SOPHOS

Cybersecurity made simple.

Sophos for Virtual Environments

Konfigurationsanleitung für Benutzer mit Enterprise Console

Inhalt

1 Einleitung

Diese Anleitung beschreibt die Konfiguration von Sophos for Virtual Environments.

Dabei wird vorausgesetzt, dass Sie Sophos Enterprise Console für die Verwaltung Ihrer Sicherheitssoftware verwenden.

Hinweis
Falls Sie Sophos Central verwenden, lesen Sie stattdessen in der Konfigurationsanleitung – Sophos Central Edition nach.

2 Konfigurieren von Richtlinien

Sie können Sophos for Virtual Environments mithilfe von Sophos Enterprise ConsoleRichtlinien konfigurieren.

Wenn Sie Ihr Sophos Security VM einer Sophos Enterprise Console-Gruppe zuweisen, werden Richtlinien zum Schutz und zur Aktualisierung der VM-Gastsysteme angewendet.

Es empfiehlt sich, die Standardeinstellungen zu übernehmen, da so das optimale Verhältnis von Schutz und Systemleistung gewährleistet ist. Sie können jedoch die Einstellungen in folgenden Richtlinien ändern:

- Antivirus und HIPS
- Updates

Die anderen Sophos Enterprise Console-Richtlinien gelten nicht für das Sophos Security VM.

Hinweis
Alle VM-Gastsysteme, die durch ein Sophos Security VM geschützt sind, wenden dieselben Richtlinien wie das Sophos Security VM an. Um auf bestimmte VM-Gastsysteme eine andere Richtlinie anzuwenden, weisen Sie diese einem anderen Sophos Security VM in einer anderen Sophos Enterprise Console-Gruppe zu. Wenden Sie dann eine andere Richtlinie auf diese Gruppe an. Hinweise zur Neuzuweisung von VM-Gastsystemen finden Sie in der Kurzanleitung zu Sophos for Virtual Environments – Enterprise Console Edition.

Informationen darüber, wie Sie eine Liste aller von einem Sophos Security VM verwalteten VM-Gastsysteme anzeigen können, finden Sie unter Anzeigen geschützter VM-Gastsysteme (Seite 10).

2.1 Antivirus- und HIPS-Richtlinie

Standardmäßig führt das Sophos Security VM Folgendes aus:

- Überprüfen von Dateien, wenn über die VM-Gastsysteme darauf zugegriffen wird.
- Sperren des Zugriffs auf infizierte Dateien.
- Automatische Entfernung erkannter Bedrohungen.

Für das Sophos Security VM gelten nicht alle Einstellungen der Antivirus- und HIPS-Richtlinie. In diesem Abschnitt ist beschrieben, welche Scanoptionen verfügbar sind und zentral konfiguriert werden können.

Nähere Informationen zu den Einstellungen finden Sie in der Hilfe zu Sophos Enterprise Console.

On-Access-Scans

Einstellungen für On-Access-Scans werden wie unten beschrieben unterstützt. Die Verhaltensüberwachung wird nicht unterstützt.

So gelangen Sie in Sophos Enterprise Console zu den Einstellungen für On-Access-Scans:

1. Doppelklicken Sie im Fensterbereich **Richtlinien** auf **Antivirus und HIPS**.
2. Doppelklicken Sie dann auf die Richtlinie, die Sie ändern möchten.

3. Gehen Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** zum Fensterbereich **On-Access-Scans**. Klicken Sie neben **On-Access-Scans aktivieren** auf **Konfigurieren**.

   Das Dialogfeld **On-Access-Scan-Einstellungen** wird angezeigt.

Die auf den Registerkarten verfügbaren Optionen werden unten angezeigt.

Scans	Unterstützt	Hinweise
Dateien prüfen beim Lesen/ Umbenennen/Schreiben	Nein	Wenn mindestens eine der Optionen aktiviert ist, scannt Sophos Security VM in allen drei Szenarien. Sind alle drei Optionen deaktiviert, ist Ihr System nicht geschützt.
Überprüfen auf Adware und PUA/ verdächtige Dateien	Nein	
Zugriff auf Laufwerke mit infizierten Bootsektoren erlauben	Nein	
Archivdateien scannen (nicht empfohlen)	Ja	
Scannen des Systemspeichers	Nein	

Erweiterungen	Unterstützt?
Alle Dateien scannen (nicht empfohlen)	Ja
Nur ausführbare und anfällige Dateien scannen	Ja
Weitere zu scannende Dateitypen	Ja
Dateien ohne Erweiterung scannen	Ja
Ausschließen von Dateitypen von der Überprüfung	Ja

Ausschlüsse	Unterstützt	Hinweise
Registerkarte **Windows-Ausschlüsse**	Ja	Um einen Ordner auszuschließen, müssen Sie den vollständigen Pfad einschließlich Laufwerksbuchstabe oder Name der Netzwerkfreigabe angeben, zum Beispiel: „`C:\Tools\logs\`“ oder „`\\Server\Tools\logs\`“. Mehr Informationen finden Sie im Abschnitt zur Konfiguration der Antivirus- und HIPS-Richtlinie in der Hilfe zu Sophos Enterprise Console.
Registerkarte **Mac-Ausschlüsse**	Nein	

Ausschlüsse	Unterstüt	Hinweise
Registerkarte **Linux-/UNIX-Ausschlüsse**	Nein	

Bereinigung	Unterstüt ?	Hinweise
Entfernen von Viren/Spyware	Ja	Die alternativen Aktionen werden ausgeführt, wenn die Bereinigung fehlschlägt. Das Sophos Security VM verweigert immer den Zugriff auf infizierte Elemente.
Entfernen verdächtiger Dateien	Nein	

Weitere Informationen zu den Einstellungen und deren Auswahl finden Sie in der Hilfe zu Sophos Enterprise Console.

Geplante Scans

So konfigurieren oder bearbeiten Sie einen geplanten Scan:

- Gehen Sie im Dialogfeld **Antivirus- und HIPS-Richtlinie** zum Fensterbereich **Geplante Scans**.
- Klicken Sie auf **Hinzufügen** oder **Bearbeiten**.

Sie können auch weitere Dateitypen festlegen, die gescannt werden sollen, oder Elemente von der Überprüfung ausnehmen, indem Sie auf **Erweiterungen und Ausschlüsse** klicken.

Einstellungen für geplante Scans werden wie unten beschrieben unterstützt. **Hinzufügen/ BearbeitenEinstellungen für geplante Scans**.

Einstellungen für geplante Scans	Unterstützt	Hinweise
Lokale Festplatten	Ja	
Diskettenlaufwerke und Wechsellaufwerke	Ja	
CD-Laufwerke	Ja	
Wann findet die Überprüfung statt	Ja	Das Sophos Security VM startet die Überprüfung zum geplanten Zeitpunkt, jedoch werden immer nur zwei VM-Gastsysteme auf einmal überprüft, damit die Leistung Ihres Systems nicht beeinträchtigt wird.

Hinzufügen/BearbeitenEinstellungen für geplante ScansKonfigurierenEinstellungen zu Scans und Bereinigung

Scans und Bereinigung	Unterstüt	Hinweise
Registerkarte **Scans**		

Scans und Bereinigung	Unterstüt	Hinweise
Dateien auf Adware und PUA/ verdächtige Dateien/Rootkits scannen	Nein	
Scannen von Archivdateien	Ja	
Scannen des Systemspeichers	Nein	Der Systemspeicher wird standardmäßig überprüft. Sie können diese Option nicht konfigurieren.
Scannen mit niedriger Priorität	Nein	
Registerkarte **Bereinigung**		
Entfernen von Viren/Spyware	Ja	Das Sophos Security VM bereinigt nicht automatisch Diskettenlaufwerke, CD-Laufwerke oder Netzwerkverzeichnisse. Aktionen für infizierte Elemente wirken sich – wenn keine Bereinigung stattgefunden hat – nicht aus. Das Sophos Security VM protokolliert immer das Ereignis, wenn keine Bereinigung stattgefunden hat.
Entfernen von Adware und PUA	Nein	
Entfernen verdächtiger Dateien	Nein	

Erweiterungen und AusschlüsseErweiterungen und Ausschlüsse für geplante Scans.

Erweiterungen und Ausschlüsse	Unterstüt	Hinweise
Registerkarte **Erweiterungen**		
Alle Dateien scannen (nicht empfohlen)	Ja	
Nur ausführbare und anfällige Dateien scannen	Ja	
Weitere zu scannende Dateitypen	Ja	
Dateien ohne Erweiterung scannen	Ja	
Ausschließen von Dateitypen von der Überprüfung	Ja	
Registerkarte **Ausschlüsse**		

Erweiterungen und Ausschlüsse	Unterstüt	Hinweise
Registerkarte **Windows-Ausschlüsse**	Ja	Um einen Ordner auszuschließen, müssen Sie den vollständigen Pfad einschließlich Laufwerksbuchstabe oder Name der Netzwerkfreigabe angeben, zum Beispiel: `C:\Tools\logs\` oder `\\Server\Tools\logs\`. Nähere Informationen entnehmen Sie bitte der Sophos Enterprise Console Hilfe.
Registerkarte **Mac-Ausschlüsse**	Nein	
Registerkarte **Linux-/UNIX-Ausschlüsse**	Nein	

Sophos Live-Schutz

Verdächtige Dateien werden durch Abgleich mit aktuellen Malware-Daten in der SophosLabs-Datenbank überprüft.

Option	Unterstützt?
Live Protection aktivieren	Ja
Live Protection für On-Demand-Scans aktivieren	Ja
Dateisamples automatisch an Sophos senden	Nein

Internetschutz

Wird nicht unterstützt.

Autorisierung

Die Autorisierung sowie die Erkennung von Adware und anderen potenziell unerwünschten Anwendungen (PUAs) werden nicht unterstützt.

Benachrichtigung

Es werden nur E-Mail-Benachrichtigungen unterstützt.

2.1.1 Überprüfte Dateierweiterungen

Dateien mit den folgenden Erweiterungen werden standardmäßig überprüft.

386	docx	jpz	pl	vlx
3gr	dot	js	pot	vs?
add	drv	jse	pps	vxd
ani	eml	lnk	ppt	wbk
asp	exe	lsp	pptm	wma
aspx	fas	mnl	pptx	wmf
asx	flt	mod	prc	wsf
bat	fon	mpd	ps1	xl?
cab	fot	mpp	psm1	xlsm
chm	hlp	mpt	rtf	xlsx
class	ht?	mso	scr	xsn
cmd	hta	mui	sh	zip
com	html	nws	shb	zipx
cpl	i13	o	shs	
dbx	ifs	ocx	src	
dex	inf	ov?	swf	
dll	ini	pdf	sys	
dmd	jar	pdr	tif	
doc	jpeg	php	tiff	
docm	jpg	pif	vb?	

Die folgenden Erweiterungen werden standardmäßig überprüft, wenn die Option **Archivdateien scannen** in der Antivirus- und HIPS-Richtlinie für die Security VM aktiviert ist.

7z	lha
7zip	lzh
??_	rar
a	rpm
arj	tar
bin	taz
bz2	tbz
gz	tbz2
hqx	tgz
hxs	uue
	z

Sie können weitere Erweiterungen hinzufügen, die überprüft werden sollen, oder Erweiterungen von der Überprüfung ausschließen. Die Vorgehensweise ist im Abschnitt zum Konfigurieren der Antivirus- und HIPS-Richtlinie der Hilfe zu Sophos Enterprise Console beschrieben.

2.2 Update-Richtlinie

Für das Sophos Security VM gelten alle Einstellungen in der Sophos Enterprise Console Update-Richtlinie.

Weitere Informationen finden Sie in der Hilfe zu Sophos Enterprise Console unter **Computer updatenKonfigurieren der Update-Richtlinie**.

3 Überprüfen, ob VM-Gastsysteme geschützt sind

In diesem Abschnitt erfahren Sie, wie Sie überprüfen, ob Ihre VM-Gastsysteme geschützt sind. Sie haben folgende Möglichkeiten:

- Überprüfen der Schutzeinstellungen auf einem VM-Gastsystem.
- Testen der Echtzeit-Scan-Funktion auf einem VM-Gastsystem.
- Probleme mit Echtzeit-Scans lösen.

3.1 Überprüfen der Schutzeinstellungen

So überprüfen Sie, ob ein VM-Gastsystem geschützt ist:

1. Gehen Sie zu dem VM-Gastsystem und suchen Sie nach **Sicherheit und Wartung** im Startmenü. Falls Sie diese Option nicht finden, suchen Sie nach **Info-Center**.

   Achtung
   Wenn Sie keine dieser Optionen finden, gibt es für das VM-Gastsystem kein Windows Sicherheitscenter. Überprüfen Sie mithilfe der unter Testen der Echtzeit-Scanfunktion (Seite 8) beschriebenen Schritte, ob das VM-Gastsystem geschützt ist.

2. Klicken Sie auf den Dropdown-Pfeil neben **Sicherheit**. Es sollte angezeigt werden, dass Sophos for Virtual Environments aktiviert ist.

   Hinweis
   Sollte dies nicht der Fall sein, lesen Sie unter Beheben von Problemen mit On-Access-Scans (Seite 9) nach.

3.2 Testen der Echtzeit-Scanfunktion

Echtzeit-Scans sind der Hauptmechanismus zum Schutz vor Threats. Bei jedem Versuch, eine Datei zu öffnen, zu verschieben oder umzubenennen oder in eine Datei zu schreiben, scannt das Sophos Security VM die Datei. Der Zugriff wird nur erlaubt, wenn die Datei keine Bedrohung darstellt. Wenn Sie ein Programm ausführen, scannt das Sophos Security VM die exe-Datei und alle anderen Dateien, die von ihr geladen werden.

Wichtig
Stellen Sie sicher, dass Sophos Endpoint für Windows nicht auf Gastsystemen installiert ist, die mit einem Sophos Security VM geschützt werden.

So prüfen Sie, ob eine Security VM Dateien bei Zugriff scannt:

1. Gehen Sie zu http://2016.eicar.org/86-0-Intended-use.html und verwenden Sie die EICAR-Testzeichenfolge. Kopieren Sie die EICAR-Testzeichenfolge in eine neue Datei. Geben Sie der Datei einen Namen mit der Erweiterung „.com“ und speichern Sie sie auf einem der VM-Gastsysteme.
2. Versuchen, Sie auf einem VM-Gastsystem auf die Datei zuzugreifen.
3. Doppelklicken Sie in Sophos Enterprise Console in der Computerliste im unteren Fensterbereich auf **Status**.
4. Suchen Sie in der Computerliste nach dem Sophos Security VM.
    - Wenn Sie die automatische Bereinigung aktiviert haben, doppelklicken Sie auf das Sophos Security VM, um die **Computerdetails** zu öffnen. Im Abschnitt „Verlauf“ sollte Ihnen angezeigt werden, dass die EICAR-Datei erkannt und bereinigt wurde.
    - Wenn Sie die automatische Bereinigung nicht aktiviert haben, sollte Ihnen in der Spalte **Alerts und Fehler** ein Alert angezeigt werden. Rechtsklicken Sie auf das Sophos Security VM. Unter **Alerts und Fehler löschen** sollte angezeigt werden, dass EICAR erkannt, jedoch nicht bereinigt wurde.

Wenn die EICAR-Datei nicht erkannt wurde, lesen Sie unter Beheben von Problemen mit On-Access-Scans (Seite 9) nach. Falls die EICAR-Datei nicht entfernt wurde, löschen Sie sie einfach.

3.3 Beheben von Problemen mit On-Access-Scans

Wenn On-Access-Scans nicht funktionieren:

1. Stellen Sie sicher, dass sich das Sophos Security VM in einer Gruppe befindet, deren Virenschutzrichtlinie vorgibt, dass On-Access-Scans aktiviert werden:
    a) Rechtsklicken Sie in Sophos Enterprise Console unter **Gruppen** auf die Gruppe mit dem Sophos Security VM und wählen Sie die Option **Gruppenrichtliniendetails anzeigen/ bearbeiten**. Überprüfen Sie, welche Anti-Virus- und HIPS-Richtlinie genutzt wird.
    b) Doppelklicken Sie unter **Richtlinien** auf **Antivirus und HIPS**.
    c) Doppelklicken Sie auf die von der Gruppe mit dem Sophos Security VM verwendete Richtlinie.
    d) Stellen in **On-Access-Scans** sicher, dass die Option **On-Access-Scans aktivieren** ausgewählt ist. Klicken Sie auf **OK**.
    e) Rechtsklicken Sie in der Computerliste auf das Sophos Security VM und wählen Sie die Option **Konformität mit**. Wählen Sie anschließend die Option **Antivirus- und HIPS-Gruppenrichtlinie**.
    f) Prüfen Sie, ob das Sophos Security VM als konform mit der Richtlinie angezeigt wird.
2. Stellen Sie sicher, dass das VM-Gastsystem geschützt ist. Gehen Sie zum Host des Sophos Security VM und schauen Sie in der Protokolldatei nach.
3. Stellen Sie sicher, dass im Windows Sicherheitscenter das VM-Gastsystem als von Sophos for Virtual Environments geschützt angezeigt wird.
4. Vergewissern Sie sich, dass keine Neustarts durch Microsoft-Updates ausstehen. Diese können verhindern, dass die Installation des Sophos Guest VM Agent abgeschlossen werden kann.
5. Vergewissern Sie sich, dass keine anderen Virenschutzprodukte installiert sind. Vergewissern Sie sich auf Serverplattformen, auf denen es kein Sicherheitscenter gibt, das Windows Defender nicht aktiv ist. Denken Sie daran, dass Sie mit Sophos for Virtual Environments keine VM-Gastsysteme schützen können, auf denen andere Virenschutzprodukte ausgeführt werden.
6. Wenn On-Access-Scans weiterhin nicht funktionieren, wenden Sie sich bitte an den technischen Support von Sophos.

4 Anzeigen geschützter VM-Gastsysteme

Sie können alle VM-Gastsysteme anzeigen, die durch ein Sophos Security VM geschützt sind.

1. Gehen Sie zu dem Sophos Security VM. Sie benötigen dazu den Windows Explorer und die IP-Adresse.
2. Doppelklicken Sie auf die Freigabe **Protokolle**.
3. Geben Sie bei Aufforderung Ihre Anmeldedaten ein.
   - Der Benutzername lautet „sophos“.
   - Das Kennwort ist das Zugangskennwort, das Sie bei der Installation des Sophos Security VM festgelegt haben.
4. Öffnen Sie **ProtectedGVMs.log**, um die geschützten VM-Gastsysteme anzuzeigen.

Hinweis
Die Datei ProtectedGVMs.log wird erst ab dem Moment angezeigt, ab dem das Sophos Security VM die VM-Gastsysteme schützt.

5 Überprüfen von VM-Gastsystemen

Sophos for Virtual Environments überprüft Dateien beim Zugriff, d. h. wenn sie geöffnet und geschlossen werden (sofern On-Access-Scans in Ihrer Richtlinie aktiviert sind).

Ein Sophos Security VM kann zudem einen vollständigen Scan aller von ihm verwalteten VM-Gastsysteme durchführen. Sie können entweder einen Scan sofort oder zu bestimmten Zeiten ausführen.

Bei der vollständigen Überprüfung werden Threats erkannt, aber nicht entfernt.

Hinweis
Das Sophos Security VM kann keine Überprüfung ausführen, wenn es sich noch in der Gruppe **Nicht zugewiesen** in Sophos Enterprise Console befindet. Es muss sich in einer Gruppe befinden, auf die Sie Richtlinien übertragen haben.

Hinweis
Das Sophos Security VM plant Scans zeitlich so, dass der Hypervisor nicht zu sehr ausgelastet wird. Standardmäßig werden zwei VM-Gastsysteme gleichzeitig überprüft. Die Überprüfung einer größeren Anzahl von VM-Gastsystemen kann einige Zeit dauern.

- So können Sie je nach Bedarf eine vollständige Überprüfung aller VM-Gastsysteme durchführen:
  a) Wechseln Sie zu Sophos Enterprise Console und suchen Sie in der Computerliste nach dem Sophos Security VM.
  b) Klicken Sie mit der rechten Maustaste auf das Sophos Security VM und wählen Sie **Vollständige Systemüberprüfung**.

  Tipp
  Sie können aber auch im Menü **Maßnahmen** die Option **Vollständige Systemüberprüfung** wählen.

- So führen Sie eine vollständige Überprüfung aller VM-Gastsysteme zu festen Zeiten aus:
  a) Gehen Sie zu Sophos Enterprise Console.
  b) Erstellen Sie einen geplanten Scan. Entsprechende Anweisungen hierzu finden im Abschnitt zum Konfigurieren der Antivirus- und HIPS-Richtlinie der Sophos Enterprise Console Hilfe.
- So zeigen Sie die Details des Scans nach dessen Ausführung an:
  a) Doppelklicken Sie in Sophos Enterprise Console in der Computerliste im unteren Fensterbereich auf das Sophos Security VM, damit die **Computerdetails** angezeigt wird.

6 Informationen zu einem Threat

Verfahren Sie wie folgt, um mehr über einen Threat und dessen Handhabung zu erfahren:

1. Doppelklicken Sie in Sophos Enterprise Console in der Computerliste im unteren Fensterbereich auf das Sophos Security VM, damit die **Computerdetails** angezeigt wird.
   Im Abschnitt **Verlauf** sind **Erkannte Objekte** aufgeführt. Den Namen des Threats finden Sie unter **Name**, und das betroffene VM-Gastsystem und die betroffene Datei unter **Details**.
2. Klicken Sie auf den Namen des Threat.
   Sie werden mit der Sophos Website verbunden. Hier finden Sie eine Beschreibung des Objekts und Hinweise zu den zu ergreifenden Gegenmaßnahmen.

7 Entfernen eines Threat

Das Sophos Security VM kann Threats automatisch entfernen, oder Sie entfernen diese manuell.

7.1 Automatische Bereinigung

Das Sophos Security VM kann erkannte Bedrohungen automatisch entfernen.

Hinweis
Die automatische Bereinigung ist nicht möglich bei CDs oder anderen schreibgeschützten Dateisystemen und Medien oder auf Remote-Dateisystemen.

Was geschieht bei einer automatischen Bereinigung?

Wenn eine Bedrohung erkannt und automatisch bereinigt wird, führt Sophos Enterprise Console folgende Aktionen aus:

- Zeigt an, dass der Threat gesperrt wurde (siehe Abschnitt „Verlauf“ im unter **Computerdetails**).
- Zeigt einen Alert an, der darüber informiert, welche Art von Threat vorliegt und ob dieser entfernt werden kann.
- Der Alert wird nach erfolgreicher Bereinigung ausgeblendet. Schlägt die Bereinigung fehl, erscheint bei dem Threat der Hinweis „Keine Bereinigung möglich“.

Es kann sein, dass ein VM-Gastsystem neu gestartet werden muss, um die Bereinigung abzuschließen. In diesem Fall wird die Meldung „Neustart erforderlich“ für das Sophos Security VM angezeigt. Um herauszufinden, auf welches VM-Gastsystem sich der Warnhinweis bezieht, doppelklicken Sie auf das Sophos Security VM, um **Computerdetails** zu öffnen und die Beschreibung des Alerts unter **Ausstehende Alerts und Fehler** zu lesen.

7.2 Manuelle Bereinigung

Sie können eine Bedrohung manuell entfernen.

Sie müssen den Alert nach dem Entfernen der Bedrohung aus Sophos Enterprise Console löschen.

7.2.1 Bereinigen eines VM-Gastsystems

Für eine manuelle Bereinigung muss das VM-Gastsystem wiederhergestellt werden. Beachten Sie, dass dabei Ihre Daten verloren gehen. Wenden Sie eine der folgenden Methoden an:

- Stellen Sie auf dem betroffenen VM-Gastsystem den letzten bekanntermaßen threatfreien Snapshot wieder her.
- Löschen Sie das betroffene VM-Gastsystem und klonen Sie es erneut über das Vorlagenimage.

Stellen Sie sicher, dass für das Vorlagenimage die erforderlichen Sophos-Tools installiert wurden (siehe Kurzanleitung zu Sophos for Virtual Environments für Benutzer mit Enterprise Console).

Ganz gleich, welche Methode Sie anwenden, führen Sie anschließend eine vollständige Überprüfung des VM-Gastsystems aus, um sicherzustellen, dass es virenfrei ist.

7.2.2 Löschen eines Alerts in Sophos Enterprise Console

Wenn Sie sich sicher sind, dass das betroffene VM-Gastsystem threatfrei ist, können Sie den Alert in Sophos Enterprise Console löschen:

1. Klicken Sie in Sophos Enterprise Console in der Computerliste im unteren rechten Fensterbereich mit der rechten Maustaste auf das Sophos Security VM und wählen Sie die Option **Alerts und Fehler löschen**.
2. Wählen Sie unter **Alerts und Fehler löschen** auf der Registerkarte **Alerts** den Alert aus und klicken Sie auf **Löschen**.

Der Alert wird nicht mehr in Sophos Enterprise Console angezeigt.

8 Alerts

In diesem Abschnitt sind die Alerts (Warnhinweise) beschrieben, die das Sophos Security VM sendet, wenn Bedrohungen festgestellt bzw. entfernt wurden.

Warnhinweise zu Bedrohungen

Wenn das Sophos Security VM eine Bedrohung auf einem VM-Gastsystem erkennt, sehen Sie diese Alerts in Sophos Enterprise Console:

- Alerts werden im Dashboard angezeigt.
- Ein rotes Warnsymbol wird in der Computerliste auf der Registerkarte **Status** neben dem Sophos Security VM unter **Alerts und Fehler** angezeigt.

Wird die Bedrohung automatisch entfernt, wird der entsprechende Alert aus Sophos Enterprise Console gelöscht.

Um herauszufinden, auf welches VM-Gastsystem sich der Alert bezieht, doppelklicken Sie in der Computerliste auf das Sophos Security VM. Lesen Sie bei **Computerdetails** unter **Ausstehende Alerts und Fehler** die Beschreibung des Alerts. Dort ist das betroffene VM-Gastsystem angegeben, gefolgt vom Pfad der Bedrohung:

```
Computername(IP-Adresse)/C:\threat.exe
```

Erkennt das Sophos Security VM beim Versuch des Benutzers, auf eine Datei zuzugreifen, eine Bedrohung, wird unter Umständen auch eine Meldung auf dem VM-Gastsystem angezeigt, die den Benutzer darüber informiert, dass kein Zugriff auf die Datei möglich ist. Dies hängt von der jeweiligen Anwendung ab, über die auf die Datei zugegriffen wird.

Alerts nach der Bereinigung

Wurde die Bedrohung entfernt, wird der entsprechende Alert aus Sophos Enterprise Console gelöscht.

Die Bereinigung wird in Sophos Enterprise Console auch in einem Report festgehalten. Um sich den Report anzeigen zu lassen, doppelklicken Sie in der Computerliste auf das Sophos Security VM, um **Computerdetails** zu öffnen, und suchen Sie nach **Verlauf**.

Wenn der Threat nur teilweise entfernt wurde und das VM-Gastsystem neu gestartet werden muss, um den Bereinigungsvorgang abzuschließen, wird die Meldung „Neustart erforderlich“ angezeigt.

9 Protokolle

Sie können Protokolle auf einer VM-Gastsystem anzeigen.

Auf einem VM-Gastsystem werden die Protokolle in das Windows Application Ereignisprotokoll geschrieben. Sie finden das Protokoll unter **Anwendungs- und Dienstprotokolle > SophosSVE**.

Auf einem Sophos Security VM können Sie die Protokolle aus dem freigegebenen Protokollverzeichnis aufrufen. Verfahren Sie hierzu wie folgt:

1. Öffnen Sie eine Konsole für das Sophos Security VM.
2. Melden Sie sich an:
   - Der Benutzername lautet „sophos“.
   - Das Kennwort ist das Zugangskennwort, das Sie bei der Installation des Sophos Security VM festgelegt haben.
3. Geben Sie folgendes Kommando ein: `sudo /opt/sophox/logcollector/diagnose`.
4. Geben Sie das Zugriffskennwort ein, wenn Sie dazu aufgefordert werden. (Dies kann bis zu einer Minute dauern.)
5. Im Windows Explorer können Sie jetzt auf die Protokolle unter `\\<SVM-IP-Address>\logs\logs.tgz` zugreifen. Geben Sie Ihre Zugangsdaten ein, wenn Sie dazu aufgefordert werden.
   - Der Benutzername lautet „sophos“.
   - Das Kennwort ist das Zugangskennwort, das Sie bei der Installation des Sophos Security VM festgelegt haben.

Nähere Informationen zu Protokollierung in Sophos Enterprise Console finden Sie in der Sophos Enterprise Console Hilfe.

10 Deinstallieren des Sophos Security VM

Stellen Sie zuvor sicher, dass die VM-Gastsysteme weiterhin geschützt sind. Gehen Sie zu dem Sophos Security VM und rufen Sie Anzeigen geschützter VM-Gastsysteme (Seite 10) auf. Weisen Sie dann die VM-Gastsysteme einem anderen Sophos Security VM mit ähnlichen Richtlinieneinstellungen zu.

Um ein Sophos Security VM zu deinstallieren, muss es gelöscht werden.

So weisen Sie Ihre VM-Gastsysteme neu zu:

1. Deinstallieren Sie den Sophos Guest VM Agent (siehe Deinstallieren des Sophos Guest VM Agent).
2. Installieren Sie den Sophos Guest VM Agent mit der neuen IP-Adresse für das Sophos Security VM neu.

Sobald Sie die VM-Gastsysteme verschoben haben, können Sie das Sophos Security VM löschen. Verfahren Sie hierzu wie folgt:

3. Gehen Sie zu Ihrem Hypervisor.
4. Schalten Sie das Sophos Security VM aus.
5. Löschen Sie das VM-System.

11 Deinstallieren des Sophos Guest VM Agent

Sie können den Sophos Guest VM Agent über die Systemsteuerung löschen.

1. Öffnen Sie auf dem VM-Gastsystem die **Systemsteuerung**.
2. Klicken Sie auf **Programme und Funktionen**.
3. Wählen Sie die folgenden Funktionen aus und klicken Sie auf **Deinstallieren**:
   - Sophos for Virtual Environments
   - Sophos Guest VM Scanning Service
   - Sophos Virus Removal Tool.

12 Anhang: Security VMs für die Migration von VM-Gastsystemen hinzufügen

Sie können jederzeit weitere Security VMs hinzufügen, um migrierende VM-Gastsysteme zu schützen

Wenn Sie in Zukunft weitere Sophos Security VMs erstellen möchten, sollten Sie IP-Adressen für die Sophos Security VMs reservieren, die Sie wahrscheinlich hinzufügen werden. Erstellen Sie dazu eine vorab aufgefüllte Master-Version dieser Datei. Diese Datei sollte alle IP-Adressen der Sophos Security VMs enthalten, die Sie haben und die Sie in der Zukunft haben werden. Sie können diese Datei dann in jede Sophos Security VM kopieren, wenn Sie sie erstellen.

Wichtig
Sie müssen diese Schritte auf dem Sophos Security VM, das Sie hinzufügen möchten, und auf den vorhandenen Security VMs ausführen.

1. Öffnen Sie eine Konsole für das Sophos Security VM.
2. Melden Sie sich an:

   Der Benutzername lautet „sophos“.

   Das Kennwort ist das Zugangskennwort, das Sie bei der Installation des Sophos Security VM festgelegt haben.
3. Öffnen Sie die Konfigurationsdatei additional_svms.txt zur Bearbeitung, indem Sie folgenden Befehl ausführen: `sudo vi /opt/sophos-svms/etc/additional_svms.txt`
4. Bearbeiten Sie die Datei um IP-Adressen der Security VMs hinzuzufügen oder zu entfernen, die zum Schutz von zu migrierenden VM-Gastsystemen zur Verfügung stehen. Geben Sie eine IP-Adresse pro Zeile ohne zusätzliche Trennzeichen an.

   a) Drücken Sie `i` um den Bearbeitungsmodus in vi zu öffnen.

   b) Schreiben Sie eine IP-Adresse pro Zeile und verwenden Sie keine Trennzeichen. Zum Beispiel:

      1.2.3.4
      5.6.7.8

   c) Sie müssen die IP-Adresse des Sophos Security VM, an das Sie derzeit angemeldet sind, nicht angeben.

   d) Drücken Sie `Esc` um den Bearbeitungsmodus in vi zu verlassen.

   e) Speichern und schließen Sie die Datei durch Eingeben von `:wq`.
5. Überprüfen Sie unter `/var/log/ssvm.log`, ob beim Verarbeiten der Liste mit den zusätzlichen Security VMs Fehler aufgetreten sind.

   Sind keine Fehler aufgetreten, wird die aktualisierte Liste an alle verbundenen VM-Gastsysteme gesendet, so dass sie durch die neuen Security VMs geschützt sind.

13 Anhang: Hinzufügen von CPUs für das Sophos Security VM

Wenn sich eine große Anzahl an VM-Gastsystemen auf einem Host befindet, müssen Sie sicherstellen, dass das Sophos Security VM über ausreichend Rechenleistung zum Scannen der Dateien beim Start verfügt.

Fügen Sie hierzu mehr CPUs für das Sophos Security VM hinzu. Dies können Sie jederzeit tun.

Hinweis
Wenn Sie CPUs hinzufügen, nachdem Sie das Sophos Security VM einer Computergruppe in Sophos Enterprise Console hinzugefügt haben, sollten Sie warten, bis das Sophos Security VM die Gruppenrichtlinie erfüllt.

Je nach Art der Last kann durch das Hinzufügen von CPUs auch die Systemleistung insgesamt verbessert werden.

CPUs in VMware ESXi hinzufügen

Fügen Sie CPUs wie folgt hinzu:

1. Schalten Sie das Sophos Security VM aus.
2. Wählen Sie in vSphere Client das Sophos Security VM aus.
3. Wählen Sie **Edit SettingsHardwareCPUs.** Geben Sie dann die Anzahl der CPUs an.

CPUs in Microsoft Hyper-V hinzufügen

Fügen Sie CPUs wie folgt hinzu:

1. Klicken Sie auf **Start**, wählen Sie **Verwaltung** und klicken Sie dann auf **Hyper-V-Manager**.
2. Wählen Sie im Ergebnisbereich unter **Virtuelle Computer** das Sophos Security VM aus.
3. Klicken Sie im Bereich **Aktion** unter dem Namen des virtuellen Computers auf **Einstellungen**.
4. Klicken Sie auf **Prozessor** und geben Sie die Anzahl von Prozessoren ein.

14 Technische Unterstützung

Technische Unterstützung zu Sophos-Produkten erhalten Sie auf folgende Weise:

- Tauschen Sie sich in der Sophos Community unter community.sophos.com/ mit anderen Benutzern aus, die dasselbe Problem haben.
- Durchsuchen Sie die Wissensdatenbank des Sophos Support unter www.sophos.com/de-de/support.aspx.
- Lesen Sie die Produktdokumentation unter www.sophos.com/de-de/support/documentation.aspx.
- Stellen Sie eine Support-Anfrage unter https://secure2.sophos.com/support/contact-support/support-query.aspx.

15 Rechtliche Hinweise

Dritt-Lizenzen

Drittlizenzen für die Nutzung dieses Produkts finden Sie in folgendem Ordner im Sophos VM-Sicherheitssystem: `/usr/share/doc`.

Für einige Softwareprogramme wird Benutzern gemäß GNU General Public License (GPL) oder ähnlichen Lizenzen für kostenlose Software eine Lizenz oder Unterlizenz gewährt, die ihnen unter anderem das Recht geben, bestimmte Programme oder Teile von Programmen zu kopieren, zu verändern oder weiterzuverbreiten und Zugriff auf den Quellcode geben. Die GLP bestimmt, dass für unter der GLP lizenzierte Software, die an Benutzer in einem ausführbaren Binärformat verteilt wird, diesen Benutzern der Quellcode ebenfalls zur Verfügung gestellt werden muss. Für Software, die zusammen mit diesem Sophos-Produkt vertrieben wird, kann der Quellcode per E-Mail bei Sophos angefordert werden: savlinuxgpl@sophos.com.