolock**. Um z.B. den Wert von **LogMaxSizeMB** festzulegen und ihn gleichzeitig zu entsperren, damit er überschrieben werden kann, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig --nolock -f corpconfig.cfg -c
LogMaxSizeMB 50
```

Wenn Sie Enterprise Console verwenden, können Sie sich über die Option **--consoleav** nur die Parameterwerte der Virenschutzrichtlinie anzeigen lassen. Geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig --consoleav query
```

Über die Option **--consoleupdate** rufen Sie die Werte der Update-Richtlinie von Enterprise Console ab. Geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig --consoleupdate query
```

16.5.2 *Vorgang*

Sie können einen Vorgang angeben. Die Vorgänge beziehen sich hauptsächlich auf Parameter. Einige Parameter können nur einen Wert besitzen, andere können eine ganze Liste von Werten aufweisen. Mit Vorgängen fügen Sie einer Liste Werte hinzu oder entfernen Werte aus einer Liste. Ein Beispiel: Der Parameter **Email** ist eine *Liste* von E-Mail-Empfängern.

Zum Anzeigen der Parameterwerte geben Sie als Vorgang **query** an. Um z.B. den Wert des Parameters **EmailNotifier** abzurufen, geben Sie Folgendes ein:

```
/opt/sophos-av/bin/savconfig query EmailNotifier
```

Wenn Sie Enterprise Console verwenden und **savconfig** Parameterwerte ausgibt, werden die Werte, die mit der entsprechenden Enterprise Console-Richtlinie in Konflikt stehen, eindeutig durch den Hinweis „Conflict“ gekennzeichnet.

16.5.3 *Parameter*

Sie können einen Parameter angeben. Durch folgende Eingabe werden alle modifizierbaren Grundparameter aufgelistet:

```
/opt/sophos-av/bin/savconfig -v
```

Für einige Parameter ist außerdem die Eingabe eines Zweitparameters erforderlich.

16.5.4 *value*

Sie können einen oder mehrere Werte angeben, die einem Parameter zugewiesen werden sollen. Sollte ein Wert Leerzeichen enthalten, muss der Wert in Apostrophe gesetzt werden.

17 Fehlersuche

Dieser Abschnitt enthält Tipps zur Fehlerbehebung in Zusammenhang mit Sophos Anti-Virus.

Nähere Informationen zu den von Sophos Anti-Virus bei der On-Demand-Überprüfung ausgegebenen Fehlercodes finden Sie unter Anhang: Fehlercodes der On-Demand-Überprüfung (Seite 54).

17.1 Befehl wird nicht ausgeführt

Symptom

Sie können keinen Sophos Anti-Virus-Befehl ausführen.

Ursache

Sie verfügen möglicherweise nicht über die erforderlichen Berechtigungen.

Lösung

Melden Sie sich als „root“ an.

17.2 Ausschlusskonfiguration wurde nicht umgesetzt

Symptom

Wenn Sie Sophos Anti-Virus so konfigurieren, dass Objekte in die Überprüfung eingeschlossen werden, die vorher davon ausgeschlossen waren, bleiben sie mitunter auch weiterhin ausgeschlossen.

Ursache

Dies kann daran liegen, dass der Cache der bereits überprüften Dateien die ausgeschlossenen Dateien noch enthält.

Lösung

Verfahren Sie je nach verwendeter Interception-Methode für On-Access-Überprüfungen wie folgt:

- Versuchen Sie in Talpa, den Cache zu leeren. Geben Sie hierzu Folgendes ein:

  ```
  echo 'disable' > /proc/sys/talpa/intercept-filters/Cache/status
  echo 'enable' > /proc/sys/talpa/intercept-filters/Cache/status
  ```

- Versuchen Sie in Fanotify, den installierten Dienst „sav-protect“ neu zu starten. Geben Sie hierzu Folgendes ein:

  `/etc/init.d/sav-protect restart`

17.3 Computermeldung „Kein manueller Eintrag für...“

Symptom

Beim Versuch, eine man page von Sophos Anti-Virus zu öffnen, wird auf dem Computer etwa folgende Meldung angezeigt `No manual entry for ...`.

Ursache

Das Problem liegt möglicherweise daran, dass die Umgebungsvariable „MANPATH“ den Pfad zur man page nicht umfasst.

Lösung

1. Wenn Sie als Shell sh, ksh oder bash verwenden, öffnen Sie `/etc/profile` zur Bearbeitung.

   Wenn Sie als Shell csh, tcsh verwenden, öffnen Sie `/etc/login` zur Bearbeitung.

   Hinweis: Wenn Sie nicht über ein Anmeldeskript oder Profil verfügen, führen Sie in der Befehlszeile folgende Schritte aus. Sie müssen das Verfahren bei jedem Neustart wiederholen.

2. Überprüfen Sie, ob die Umgebungsvariable „MANPATH“ den Pfad zum Verzeichnis `/usr/local/man` umfasst.

3. Wenn „MANPATH“ das Verzeichnis nicht umfasst, fügen Sie es wie folgt hinzu: Ändern Sie nicht die vorhandenen Einstellungen.

   Wenn Sie als Shell sh, ksh oder bash verwenden, geben Sie ein:

   `MANPATH=$MANPATH:/usr/local/man`

   `export MANPATH`

   Wenn Sie als Shell csh oder tcsh verwenden, geben Sie ein:

   `setenv MANPATH` *`Werte`***`:/usr/local/man`**

   Dabei ist *Werte* durch die vorhandenen Einstellungen zu ersetzen.

4. Speichern Sie das Anmeldeskript oder Profil.

17.4 Nicht genug Speicherplatz auf Festplatte

Symptom

Sophos Anti-Virus steht nicht genug Speicher für die Überprüfung umfangreicher Archive zur Verfügung.

Mögliche Ursachen

Folgende Ursachen sind möglich:

- Beim Entpacken der Archive lagert Sophos Anti-Virus die Zwischenergebnisse im temporären Verzeichnis (`/tmp`) aus. Wenn dieses Verzeichnis nicht groß genug ist, kann Sophos Anti-Virus nicht alle erforderlichen Dateien darin auslagern.
- Sophos Anti-Virus hat das Speicherkontingent des Benutzers überschritten.

Lösung

Führen Sie einen der folgenden Schritte aus:

- Vergrößern Sie `/tmp`.
- Vergrößern Sie das Speicherkontingent des Benutzers.
- Oder geben Sie für die Auslagerung der Zwischenergebnisse von Sophos Anti-Virus ein anderes Verzeichnis an. Verwenden Sie dazu die Umgebungsvariable SAV_TMP.

17.5 Langsame On-Demand-Überprüfung

Dieses Problem kann zwei Ursachen haben:

Symptom

Überprüfungen in Sophos Anti-Virus dauern außergewöhnlich lange.

Mögliche Ursachen

Folgende Ursachen sind möglich:

- Normalerweise führt Sophos Anti-Virus eine schnelle Überprüfung durch, die nur die auf Virenbefall verdächtigten Bereiche einer Datei untersucht. Bei Auswahl einer vollständigen Überprüfung (über die Option **-f**), wird jedoch die gesamte Datei untersucht.
- Normalerweise überprüft Sophos Anti-Virus nur bestimmte Dateitypen. Wenn jedoch die Überprüfung *aller* Dateitypen eingestellt ist, dauert der Vorgang länger.

Lösung

Versuchen Sie, das Problem anhand einer der folgenden Methoden zu beheben:

- Sofern Sie nicht beispielsweise vom technischen Support von Sophos dazu aufgefordert wurden, wird von der vollständigen Überprüfung abgeraten.
- Sollen Dateien mit bestimmten Erweiterungen überprüft werden, nehmen Sie diese Erweiterungen in die Liste der von Sophos Anti-Virus standardmäßig überprüften Dateitypen auf. Weitere Informationen finden Sie unter Überprüfen eines bestimmten Dateityps (Seite 11).

17.6 Archiver legt Backups aller Dateien an, die einer On-Demand-Überprüfung unterzogen wurden

Symptom

Ihr Archivierungsprogramm kann so eingestellt sein, dass es nach einer On-Demand-Überprüfung immer Backups der in Sophos Anti-Virus überprüften Dateien anlegt.

Ursache

Dies kann auf Änderungen zurückzuführen sein, die Sophos Anti-Virus in der Zeit des geänderten Status von Dateien vornimmt. Standardmäßig versucht Sophos Anti-Virus, die Zugriffszeit (**atime**) von Dateien auf die vor der Überprüfung angegebene Zeit zurückzusetzen. Dadurch wird jedoch das im Indexeintrag festgesetzte Attribut „status-changed time“ (**ctime**) geändert. Wenn Ihr Archivierungsprogramm anhand der **ctime** ermittelt Sophos Anti-Virus, ob eine Datei geändert wurde, legt es von allen überprüften Dateien Backups an.

Lösung

Führen Sie **savscan** with the option **--no-reset-atime**.

17.7 Viren nicht beseitigt

Symptome

- Sophos Anti-Virus hat nicht versucht, einen Virus zu bereinigen.
- In Sophos Anti-Virus wird die Fehlermeldung `Disinfection failed` angezeigt.

Mögliche Ursachen

Folgende Ursachen sind möglich:

- Die automatische Bereinigung wurde nicht aktiviert.
- Sophos Anti-Virus kann diese Virenart nicht bereinigen.
- Die infizierte Datei befindet sich auf einem schreibgeschützten Wechselmedium.
- Die infizierte Datei befindet sich auf einem NTFS-Dateisystem.
- Sophos Anti-Virus bereinigt keine Viren-Fragmente, da es keine exakte Übereinstimmung mit dem Virus gefunden hat.

Lösung

Versuchen Sie, das Problem anhand einer der folgenden Methoden zu beheben:

- Aktivieren Sie die automatische Bereinigung.

- Versehen Sie das Medium mit Schreibzugriff (sofern möglich).
- Wenn sich die Dateien auf einem NTFS-Dateisystem befinden, bereinigen Sie sie lokal auf dem Computer.

17.8 Viren-Fragment

Symptom

Sophos Anti-Virus hat ein Viren-Fragment erkannt.

Mögliche Ursachen

Teile einer Datei entsprechen Bestandteilen von Viren. Dies passiert aus einem der folgenden Gründe:

- Viren werden häufig auf der Basis vorhandener Malware entwickelt. Es kann daher vorkommen, dass Code-Fragmente von bekannten Viren in Dateien auftreten, die von neuen Viren betroffen sind.
- Viele Viren enthalten Fehler in ihren Replikationsroutinen und die Zieldateien werden nicht wie geplant infiziert. Ein nicht aktiver Teil eines Virus (möglicherweise ein wesentlicher Teil) kann in einer Hostdatei auftauchen und von Sophos Anti-Virus erkannt werden.
- Bei einer vollständigen Systemüberprüfung kann Sophos Anti-Virus ein Viren-/Spyware-Fragment in einer Datenbankdatei melden.

Lösung

1. Führen Sie auf dem betroffenen Computer ein Update von Sophos Anti-Virus aus.
2. Anweisungen zum Entfernen der Datei finden Sie unter Löschen einer bestimmten infizierten Datei (Seite 17).
3. Wenn Viren-Fragmente immer noch gemeldet werden, wenden Sie sich bitte an den technischen Support von Sophos.

17.9 Kein Zugriff auf Datenträger

Symptom

Sie können nicht auf Dateien auf einem Wechseldatenträger zugreifen.

Ursache

Sophos Anti-Virus verhindert standardmäßig den Zugriff auf Wechseldatenträger mit infizierten Bootsektoren.

Lösung

So geben Sie den Zugriff auf einen Datenträger mit infiziertem Bootsektor frei:

1. Geben Sie Folgendes ein:

   `/opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat enabled`

2. Geben Sie nach Zugriff auf den Datenträger Folgendes ein:

   `/opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat disabled`

3. Entfernen Sie den Datenträger aus dem Computer, so dass er den Computer beim Neustart nicht nochmals infizieren kann.

18 Anhang: Fehlercodes der On-Demand-Überprüfung

Der Ausgabe-Code von **savscan** an die Shell zeigt das Ergebnis der Überprüfung an. Nach Abschluss der Überprüfung können Sie sich den Code durch Eingabe eines weiteren Befehls anzeigen lassen. Beispiel:

echo $?

Erweiterte Rückgabewerte	Beschreibung
0	Keine Fehler und keine Viren
1	Die Überprüfung des Befehls wurde durch die Tastenkombination STRG+C unterbrochen.
2	Es ist ein Fehler aufgetreten, der die weitere Ausführung der Überprüfung verhindert.
3	Es wurde ein Virus erkannt.

18.1 Erweiterte Fehlercodes

Die Code-Ausgabe von **savscan** für die Shell ist bei Kombination mit der Option **-eec** ausführlicher. Nach Abschluss der Überprüfung können Sie sich den Code durch Eingabe eines weiteren Befehls anzeigen lassen. Beispiel:

echo $?

Erweiterter Fehlercode	Beschreibung
0	Keine Fehler und keine Viren
8	Nicht schwerwiegender Fehler
16	Eine kennwortgeschützte Datei wurde gefunden (nicht überprüft)
20	Ein Objekt mit Virus wurde entdeckt und desinfiziert

Erweiterter Fehlercode	Beschreibung
24	Ein Objekt mit Virus wurde entdeckt und nicht desinfiziert
28	Ein Virus im Speicher wurde erkannt
32	Bei der Integritätsprüfung ist ein Fehler aufgetreten
36	Es sind unüberwindbare Fehler aufgetreten.
40	Die Überprüfung wird unterbrochen

19 Anhang: Konfigurieren der Phone-Home-Funktion

Sophos Anti-Virus kann Sophos kontaktieren und Produkt- und Plattforminformationen an uns senden. Diese „Phone-Home“-Funktion hilft uns, das Produkt und das Benutzererlebnis zu verbessern.

Wenn Sie Sophos Anti-Virus installieren, wird die Phone-Home-Funktion standardmäßig aktiviert. Deaktivieren Sie sie bitte nicht. Ihre Sicherheit oder die Leistung Ihres Computers wird dadurch nicht beeinträchtigt:

- Ihre Daten werden verschlüsselt an einen sicheren Speicherort gesendet und höchstens drei Monate gespeichert.
- Das Produkt sendet einmal in der Woche ca. 2 KB. Die Informationen werden in zufälligen zeitlichen Abständen gesendet, um zu vermeiden, dass mehrere Computer gleichzeitig Daten senden.

Sie können die Funktion nach der Installation jederzeit deaktivieren.

Geben Sie zum Deaktivieren der Phone-Home-Funktion folgenden Befehl ein:

```
/opt/sophos-av/bin/savconfig set DisableFeedback true
```

Geben Sie zum erneuten Aktivieren der Phone-Home-Funktion folgenden Befehl ein:

```
/opt/sophos-av/bin/savconfig set DisableFeedback false
```

20 Anhang: Konfigurieren von Neustarts für RMS

Wenn das RMS (Remote Management System), das die Kommunikation mit dem Server steuert, abstürzt oder nicht richtig hochfährt, startet ein Adapter die RMS-Komponenten mrouter und magent neu.

Wenn das RMS in regelmäßigen Abständen neu gestartet werden soll, fügen Sie

`RestartIntervalHours=<Hours>`

zu $INST/etc/sophosmgmtd.conf hinzu.

21 Glossar

Bootsektor-Virus	Virenart, die die Anfangsphase des Boot-Vorgangs untergräbt. Bootsektor-Viren greifen entweder den Master-Bootsektor oder den Partitions-Bootsektor an.
Desinfektion	Unter Desinfektion bzw. Beseitigung ist das Löschen eines Virus aus einer Datei oder dem Bootsektor zu verstehen.
Extradateien	Ein Verzeichnis, in dem die Konfiguration von Sophos Anti-Virus für das Netzwerk gespeichert wird. Wenn Computer Updates durchführen, laden Sie die Konfiguration hier herunter.
Geplanter Scan	Ein vollständiger oder teilweiser Scans eines Computers zu festgesetzten Zeiten.
On-Access-Scans	Der zentrale Schutz vor Viren. Beim Versuch, auf eine Datei (d.h. Kopieren, Speichern, Verschieben oder Öffnen der Datei) zuzugreifen, überprüft Sophos Anti-Virus die Datei. Der Zugriff wird nur erlaubt, wenn die Datei threatfrei ist.
On-Demand-Scans	Vom Benutzer eingeleiteter Scan. Sie können alle Objekte mit On-Demand-Scans scannen, für die Sie Lesezugriff besitzen – der Umfang reicht von einzelnen Dateien bis hin zum gesamten Computer.
Primäre Update-Quelle	Hierbei handelt es sich um den Netzwerkpfad, über den Updates verfügbar gemacht werden. Zum Zugriff auf diesen Pfad sind u.U. Zugangsdaten erforderlich.
Sekundäre Update-Quelle	Hierbei handelt es sich um den Netzwerkpfad, über den Updates verfügbar gemacht werden, wenn die primäre Update-Quelle nicht verfügbar ist. Zum Zugriff auf diesen Pfad sind u.U. Zugangsdaten erforderlich.
Sophos Live-Schutz	Mit dieser Funktion lässt sich über ein „In-the-Cloud“-Verfahren sofort feststellen, ob eine Datei eine Bedrohung darstellt. Bei Bedarf werden umgehend die in der Bereinigungskonfiguration von Sophos Anti-Virus festgelegten Maßnahmen ergriffen.
Update-Client	Ein Computer, auf dem Sophos Anti-Virus installiert ist, der anderen Computern nicht als Update-Quelle dient.

Update-Server	Ein Computer, auf dem Sophos Anti-Virus installiert ist, der anderen Computern als Update-Quelle dient. Die anderen Computer können entweder Update-Server oder Update-Clients sein. Dies richtet sich danach, auf welche Weise Sophos Anti-Virus im Netzwerk eingesetzt wird.
Virus	Computerprogramm, das sich selbst kopiert. Durch Viren werden Computersysteme gestört oder darauf befindliche Daten beschädigt. Viren benötigen ein Hostprogramm und infizieren Computer erst, wenn sie ausgeführt werden. Viren kopieren sich selbst oder leiten sich selbst über E-Mails weiter und breiten sich so im Netzwerk aus. Häufig bezieht sich der Begriff „Virus“ auch auf Spyware, Würmer und Trojaner.
Zentrales Installationsverzeichnis (CID)	Netzwerkfreigabe, in der Sophos Sicherheitssoftware und Updates bereitgestellt werden. Netzwerkcomputer beziehen ihre Updates über dieses Verzeichnis.

22 Technischer Support

Technischen Support zu Sophos Produkten können Sie wie folgt abrufen:

- Rufen Sie das Sophos Community unter community.sophos.com/ auf und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Support-Knowledgebase unter www.sophos.com/de-de/support.aspx.
- Begleitmaterial zu den Produkten finden Sie hier: www.sophos.com/de-de/support/documentation.aspx.
- Öffnen Sie ein Ticket bei unserem Support-Team unter https://secure2.sophos.com/de-de/support/contact-support/support-query.aspx.

23 Rechtlicher Hinweis

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

GNU General Public License

Some software programs are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or similar Free Software licenses which, among other rights, permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires for any software licensed under the GPL, which is distributed to a user in an executable binary format, that the source code also be made available to those users. For any such software which is distributed along with this Sophos product, the source code is available by submitting a request to Sophos via email to savlinuxgpl@sophos.com. A copy of the GPL terms can be found at www.gnu.org/copyleft/gpl.html

libmagic – file type detection

Copyright © Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994–2004 Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)

ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Medusa web server

Medusa was once distributed under a 'free for non-commercial use' license, but in May of 2000 Sam Rushing changed the license to be identical to the standard Python license at the time. The standard Python license has always applied to the core components of Medusa, this change just frees up the rest of the system, including the http server, ftp server, utilities, etc. Medusa is therefore under the following license:

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Sam Rushing not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SAM RUSHING DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL SAM RUSHING BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Sam would like to take this opportunity to thank all of the folks who supported Medusa over the years by purchasing commercial licenses.

OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998-2016 The OpenSSL Project. Alle Rechte vorbehalten.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

   The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Protocol Buffers (libprotobuf)

Copyright 2008, Google Inc.

Alle Rechte vorbehalten.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

pycrypto

Distribute and use freely; there are no restrictions on further dissemination and usage except those imposed by the laws of your country of residence. This software is provided “as is” without warranty of fitness for use or suitability for any purpose, express or implied. Use at your own risk or not at all.

Incorporating the code into commercial products is permitted; you do not have to make source available or contribute your changes back (though that would be nice).

– –amk (www.amk.ca)

Python

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

1. This LICENSE AGREEMENT is between the Python Software Foundation (“PSF”), and the Individual or Organization (“Licensee”) accessing and otherwise using this software (“Python”) in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, worldwide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF’s License Agreement and PSF’s notice of copyright, i.e., “Copyright © 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 Python Software Foundation; All Rights Reserved” are retained in Python alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.
4. PSF is making Python available to Licensee on an “AS IS” basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

TinyXML XML parser

www.sourceforge.net/projects/tinyxml

Original code by Lee Thomason (www.grinninglizard.com)

This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

zlib data compression library

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

20161125

Index

R

S

U

V

Z