SOPHOS

Cybersecurity made simple.

Sophos for Virtual Environments

Konfigurationsanleitung – Enterprise Console Edition

Inhalt

Einleitung 1
Konfigurieren von Richtlinien 2
    Antivirus- und HIPS-Richtlinie 2
    Update-Richtlinie 6
Anzeigen geschützter VM-Gastsysteme 8
Überprüfen von VM-Gastsystemen 9
Informationen zu einem Threat 10
Entfernen eines Threat 11
    Automatische Bereinigung 11
    Manuelle Bereinigung 11
Anhang: VM-Sicherheitssysteme für die Migration von VM-Gastsystemen hinzufügen 13
Alerts 14
Protokolle 15
Technischer Support 16
Rechtliche Hinweise 17

1 Einleitung

Diese Anleitung beschreibt die Konfiguration von Sophos für 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 für Virtual Environments mithilfe von Sophos Enterprise Console Richtlinien 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 VM-Sicherheitssystem.

Hinweis
Alle VM-Gastsysteme, die durch ein Sophos VM-Sicherheitssystem geschützt sind, wenden dieselben Richtlinien wie das Sophos VM-Sicherheitssystem an. Um auf bestimmte VM-Gastsysteme eine andere Richtlinie anzuwenden, weisen Sie diese einem anderen Sophos VM-Sicherheitssystem 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 für Virtual Environments – Enterprise Console Edition.

Informationen darüber, wie Sie eine Liste aller von einem Sophos VM-Sicherheitssystem verwalteten VM-Gastsysteme anzeigen können, finden Sie unter Anzeigen geschützter VM-Gastsysteme (Seite 8).

2.1 Antivirus- und HIPS-Richtlinie

Standardmäßig führt das Sophos VM-Sicherheitssystem 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 VM-Sicherheitssystem 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 VM-Sicherheitssystem 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	Hinweise
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 in der Hilfe zu Sophos Enterprise Console im Abschnitt zur Konfiguration der Antivirus- und HIPS-Richtlinie.
Registerkarte Mac-Ausschlüsse	Nein	
Registerkarte Linux-/UNIX-Ausschlüsse	Nein	

Bereinigung	Unterstützt	Hinweise
Entfernen von Viren/Spyware	Ja	Die alternativen Aktionen werden ausgeführt, wenn die Bereinigung fehlschlägt. Das Sophos VM-Sicherheitssystem 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.

Gehen Sie zu **Hinzufügen/Bearbeiten > Einstellungen 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 VM-Sicherheitssystem startet die Überprüfung zum geplanten Zeitpunkt, jedoch werden immer nur zwei VM-Gastsysteme auf einmal überprüft, damit die Leistung Ihres Systems nicht beeinträchtigt wird.

Gehen Sie zu **Hinzufügen/Bearbeiten > Einstellungen für geplante Scans > Konfigurieren > Einstellungen zu Scans und Bereinigung**.

Scans und Bereinigung	Unterstützt	Hinweise
Registerkarte Scans		
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 VM-Sicherheitssystem bereinigt nicht automatisch Diskettenlaufwerke, CD-Laufwerke oder Netzwerkverzeichnisse. Aktionen für infizierte Elemente wirken sich – wenn keine Bereinigung stattgefunden hat – nicht aus. Das Sophos VM-Sicherheitssystem protokolliert immer das Ereignis, wenn keine Bereinigung stattgefunden hat.
Entfernen von Adware und PUA	Nein	
Entfernen verdächtiger Dateien	Nein	

Gehen Sie zu **Erweiterungen und Ausschlüsse > Erweiterungen und Ausschlüsse für geplante Scans**.

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

Die folgenden Erweiterungen werden standardmäßig überprüft, wenn die Option **Archivdateien scannen** in der Antivirus- und HIPS-Richtlinie für das VM-Sicherheitssystem 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 in der Hilfe zu Sophos Enterprise Console im Abschnitt zum Konfigurieren der Antivirus- und HIPS-Richtlinie beschrieben.

2.2 Update-Richtlinie

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

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

3 Anzeigen geschützter VM-Gastsysteme

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

1. Gehen Sie zu dem Sophos VM-Sicherheitssystem. 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 VM-Sicherheitssystem 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 VM-Sicherheitssystem die VM-Gastsysteme schützt.

4 Überprüfen von VM-Gastsystemen

Sophos für 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 VM-Sicherheitssystem 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 VM-Sicherheitssystem 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 VM-Sicherheitssystem 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.

VM-Gastsysteme je nach Bedarf überprüfen

So können Sie je nach Bedarf eine vollständige Überprüfung aller VM-Gastsysteme durchführen:

1. Wechseln Sie zu Sophos Enterprise Console und suchen Sie in der Computerliste nach dem Sophos VM-Sicherheitssystem.
2. Klicken Sie mit der rechten Maustaste auf das Sophos VM-Sicherheitssystem und wählen Sie **Vollständige Systemüberprüfung**.

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

VM-Gastsysteme zu bestimmten Zeiten überprüfen

So führen Sie eine vollständige Überprüfung aller VM-Gastsysteme zu festen Zeiten aus:

1. Rufen Sie Sophos Enterprise Console auf.
2. Erstellen Sie einen geplanten Scan. Entsprechende Anweisungen hierzu finden Sie in der Hilfe zu Sophos Enterprise Console im Abschnitt zur Konfiguration der Antivirus- und HIPS-Richtlinie.

So zeigen Sie die Details des Scans nach dessen Ausführung an:

Doppelklicken Sie in Sophos Enterprise Console in der Computerliste im unteren Fensterbereich auf das Sophos VM-Sicherheitssystem, damit das Dialogfeld **Computerdetails** angezeigt wird.

5 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 VM-Sicherheitssystem, damit das Dialogfeld **Computerdetails** angezeigt wird. Im Abschnitt **Verlauf** sind **Erkannte Objekte** aufgeführt. Den Namen des Threat finden Sie in der Spalte **Name**, und das betroffene VM-Gastsystem und die betroffene Datei gehen aus der Spalte **Details** hervor.
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.

6 Entfernen eines Threat

6.1 Automatische Bereinigung

Das Sophos VM-Sicherheitssystem 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 Dialogfeld **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 VM-Sicherheitssystem angezeigt. Um herauszufinden, auf welches VM-Gastsystem sich der Warnhinweis bezieht, doppelklicken Sie auf das Sophos VM-Sicherheitssystem, um das Dialogfeld **Computerdetails** zu öffnen und die Beschreibung des Alerts im Abschnitt **Ausstehende Alerts und Fehler** zu lesen.

6.2 Manuelle Bereinigung

Sie können eine Bedrohung manuell entfernen.

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

6.2.1 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 für Virtual Environments – Enterprise Console Edition).

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

6.2.2 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 VM-Sicherheitssystem und wählen Sie die Option **Alerts und Fehler löschen**.
2. Wählen Sie im Dialogfeld **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.

7 Anhang: VM-Sicherheitssysteme für die Migration von VM-Gastsystemen hinzufügen

Sie können jederzeit mehr VM-Sicherheitssysteme hinzufügen, um migrierende VM-Gastsysteme zu schützen

Wichtig
Sie müssen diese Schritte auf dem VM-Sicherheitssystem, das Sie hinzufügen möchten, und auf den vorhandenen VM-Sicherheitssystemen ausführen.

1. Öffnen Sie über SSH die Konfigurationsdatei additional_svms.txt zur Bearbeitung:
   /opt/sophos-svms/etc/additional_svms.txt
2. Bearbeiten Sie die IP-Adressen der VM-Sicherheitssysteme, die zum Schutz von VM-Gastsystemen zur Verfügung stehen.
   - Schreiben Sie eine IP-Adresse pro Zeile und verwenden Sie keine Trennzeichen. Zum Beispiel:
     1.2.3.4
     5.6.7.8
   - Sie müssen die IP-Adresse des Sophos VM-Sicherheitssystem, an das Sie derzeit angemeldet sind, nicht angeben.
3. Speichern und schließen Sie die Datei.
4. Überprüfen Sie unter /var/log/ssvm.log, ob beim Verarbeiten der Liste mit den zusätzlichen VM-Sicherheitssystemen Fehler aufgetreten sind.
   Sind keine Fehler aufgetreten, wird die aktualisierte Liste an alle verbundenen VM-Gastsysteme gesendet, so dass sie durch die neuen VM-Sicherheitssysteme geschützt sind.

8 Alerts

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

Warnhinweise zu Bedrohungen

Wenn das Sophos VM-Sicherheitssystem 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 VM-Sicherheitssystem in der Spalte **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 VM-Sicherheitssystem. 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 VM-Sicherheitssystem 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 VM-Sicherheitssystem, um das Dialogfeld **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

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

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

1. Öffnen Sie eine Konsole für das Sophos VM-Sicherheitssystem.
2. Melden Sie sich an:
   - Der Benutzername lautet „sophos“.
   - Das Kennwort ist das Zugangskennwort, das Sie bei der Installation des Sophos VM-Sicherheitssystem festgelegt haben.
3. Geben Sie folgendes Kommando ein:

   ```
   sudo /opt/sophox/logcollector/diagnose
   ```

   Geben Sie das Zugriffskennwort ein, wenn Sie dazu aufgefordert werden. (Dies kann bis zu einer Minute dauern.)
4. 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 VM-Sicherheitssystem festgelegt haben.

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

10 Technischer Support

Sie können sich wie folgt an den technischen Support von Sophos wenden:

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

11 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.