SOPHOS
Security made simple.

Sophos Anti-Virus für Unix

Konfigurationsanleitung

Produktversion:9

Inhalt

1 Einleitung

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

Hinweise zum *Installieren von* Sophos Anti-Virus finden Sie hier: *Sophos Anti-Virus für UNIXSchnellstart-Anleitung*.

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

2 Über Sophos Anti-Virus für UNIX

2.1 Funktionen von Sophos Anti-Virus

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

2.2 Funktionsweise von Sophos Anti-Virus

Mit Sophos Anti-Virus können Sie eine *On-Demand-Überprüfung* ausführen. 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

Sophos Anti-Virus wird über eine Befehlszeilenschnittstelle ausgeführt. Darüber können Sie auf alle Funktionen von Sophos Anti-Virus zugreifen und die Software konfigurieren.

Hinweis
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

Wenn Sie über ein Netzwerk mit UNIX-Computern verfügen, die *nicht* von Enterprise Console verwaltet werden, konfigurieren Sie Sophos Anti-Virus wie folgt:

- Sie können **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 16).
- Konfigurieren Sie **On-Demand-Überprüfungen** von Sophos Anti-Virus lokal über die Befehlszeile auf allen Computern.

Bei Einzelplatzrechnern mit UNIX, die *nicht* von Enterprise Console verwaltet werden, konfigurieren Sie sämtliche Funktionen von Sophos Anti-Virus über die Sophos Anti-Virus-Befehlszeilenschnittstelle.

Wenn Ihre UNIX-Computer von Sophos Enterprise Console verwaltet werden, konfigurieren Sie Sophos Anti-Virus wie folgt:

- Die **zeitgesteuerte Überprüfung, Benachrichtigungen und Alarme sowie die Protokolle und Updates** werden zentral über Enterprise Console konfiguriert. Nähere Informationen finden Sie in der Hilfe zu Enterprise Console.

  Hinweis
  Die Funktionen umfassen auch Parameter, die mit Enterprise Console nicht festgelegt werden können. Sie können die Parameter von Sophos Anti-Virus lokal über die Befehlszeile auf allen UNIX-Computern festlegen. Enterprise Console ignoriert sie.

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

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

3 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.

3.1 Ausführen einer On-Demand-Überprüfung

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

3.1.1 Durchführen einer On-Demand-Überprüfung

Wir empfehlen Ihnen, nach der Installation von Sophos Anti-Virus den gesamten Computer auf Viren zu überprüfen. Führen Sie hierzu eine On-Demand-Überprüfung durch.

> **Hinweis**
> Dies ist besonders wichtig, wenn es sich bei dem Computer um einen Server handelt und verhindert werden soll, dass sich Viren auf andere Computer ausbreiten.

- Geben Sie zum Durchführen einer On-Demand-Überprüfung auf dem Computer Folgendes ein:
  ```
  savscan /
  ```

3.1.2 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.

3.1.3 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.

3.2 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
```

3.2.1 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.

3.2.2 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.

3.2.3 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.

3.2.4 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.

3.2.5 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`

3.2.6 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.

3.2.7 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`

3.2.8 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
```

3.2.9 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`.

4 Was passiert, wenn ein Virus erkannt wird?

Wenn Viren gefunden werden, geht Sophos Anti-Virus wie folgt vor:

- Festhalten des Ereignisses im Systemprotokoll und im Sophos Anti-Virus-Protokoll (Details entnehmen Sie bitte dem Abschnitt Abrufen des Sophos Anti-Virus-Protokolls(Seite 12)).
- Versenden eines Alarms an Enterprise Console (bei Verwaltung mit Enterprise Console).
- Versenden einer E-Mail-Benachrichtigung an „root@localhost“.

Standardmäßig zeigt Sophos Anti-Virus auch Benachrichtigungen an.

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. Alle Rechte vorbehalten.

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 or email support@sophos.com
End of Scan.
```

Anweisungen zur Bereinigung von Viren finden Sie im Abschnitt Bereinigen von Viren(Seite 9).

5 Bereinigen von Viren

5.1 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.

5.2 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 9)) 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.

5.2.1 Angabe der Parameter für Quarantäne

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

5.3 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.

5.3.1 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. (Im Abschnitt Bereinigungs-Details(Seite 9) erfahren Sie, wo Sie auf der Sophos Website nähere Informationen über das Verhalten von Viren erhalten.)

5.3.2 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. (Im Abschnitt Bereinigungs-Details(Seite 9) erfahren Sie, wo Sie auf der Sophos Website nähere Informationen über das Verhalten von Viren erhalten.)

5.3.3 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.

5.3.4 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.

5.4 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.

6 Abrufen des Sophos Anti-Virus-Protokolls

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.

Weitere Informationen zu den im syslog protokollierten Informationen finden Sie hier: Anhang: Syslog-Meldungen(Seite 30).

- Geben Sie zum Abrufen des Protokolls von Sophos Anti-Virus den Befehl `savlog` in die Befehlszeile 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
  ```

7 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 über Sophos Enterprise Console möglich.

8 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.

8.1 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
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

Erweiterter Fehlercode	Beschreibung
36	Es sind unüberwindbare Fehler aufgetreten.
40	Die Überprüfung wird unterbrochen

9 Anhang: Konfiguration mit Extradateien

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

9.1 Die Konfiguration mit Extradateien

Dieser Abschnitt enthält einen Überblick über die Konfiguration mit Extradateien.

9.1.1 Was bedeutet Konfiguration mit Extradateien?

Die Konfiguration mit Extradateien ist eine Methode, um Sophos Anti-Virus 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 5)) konfigurieren.

9.1.2 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 entsprechende 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.

9.2 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.

9.2.1 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
   ```

9.2.2 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 20)).
- *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 20).

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-path live-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
   ```

9.2.3 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
   ```


9.2.4 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
   ```

9.3 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-path live-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
   ```

9.4 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.

9.5 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
```

9.5.1 *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
```

9.5.2 *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.

9.5.3 *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.

9.5.4 *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.

10 Anhang: 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 über Sophos Anti-Virus eine zeitgesteuerte Überprüfung 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 Sie alle geplanten Scans (einschl. der mit Enterprise Console erstellten Scans) von Sophos Anti-Virus in eine Datei exportieren möchten, geben Sie den Befehl `savconfig` und anschließend den 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. 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.

10.9 Abrufen des Sophos Anti-Virus-Protokolls

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.

Weitere Informationen zu den im syslog protokollierten Informationen finden Sie hier: Anhang: Syslog-Meldungen(Seite 30).

- Geben Sie zum Abrufen des Protokolls von Sophos Anti-Virus den Befehl `savlog` in die Befehlszeile 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`

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 Anhang: Konfigurieren von E-Mail-Benachrichtigungen

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

Sie können Sophos Anti-Virus so konfigurieren, dass bei Virenerkennung, Überprüfungsfehlern oder sonstigen Fehlern eine E-Mail-Benachrichtigung versendet wird. E-Mail-Benachrichtigungen können auf Englisch und Japanisch verfasst werden.

11.1 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`

11.2 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 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“ wählen. 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.

11.4 Angeben der E-Mail-Empfänger

Standardmäßig sendet Sophos Anti-Virus E-Mail-Benachrichtigungen an „root@localhost“.

- 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`

11.5 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`

11.6 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`

11.7 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`

11.8 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 Anhang: Konfigurieren der Protokollierung

Hinweis

Wenn Sie einen einzelnen Computer im Netzwerk konfigurieren, könnte die Konfiguration beim Download einer neuen Enterprise Console-Konfiguration 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 Anhang: Syslog-Meldungen

Sophos Anti-Virus protokolliert drei Arten von Meldungen in syslog. Zu diesen zählen:

- `ACTION-REQUIRED`: Diese Meldungen besagen, dass Sie Korrekturmaßnahmen ergreifen müssen.
- `ERROR`: Diese Meldungen verweisen auf Fehler, die beim Scannen aufgetreten sind.
- `INFO`: Diese Meldungen enthalten Informationen zum Scanvorgang.

Die Meldungen werden nach Schwere geordnet angezeigt.

Meldungen „Maßnahme erforderlich“

Bei den folgenden Meldungen müssen Sie Korrekturmaßnahmen ergreifen:

Syslog-Meldung	Beschreibung	Nachrichten-ID	Hinweise
“The threat data is out of date and should be updated.”	Die Bedrohungsdaten sind veraltet und sollten aktualisiert werden.	`VIRUS-DATA-OLD`	Das bedeutet, dass Ihre Update-Quelle keine Updates von Sophos bezieht. Überprüfen Sie dies, um sicherzustellen, dass immer aktuelle Updates von Sophos bereitgestellt werden.
“Sophos Anti-Virus is not configured to update.”	Für Sophos Anti-Virus sind keine Updates eingerichtet.	`NO-UPDATE-CONFIGURATION`	Sophos Anti-Virus stellt nur echten Schutz bereit, wenn Updates von Sophos bezogen werden. Für diesen Rechner sind keine Updates eingerichtet.
“Not updating from Sophos as updates directly from Sophos are not supported.”	Kein Bezug von Updates von Sophos, da Updates direkt von Sophos nicht unterstützt werden.	`NO-UPDATE-FROM-SOPHOS`	Das ist eine alte Meldung, die nicht angezeigt werden dürfte.
"Threat detected in %s: %s during on-demand scan. [The file is still infected.]"	Sophos Anti-Virus hat bei der On-Demand-Überprüfung eine Bedrohung festgestellt. Die Datei ist immer noch infiziert.	`NOTIFY-ONDEMAND-THREAT-INFECTED`	Melden Sie sich an und entfernen Sie die Datei oder versuchen Sie, die Infektion mit savscan zu entfernen.

Syslog-Meldung	Beschreibung	Nachrichten-ID	Hinweise
"Threat detected in %s: %s during on-demand scan. (The file has been quarantined.)"	Sophos Anti-Virus hat bei der On-Demand-Überprüfung eine Bedrohung festgestellt. Die Datei ist immer noch infiziert. Die Datei ist nicht ausführbar und nicht für normale Benutzer zugänglich, wenn der Scan als Root ausgeführt wurde.	`NOTIFY-ONDEMAND-THREAT-QUARANTINED`	Melden Sie sich an und entfernen Sie die Datei oder versuchen Sie, die Infektion mit savscan zu entfernen.

Fehlermeldungen

Diese Meldungen verweisen auf Fehler, die beim Scanvorgang aufgetreten sind. Außerdem bekommen Sie mitgeteilt, ob und welche Korrekturmaßnahmen Sie ergreifen müssen.

Syslog-Meldung	Beschreibung	Nachrichten-ID
“Too many incidents occurred (%s incident notifications were discarded).”	Zu viele Vorfälle aufgetreten (%s Vorfallmeldungen wurden verworfen). Das bedeutet, dass savd mit Meldungen überlastet war und einige Meldungen verworfen wurden.	`MESSAGES_DROPPED %s`
"Respawn limit exceeded[no further scan processors will be started."	Respawn-Limit überschritten, es werden keine weiteren Prozessoren gestartet. savd hat das Spawning von savscand gestoppt, weil savscand nicht gestartet werden konnte. savd wird erneut gestartet, sobald das Problem behoben ist.	`RESPAWN-LIMIT`
"Throttling scan processor respawn."	Savd steuert, wie schnell savscand-Prozesse gestartet werden, weil sie zu schnell beendet werden.	`RESPAWN-THROTTLE`
"Previous instance of Sophos Anti-Virus daemon did not exit cleanly."	Sophos Anti-Virus wurde das letzte Mal nicht richtig beendet. Keine weitere Maßnahme erforderlich.	`SAVD-CLEANUP`

Syslog-Meldung	Beschreibung	Nachrichten-ID
"Force-terminated a scan processor."	Sophos Anti-Virus Scanner beendet. Savd hat savscand zwangsbeendet. Keine weitere Maßnahme erforderlich, außer dies tritt häufiger auf.	`SCANNER-DIED-KILLED`
"Force-terminated a scan processor."	Sophos Anti-Virus Scanner beendet. Savd hat savscand zwangsbeendet. Keine weitere Maßnahme erforderlich, außer dies tritt häufiger auf.	`SCANNER-DIED-KILLED-PID`
"A scan processor unexpectedly terminated with signal: %s."	Sophos Anti-Virus Scanner beendet. savscand aufgrund des Empfangs eines Signals beendet. Keine weitere Maßnahme erforderlich, außer dies tritt häufiger auf.	`SCANNER-DIED-SIGNAL`
"A scan processor died during startup with signal: %s."	Sophos Anti-Virus Scanner konnte nicht gestartet werden. savscand aufgrund des Empfangs eines Signals während des Startvorgangs beendet. Keine weitere Maßnahme erforderlich, außer dies tritt häufiger auf.	`SCANNER-DIED-STARTUP-SIGNAL`
"A scan processor died during startup with status code: %s."	Sophos Anti-Virus Scanner konnte nicht gestartet werden. savscand während des Startvorgangs beendet. Keine weitere Maßnahme erforderlich, außer dies tritt häufiger auf.	`SCANNER-DIED-STARTUP-STATUS`

Syslog-Meldung	Beschreibung	Nachrichten-ID
"A scan processor unexpectedly terminated with status code: %s."	Sophos Anti-Virus Scanner unerwartet beendet. savscand unerwartet beendet. Keine weitere Maßnahme erforderlich, außer dies passiert häufiger.	`SCANNER-DIED-STATUS`
"Terminated a scan processor."	Sophos Anti-Virus Scanner beendet. Savd hat savscand beendet. Keine weitere Maßnahme erforderlich, außer dies tritt häufiger auf.	`SCANNER-DIED-TERMED`
"Terminated a scan processor."	Sophos Anti-Virus Scanner beendet. Savd hat savscand beendet. Keine weitere Maßnahme erforderlich, außer dies tritt häufiger auf.	`SCANNER-DIED-TERMED-PID`
"Scan processor failed to send heartbeat messages and will be stopped."	Sophos Anti-Virus hat keine Heartbeat-Meldungen gesendet und wurde angehalten. savscand hat nicht zu den erwarteten Zeitpunkten Heartbeat-Meldungen gesendet. Wurde von savd beendet. Keine weitere Maßnahme erforderlich, außer dies tritt häufiger auf.	`TIMEOUT-SCANNER-HEARTBEAT`
"A scan processor timed out during startup."	Sophos Anti-Virus hat ein Timeout erfahren und konnte nicht gestartet werden. savscand konnte nicht innerhalb des Timeout gestartet werden. Wurde von savd beendet. Keine weitere Maßnahme erforderlich, außer dies tritt häufiger auf.	`TIMEOUT-SCANNER-STARTUP`
"Threat detected in %s: %s during on-demand scan. (The file has been deleted.)"	Sophos Anti-Virus hat bei der On-Demand-Überprüfung eine Bedrohung festgestellt. Die Datei wurde gelöscht.	`NOTIFY-ONDEMAND-THREAT-DELETED`

Syslog-Meldung	Beschreibung	Nachrichten-ID
"Threat detected in %s: %s during on-demand scan. (The file has been disinfected.)"	Sophos Anti-Virus hat bei der On-Demand-Überprüfung eine Bedrohung festgestellt. Die Datei wurde desinfiziert.	NOTIFY-ONDEMAND-THREAT-DISINFECTED
"On-demand scan aborted by user."	Sophos Anti-Virus Scan vom Benutzer angehalten.	SAVSCAN-ABORTED
"Scheduled scan \"%s\" failed with error %s (%s)."	Geplanter Sophos Anti-Virus Scan mit Fehler fehlgeschlagen. Die Überprüfung wird zum nächsten geplanten Intervall erneut versucht.	SCHEDULED-SCAN-FAILED
"Scheduled scan \"%s\" failed: unable to parse mounts."	Geplanter Sophos Anti-Virus Scan fehlgeschlagen, da die Mount-Tabelle nicht geparst werden konnte. Sollte dies wiederholt auftreten, melden Sie das Problem bitte dem Sophos Support. Überprüfen Sie die „Mount"-Ausgabe.	SCHEDULED-SCAN-FAILED-MOUNT-PARSING
"Scheduled scan \"%s\" failed: unable to load threat data (%s)."	Geplanter Sophos Anti-Virus Scan beim Laden von Bedrohungsdaten fehlgeschlagen. Keine Maßnahme erforderlich, sofern die Überprüfung nicht wiederholt fehlschlägt.	SCHEDULED-SCAN-FAILED-VDL-LOAD-ERROR
"Unable to load threat data (%s)."	Sophos Anti-Virus Scan beim Laden von Bedrohungsdaten fehlgeschlagen. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird.	SAVI_VDL_LOAD_ERROR
"Failed to replicate from all update sources."	Sophos Anti-Virus konnte nicht aktualisiert werden. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt die Aktualisierung wiederholt fehl, überprüfen Sie, ob die primären Update-Einstellungen korrekt sind.	ALL_UPDATE _SOURCES_FAILED

Syslog-Meldung	Beschreibung	Nachrichten-ID
"Failed to download '%s': invalid authentication."	Sophos Anti-Virus wurde nicht aktualisiert. Keine Maßnahme erforderlich, sofern diese Meldung nicht erneut angezeigt wird. Schlägt die Aktualisierung wiederholt fehl, überprüfen Sie, ob die primären Update-Einstellungen korrekt sind.	`BAD-BACKUP-AUTHENTICATION`
"Failed to download '%s': invalid proxy authentication."	Sophos Anti-Virus wurde nicht aktualisiert. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt die Aktualisierung wiederholt fehl, überprüfen Sie, ob die primären Update-Einstellungen korrekt sind.	`BAD-BACKUP-PROXY-AUTHENTICATION`
"Failed to download '%s': no such file."	Sophos Anti-Virus kann nicht aktualisiert werden. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt die Aktualisierung wiederholt fehl, überprüfen Sie, ob die primären Update-Einstellungen korrekt sind.	`BAD-BACKUP-URL`
"Failed to download '%s': invalid authentication. Please check `ExtraFilesUsername` and `ExtraFilesPassword`."	Sophos Anti-Virus konnte `ExtraFiles` nicht herunterladen. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt dies wiederholt fehl, überprüfen Sie, ob `ExtraFilesUsername` und `ExtraFilesPassword` korrekt sind.	`BAD-EXTRAFILES-AUTHENTICATION`

Syslog-Meldung	Beschreibung	Nachrichten-ID

"Failed to download '%s': invalid proxy authentication.
Please check
`ExtraFilesProxyUsername`
and
`ExtraFilesProxyPassword`."
	Sophos Anti-Virus konnte `ExtraFiles` nicht herunterladen.
	Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt dies wiederholt fehl, überprüfen Sie, ob
	`ExtraFilesProxyUsername`
	und
	`ExtraFilesProxyPassword`
	korrekt sind.
		`BAD-EXTRAFILES-PROXY-AUTHENTICATION`

"Failed to download '%s': no such file. Please check `ExtraFilesSourcePath`."	Sophos Anti-Virus konnte `ExtraFiles` nicht herunterladen. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt dies wiederholt fehl, überprüfen Sie, ob `ExtraFilesSourcePath` korrekt ist.	`BAD-EXTRAFILES-URL`
"Failed to download '%s': invalid authentication. Please check `PrimaryUpdateUsername` and `PrimaryUpdatePassword`."	Sophos Anti-Virus kann sich nicht bei der primären Update-Quelle authentifizieren. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt dies wiederholt fehl, überprüfen Sie, ob `PrimaryUpdateUsername` und `PrimaryUpdatePassword` korrekt sind.	`BAD-PRIMARY-AUTHENTICATION`

Syslog-Meldung	Beschreibung	Nachrichten-ID

"Failed to download '%s': invalid proxy authentication.
Please check
`PrimaryUpdate`
`ProxyUsername` and
`PrimaryUpdate`
`ProxyPassword`."
	Sophos Anti-Virus kann sich nicht beim primären Quell-Proxy authentifizieren.
	Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt dies wiederholt fehl, überprüfen Sie Folgendes:
	Überprüfen Sie, ob
	`PrimaryUpdate`
	`ProxyUsername`
	und `PrimaryUpdate`
	`ProxyPassword`
	korrekt sind.
		`BAD-PRIMARY-PROXY-AUTHENTICATION`

"Failed to download '%s': no such file. Please check `PrimaryUpdateSourcePath`."	Sophos Anti-Virus kann die primäre Update-Quelle nicht erreichen. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt dies wiederholt fehl, überprüfen Sie Folgendes: Überprüfen Sie, ob `PrimaryUpdateSourcePath` korrekt ist.	`BAD-PRIMARY-URL`

"Failed to download '%s': invalid authentication.
Please check
`SecondaryUpdateUsername`
and
`SecondaryUpdatePassword`."
	Sophos Anti-Virus kann sich nicht bei der sekundären Update-Quelle authentifizieren.
	Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt dies wiederholt fehl, überprüfen Sie, ob
	`SecondaryUpdateUsername`
	und
	`SecondaryUpdatePassword`
	korrekt sind.
		`BAD-SECONDARY-AUTHENTICATION`

Syslog-Meldung	Beschreibung	Nachrichten-ID

"Failed to download '%s': invalid proxy authentication.
Please check
`SecondaryUpdate`
`ProxyUsername`
and `SecondaryUpdate`
`ProxyPassword`."
	Sophos Anti-Virus kann sich nicht beim primären Quell-Proxy authentifizieren.
	Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt dies wiederholt fehl, überprüfen Sie Folgendes:
	Überprüfen Sie, ob
	`SecondaryUpdate`
	`ProxyUsername`
	und `SecondaryUpdate`
	`ProxyPassword`
	korrekt sind.
		`BAD-SECONDARY-PROXY-AUTHENTICATION`

"Failed to download '%s': no such file. Please check `SecondaryUpdate` `SourcePath`."	Sophos Anti-Virus kann die primäre Update-Quelle nicht erreichen. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt dies wiederholt fehl, überprüfen Sie Folgendes: Überprüfen Sie, ob `SecondaryUpdate` `SourcePath`. korrekt ist.	`BAD-SECONDARY-URL`
"Failed to find validation certificate at %s"	Sophos Anti-Virus konnte aufgrund eines fehlenden Verifizierungszertifikats nicht aktualisiert werden. Falls diese Meldung erneut angezeigt wird, deinstallieren und installieren Sie Sophos Anti-Virus neu.	`CERTIFICATE_NOT_FOUND`
"Timeout connecting to server %s"	Timeout bei Savupdate beim Versuch, sich mit einem Update-Server unter der festgelegten Adresse zu verbinden.	`CONNECTION-TIMEOUT`

Syslog-Meldung	Beschreibung	Nachrichten-ID
"Savupdate control script for 'after upgrade' reported code %s"	Benutzerdefiniertes Scripting nach Upgrade ist fehlgeschlagen. Beheben Sie das Problem mit dem benutzerdefinierten Skript oder entfernen Sie es. Sophos Anti-Virus wurde aktualisiert.	CONTROL_SCRIPT _AFTER_UPGRADE_ABORT
"Savupdate control script for 'before upgrade' aborted upgrade with code %s"	Benutzerdefiniertes Scripting vor Upgrade ist fehlgeschlagen. Beheben Sie das Problem mit dem benutzerdefinierten Skript oder entfernen Sie es. Sophos Anti-Virus wurde nicht aktualisiert.	CONTROL_SCRIPT_ BEFORE_UPGRADE_ABORT
"Failed to replicate from %s."	Sophos Anti-Virus wurde nicht aktualisiert. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt die Aktualisierung wiederholt fehl, überprüfen Sie die Update-Einstellungen.	FAILED-TO-UPDATE-FROM
"Failed to verify a manifest file '%s'."	Sophos Anti-Virus wurde nicht aktualisiert. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wenn die Aktualisierung wiederholt fehlschlägt: Bei Aktualisierung über CID die Quelle neu erstellen. Bei Aktualisierung über Sophos Sophos Anti-Virus neu installieren.	FAILED_VERIFY_MANIFEST

Syslog-Meldung	Beschreibung	Nachrichten-ID
"Update failed: Invalid checksum for %s from %s."	Sophos Anti-Virus wurde nicht aktualisiert. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wenn die Aktualisierung wiederholt fehlschlägt: Bei Aktualisierung über CID die Quelle neu erstellen. Bei Aktualisierung über Sophos Sophos Anti-Virus neu installieren.	INVALID-CHECKSUM-FROM
"Failed to validate contents of cache directory '%s'"	Sophos Anti-Virus wurde nicht aktualisiert. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wenn die Aktualisierung wiederholt fehlschlägt: Bei Aktualisierung über CID die Quelle neu erstellen. Bei Aktualisierung über Sophos Sophos Anti-Virus neu installieren.	MSG_COMPOUNDSINK _VALIDATE_FAIL
"Failed to update Sophos Anti-Virus ."	Sophos Anti-Virus wurde nicht aktualisiert. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt die Aktualisierung wiederholt fehl, schauen Sie in den anderen Protokollmeldungen nach, welche Maßnahme zu ergreifen ist.	MSG_RTC_UPDATE_FAIL
"Failed to update - no valid configuration found."	Sophos Anti-Virus kann nicht aktualisiert werden. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Schlägt die Aktualisierung wiederholt fehl, überprüfen Sie die Update-Einstellungen.	NO_VALID _CONFIGURATION_FOUND

Syslog-Meldung	Beschreibung	Nachrichten-ID
"Failed to update from primary update source. Redirecting to secondary update source."	Sophos Anti-Virus wurde über die sekundären Einstellungen aktualisiert, da eine Aktualisierung über die primären Einstellungen nicht möglich war. Überprüfen Sie die primären Update-Einstellungen und die Verfügbarkeit des primären Servers.	SECONDARY-REPORT-AS-ERROR
"Updated to versions - SAV: %s[Engine: %s[Data: %s]"	Sophos Anti-Virus aktualisiert. Keine Maßnahme erforderlich.	UPDATED_TO_VERSION %s %s %s
"Failed to find suitable product in warehouse at %s."	Sophos Anti-Virus wurde nicht aktualisiert. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wenn die Aktualisierung wiederholt fehlschlägt, installieren Sie Sophos Anti-Virus neu.	UPDATE_FAILURE _PRODUCT_UNAVAILABLE
"Warehouse certificate chain is invalid. The update source address is %s."	Sophos Anti-Virus wurde nicht aktualisiert. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wenn die Aktualisierung wiederholt fehlschlägt, installieren Sie Sophos Anti-Virus neu.	UPDATE_FAILURE_SDDS _BAD_CERTIFICATE_CHAIN
"Failed to validate warehouse signatures. The update source address is %s."	Sophos Anti-Virus wurde nicht aktualisiert. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wenn die Aktualisierung wiederholt fehlschlägt, installieren Sie Sophos Anti-Virus neu.	UPDATE_FAILURE_SDDS _SIGNING_ERROR
"Failed to find supplement warehouse. The update source address is %s."	Sophos Anti-Virus wurde nicht aktualisiert. Zusatz-Warehouse kann nicht gefunden werden. Überprüfen Sie die Einstellungen.	UPDATE_FAILURE_SUPPLEMENT _WAREHOUSE_UNAVAILABLE

Syslog-Meldung	Beschreibung	Nachrichten-ID
"Updating from versions - SAV: %s[Engine: %s[Data: %s]."	Sophos Anti-Virus wird aktualisiert. Keine Maßnahme erforderlich.	`UPDATING_FROM_VERSION`
"Main configuration is not available[using backup configuration."	Sophos Anti-Virus über die Backup-Einstellungen aktualisiert. Stellen Sie sicher, dass die primären Update-Einstellungen korrekt konfiguriert sind.	`USING_BACKUP` `_CONFIGURATION`
"Unable to use %s policy. Using %s policy instead."	Sophos Anti-Virus ist für die Aktualisierung über ein SDDS Tag konfiguriert, das in Ihrem Warehouse nicht verfügbar ist. Stellen Sie sicher, dass `PrimaryUpdatePolicy` richtig eingerichtet ist.	`Unable to follow %s policy[following %s instead`
"Failed to validate contents of package directory '%s'."	Sophos Anti-Virus wurde nicht aktualisiert. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wenn die Aktualisierung wiederholt fehlschlägt, installieren Sie Sophos Anti-Virus neu.	`VERIFICATION_FAILED`
"Unable to locate signature verifier at %s."	Sophos Anti-Virus wurde nicht aktualisiert. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wenn die Aktualisierung wiederholt fehlschlägt, installieren Sie Sophos Anti-Virus neu.	`VERSIG_MISSING`
"magent (%s) unexpectedly terminated with signal: %s."	magent wurde aufgrund eines Signals beendet. sophosmgmtd startet magent automatisch neu. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wird die Meldung wiederholt angezeigt, kontaktieren Sie bitte den Sophos Support.	`MAGENT-DIED-SIGNAL`

Syslog-Meldung	Beschreibung	Nachrichten-ID
"magent (%s) exited with an error (%s)."	magent wurde unerwartet beendet. sophosmgmtd startet magent automatisch neu. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wird die Meldung wiederholt angezeigt, kontaktieren Sie bitte den Sophos Support.	`MAGENT-EXIT-ERROR`
"mrouter (%s) unexpectedly terminated with signal: %s."	mrouter wurde aufgrund eines Signals beendet. sophosmgmtd startet mrouter automatisch neu. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wird die Meldung wiederholt angezeigt, kontaktieren Sie bitte den Sophos Support.	`MROUTER-DIED-SIGNAL`
"mrouter (%s) exited with an error (%s)."	mrouter wurde unerwartet beendet. sophosmgmtd startet mrouter automatisch neu. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wird die Meldung wiederholt angezeigt, kontaktieren Sie bitte den Sophos Support.	`MROUTER-EXIT-ERROR`

Info-Meldungen

Diese Meldungen enthalten Informationen zum Scanvorgang.

Syslog-Meldung	Beschreibung	Nachrichten-ID
"Sophos Anti-Virus daemon started."	Sophos Anti-Virus gestartet.	`SAVD-STARTED`
"Sophos Anti-Virus daemon stopped."	Sophos Anti-Virus angehalten.	`SAVD-STOPPED`
"Loading SAV Interface returned the error %s : %s."	Die Benutzeroberfläche von Sophos Anti-Virus wurde aufgrund eines Fehlers nicht geöffnet.	`SAVI_LOAD_ERROR`

Syslog-Meldung	Beschreibung	Nachrichten-ID
"scan processor running."	Der Sophos Anti-Virus Scanner wird ausgeführt.	SCANNER-RUNNING
"scan processor stopped."	Der Sophos Anti-Virus Scanner wurde angehalten.	SCANNER-SHUTDOWN
"Shut down a scan processor with a signal: %s."	savscand wurde aufgrund eines Signals beendet. sophosmgmtd startet savscand automatisch neu. Keine Maßnahme erforderlich, sofern diese Meldung nicht wiederholt angezeigt wird. Wird die Meldung wiederholt angezeigt, kontaktieren Sie bitte den Sophos Support.	SCANNER-SHUTDOWN-WITH-SIGNAL
"Failed to disinfect %s: too many disinfection attempts."	Sophos Anti-Virus On-Demand-Scanner hat eine Datei nicht desinfiziert. Bitte entfernen Sie diese Datei.	NOTIFY-ONDEMAND-MAX-DISINFECT-ERROR
"Failed to open %s."	Sophos Anti-Virus On-Demand-Scanner kann eine Datei nicht öffnen. Dies kann vorkommen, wenn der Scanner bestimmte Dateien nicht öffnen kann, z. B. Netzwerkdateien. Beachten Sie, dass diese Dateien nicht überprüft wurden.	NOTIFY-ONDEMAND-OPEN-ERROR
"Failed to scan specified path %s."	Bei dem geplanten Sophos Anti-Virus Scan konnte ein explizit angeforderter Pfad nicht überprüft werden. Stellen Sie sicher, dass die Konfiguration des geplanten Scans korrekt ist.	NOTIFY-ONDEMAND-SPECIFIED-PATH-ERROR
"On-demand scan details: master boot records scanned: %s[boot records scanned: %s[files scanned: %s[scan errors: %s[threats detected: %s, infected files detected: %s."	Sophos Anti-Virus hat eine On-Demand-Überprüfung abgeschlossen. Die Ergebnisse sind hier zusammengefasst:	SAVSCAN-DETAILS
"On-demand scan finished."	Sophos Anti-Virus On-Demand-Überprüfung abgeschlossen.	SAVSCAN-FINISHED
"On-demand scan started."	Sophos Anti-Virus On-Demand-Überprüfung begonnen.	SAVSCAN-START

Syslog-Meldung	Beschreibung	Nachrichten-ID
" Scheduled scan \"%s\" started."	Geplanter Sophos Anti-Virus Scan hat begonnen.	SCHEDULED-SCAN-BEGIN
" Scheduled scan \"%s\" completed: master boot records scanned: %s[boot records scanned: %s[files scanned: %s[scan errors: %s[threats detected: %s, infected files detected: %s."	Sophos Anti-Virus hat eine geplante Überprüfung abgeschlossen. Die Ergebnisse sind hier zusammengefasst:	SCHEDULED-SCAN-DETAILS
"Successfully updated Sophos Anti-Virus from %s"	Sophos Anti-Virus wurde erfolgreich aktualisiert.	SUCCESSFULLY_ UPDATED_FROM

14 Anhang: Konfigurieren der Updates

Wichtig
Wenn Sie Sophos Anti-Virus über Sophos Enterprise Console verwalten, müssen Sie die Updates mit Enterprise Console konfigurieren. In der Hilfe zu Enterprise Console wird die Konfiguration von Updates genau beschrieben.

14.1 Grundbegriffe

Update-Server

Unter *Update-Server* ist ein Computer mit Sophos Anti-Virus 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.

14.2 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
```

14.3 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 **Display update configuration**, um die aktuelle Konfiguration anzuzeigen.

14.4 Konfigurieren von Updates für mehrere Clients von Sophos bei Störung des Update-Servers

Hinweis
Wenn Sie die Konfiguration für nur einen Update-Client ändern möchten, lesen Sie bitte den Abschnitt Konfigurieren von Updates für einen Update-Client vom Update-Server(Seite 48).

Auf dem Update-Server nehmen Sie Ihre Änderungen an der Offline-Konfigurationsdatei vor und übertragen die Änderungen auf die Live-Konfigurationsdatei, so dass die Update-Clients für den nächsten Download korrekt konfiguriert sind. Im Folgenden steht *offline-config-file-path* für den Pfad zur Offline-Konfigurationsdatei und *live-config-file-path* für den Pfad zur Live-Konfigurationsdatei.

Verfahren Sie zum Konfigurieren von Updates für mehrere Clients von Sophos bei Störung des Update-Servers wie folgt:

1. Geben Sie als sekundäre Update-Quelle `sophos:` ein. Verwenden Sie hierzu den Parameter SecondaryUpdateSourcePath. Geben Sie z.B. Folgendes ein:
   `/opt/sophos-av/bin/savconfig -f Offline-Konfigurationsdatei -c set SecondaryUpdateSourcePath 'sophos:'`
2. Geben Sie als Benutzernamen für die sekundäre Update-Quelle den in der Lizenz enthaltenen Benutzernamen an. Verwenden Sie hierzu den Parameter SecondaryUpdateUsername. Geben Sie z.B. Folgendes ein:
   `/opt/sophos-av/bin/savconfig -f Offline-Konfigurationsdatei -c set SecondaryUpdateUsername 'cust123'`
3. Geben Sie als Kennwort für die sekundäre Update-Quelle das in der Lizenz enthaltene Kennwort an. Verwenden Sie hierzu den Parameter SecondaryUpdatePassword. Geben Sie z.B. Folgendes ein:
   `/opt/sophos-av/bin/savconfig -f Offline-Konfigurationsdatei -c set SecondaryUpdatePassword 'j23rjjfwj'`
4. Wenn Sie die Verbindung über einen Proxyserver herstellen, legen Sie über die Parameter SecondaryUpdateProxyAddress, SecondaryUpdateProxyUsername und SecondaryUpdateProxyPassword jeweils die Adresse, den Benutzernamen und das Kennwort fest. Geben Sie z.B. Folgendes ein:
   `/opt/sophos-av/bin/savconfig -f Offline-Konfigurationsdatei -c set SecondaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'`
   `/opt/sophos-av/bin/savconfig -f Offline-Konfigurationsdatei -c set SecondaryUpdateProxyUsername 'penelope'`

```
/opt/sophos-av/bin/savconfig -f Offline-Konfigurationsdatei -c set
SecondaryUpdateProxyPassword 'fj202jrjf'
```

5. 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-path live-config-file-path
   ```

   Beispiel:

   ```
   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /opt/sophos-av/extrafiles/LiveConfig.cfg
   ```

14.5 Konfigurieren von Updates für einen Update-Client vom Update-Server

Hinweis

Wenn Sie die Konfiguration für mehrere Update-Clients ändern möchten, lesen Sie bitte den Abschnitt Konfigurieren von Updates für mehrere Clients von Sophos bei Störung des Update-Servers(Seite 47).

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 die Option zur Konfiguration der primären (oder sekundären) Update-Quelle auf Ihrem Server.
   Geben Sie daraufhin die Details der Update-Quelle ein.
3. Geben Sie die Adresse der Update-Quelle und ggf. die Zugangsdaten (Benutzername und Kennwort) ein.

   Sie können entweder eine HTTP-Adresse oder einen UNC-Pfad angeben, je nachdem, wie Sie den Update-Server eingerichtet haben.

   Nun fragt „`savsetup`“, ob die Verbindung zum Update-Server über einen Proxyserver hergestellt werden soll.
4. Wenn dies der Fall ist, drücken Sie „Y“ und geben Sie die entsprechenden Details ein.

15 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
```

16 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 14).

16.1 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.

16.2 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.

16.3 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.

16.4 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 Verzeichnisses oder einer Datei(Seite 4).

16.5 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.

16.6 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 keine exakte Viren-Entsprechung findet, können Viren-Fragmente nicht beseitigt werden.

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.

16.7 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-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 10).
3. Wenn Viren-Fragmente immer noch gemeldet werden, wenden Sie sich bitte an den technischen Support von Sophos.

17 Glossar

Zentrales Installationsverzeichnis (CID)	Netzwerkfreigabe, in der Sophos Sicherheitssoftware und Updates bereitgestellt werden. Netzwerkcomputer beziehen ihre Updates über dieses Verzeichnis.
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.
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.
Geplanter Scan	Ein vollständiger oder teilweiser Scans eines Computers zu festgesetzten Zeiten.
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.
Update-Client	Ein Computer, auf dem Sophos Anti-Virus installiert ist, der anderen Computern nicht als Update-Quelle dient.
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.

18 Technischer Support

Technischen Support zu Sophos Produkten finden Sie hier:

- Besuchen Sie die Sophos Community unter community.sophos.com/ und suchen Sie nach Benutzern mit dem gleichen Problem.
- Durchsuchen Sie die Sophos Support-Knowledgebase von Sophos unter www.sophos.com/de-de/support.aspx.
- Laden Sie die Produktdokumentation herunter von 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.

19 Rechtlicher Hinweis

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

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

curl

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2014, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

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

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

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

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.

All rights reserved.

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

Copyright © 1995–2013 Jean-loup Gailly and Mark Adler

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.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

Index

U

V

Z