SOPHOS

Cybersecurity made simple.

Sophos Anti-Virus per Linux

Guida alla configurazione

Sommario

Informazioni su questa guida....1
SAV per Linux....2
- Le funzioni di Sophos Anti-Virus per Linux....2
- Protezione del computer da parte di Sophos Anti-Virus....2
- Come utilizzare Sophos Anti-Virus....2
- Configurazione Sophos Anti-Virus per Linux....2

Scansione in accesso....4
- Verifica che la scansione in accesso sia attiva....4
- Verifica che la scansione in accesso sia impostata per cominciare automaticamente all'avvio....4
- Avvio della scansione in accesso....5
- Blocco della scansione in accesso....5

Scansione su richiesta....6
- Esecuzione delle scansioni su richiesta....6
- Configurazione delle scansioni su richiesta....7

Cosa accade se i virus vengono rilevati in accesso....10
Rimozione virus....12
- Informazioni sulla disinfezione....12
- Messa in quarantena dei file infetti....12
- Disinfezione di file infetti....13
- Rimozione degli effetti collaterali dei virus....14

Visualizzazione del log di Sophos Anti-Virus....15
Aggiornamento immediato di Sophos Anti-Virus....16
Supporto kernel....17
- Supporto per nuovi rilasci di kernel....17
- Supporto per kernel personalizzati....17

Appendice: creazione di una scansione pianificata....18
- Aggiunta di una scansione pianificata da un file....18
- Aggiunta di una scansione pianificata dall'input standard....18
- Esportazione di una scansione pianificata in un file....19
- Esportazione dei nomi di tutte le scansioni pianificate in un file....19
- Esportazione di una scansione pianificata nell'output standard....19
- Esportazione dei nomi di tutte le scansioni pianificate nell'output standard....19
- Aggiornamento di una scansione pianificata da un file....20
- Aggiornamento di una scansione pianificata dall'input standard....20
- Visualizzazione del log della scansione pianificata....21
- Rimozione di una scansione pianificata....21
- Rimozione di tutte le scansioni pianificate....21

Appendice: configurazione degli allarmi....22
- Configurazione di allarmi pop-up nel desktop....22
- Configurazione degli allarmi da riga di comando....23
- Configurazione degli allarmi e-mail....23

Appendice: configurazione log....26
Appendice: configurazione aggiornamenti....27
- Concetti di base....27
- Comando di configurazione savsetup....27
- Verifica della configurazione dell'aggiornamento automatico per un computer....28
- Configurazione del server degli aggiornamenti....28
- Configurazione di un singolo client di aggiornamento perché si aggiorni da un server di aggiornamento....28

Appendice: configurazione di Sophos Live Protection....30
- Verifica di Sophos Live Protection....30
- Attivazione e disattivazione di Sophos Live Protection....30

Appendice: configurazione della scansione in accesso....31
Modifica del metodo di intercettazione dei file della scansione in accesso....31
Esclusione di file e directory dalla scansione....31
Esclusione di un tipo di filesystem dalla scansione....33
Scansione degli archivi....33
Disinfezione di file infetti....33
Risoluzione dei problemi....35
Impossibile eseguire un comando....35
Non è stata applicata la configurazione delle esclusioni....35
Report del computer “No manual entry for …”....36
Non ha sufficiente spazio su disco....36
La scansione su richiesta è lenta....37
Il programma di archiviazione esegue il backup di tutti i file sottoposti alla scansione su richiesta....38
Virus non rimosso....38
Frammento di virus rilevato....39
Consenso dell'accesso al disco....39
Appendice: codici di ritorno della scansione su richiesta....41
Codici di ritorno estesi....41
Appendice: configurazione della funzionalità "phone home"....43
Appendice: configurazione dei riavvii per RMS....44
Glossario....45
Supporto....47
Note legali....48
ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™....48
GNU General Public License....49
libcap....49
OpenSSL....50
protobuf....52
pycrypto....52
TinyXML XML parser....53
zlib....53

1 Informazioni su questa guida

Questa guida spiega come configurare ed utilizzare Sophos Anti-Virus per Linux.

Le informazioni relative a:

Installazione di Sophos Anti-Virus in modo tale che possa essere gestito con Sophos Central: accedere a Sophos Central, caricare la pagina dei Download e seguire le istruzioni indicate nella pagina stessa.

Installazione di Sophos Anti-Virus in modo tale che possa essere gestito tramite Sophos Enterprise Console, sono incluse nella Guida di avvio di Sophos Enterprise Console per Linux e UNIX.

Installazione o disinstallazione di Sophos Anti-Virus non gestito nei computer Linux in rete o indipendenti: consultare la Guida di avvio di Sophos Anti-Virus per Linux.

La documentazione di Sophos è pubblicata alla pagina web http://www.sophos.com/it-it/support/documentation.aspx.

Installazioni gestite da Sophos Central

Se si utilizzano server Linux a 32 bit gestiti da Sophos Central, consultare la Guida di avvio di Sophos Anti-Virus per Linux.

Se si utilizzano server Linux a 64 bit gestiti da Sophos Central, consultare la Guida di avvio di Sophos Anti-Virus per Linux 10.

Attenzione
Le informazioni relative alla configurazione contenute in questa guida sono applicabili anche a Sophos Anti-Virus per Linux 10.

2 Informazioni su Sophos Anti-Virus per Linux

2.1 Le funzioni di Sophos Anti-Virus per Linux

Sophos Anti-Virus per Linux rileva e si occupa dei virus (compresi worm e tojan) presenti nei computer con sistema operativo Linux. Oltre a rilevare tutti i virus specifici di Linux, riesce anche a rilevare tutti i virus non specifici di questo sistema operativo, ma che possono essere stati memorizzati nei computer Linux e quindi venire trasferiti a computer non-Linux. Tutto ciò avviene tramite scansione del computer.

2.2 Protezione del computer da parte di Sophos Anti-Virus

La scansione in accesso rappresenta il principale metodo di protezione antivirus. Ogniqualvolta venga aperto, salvato o copiato un file, Sophos Anti-Virus ne effettua la scansione consentendone l'accesso solo se sicuro.

Sophos Anti-Virus consente, inoltre, di eseguire la scansione su richiesta per consentire protezione aggiuntiva. La scansione su richiesta è una scansione avviata dall'utente. È possibile eseguire la scansione di qualsiasi elemento, da un solo file a tutto ciò che è contenuto nel proprio computer e per cui si dispone di autorizzazione per la lettura. È possibile eseguire la scansione su richiesta sia manualmente che automaticamente.

Sophos Anti-Virus consente di eseguire la *scansione su richiesta*. La scansione su richiesta è una scansione avviata dall'utente. È possibile eseguire la scansione di qualsiasi elemento, da un solo file a tutto ciò che è contenuto nel proprio computer e per cui si dispone di autorizzazione per la lettura. È possibile eseguire la scansione su richiesta sia manualmente che automaticamente.

2.3 Come utilizzare Sophos Anti-Virus

Tutte le attività possono essere svolte utilizzando l'interfaccia della riga di comando.

è necessario essere connessi al computer con privilegi di root per poter eseguire tutti i comandi, eccezion fatta per `savscan`, utilizzato per effettuare la scansione su richiesta.

In questo manuale si presuppone che Sophos Anti-Virus sia stato installato nel percorso predefinito `/opt/sophos-av`. I percorsi dei comandi descritti si basano su tale percorso.

2.4 Configurazione Sophos Anti-Virus per Linux

I metodi di configurazione di Sophos Anti-Virus per Linux dipendono dall'utilizzo o meno dei software di gestione Sophos (Sophos Enterprise Console o Sophos Central).

Computer gestiti da Sophos Enterprise Console o Sophos Central

Se i computer Linux sono gestiti da Sophos Enterprise Console o Sophos Central, configurare Sophos Anti-Virus per Linux in questo modo:

- Configurare centralmente **scansioni in accesso o pianificate, allarmi, log e aggiornamenti** dalla console di gestione. Per informazioni, consultare la Guida in linea presente nella console di gestione.

  Nota
  queste funzionalità includono anche alcuni parametri che non possono essere impostati centralmente dalla console di gestione. Per impostarli localmente utilizzare l'interfaccia CLI di Sophos Anti-Virus in ciascun computer Linux. La console di gestione li ignora.

  Nota
  Se si utilizzano server Linux a 64 bit gestiti da Sophos Central, consultare la Guida di avvio di Sophos Anti-Virus per Linux versione 10.

- Configurare la scansione su richiesta dall'interfaccia CLI di Sophos Anti-Virus per Linux localmente, su ciascun computer Linux.

Computer in rete non gestiti da Sophos Enterprise Console o Sophos Central

Se è presente una rete di computer Linux che non è gestita da Sophos Enterprise Console o da Sophos Central, configurare le scansioni su richiesta dall'interfaccia CLI di Sophos Anti-Virus per Linux localmente, su ciascun computer.

Computer autonomi non gestiti da Sophos Enterprise Console o Sophos Central

Se si dispone di computer Linux che *non sono* gestiti da Sophos Enterprise Console o Sophos Central, configurare tutte le funzionalità di Sophos Anti-Virus per Linux dall'interfaccia CLI.

3 Scansione in accesso

La scansione in accesso rappresenta il principale metodo di protezione antivirus. Ogniqualvolta venga aperto, salvato o copiato un file, Sophos Anti-Virus ne effettua la scansione consentendone l'accesso solo se sicuro.

Per impostazione predefinita, la scansione in accesso è abilitata. È possibile verificare che sia effettivamente attiva e se necessario avviarla.

Nota
per eseguire i comandi riportati in questa sezione, è necessario essere collegati al computer come utente root.

In questo manuale si presuppone che Sophos Anti-Virus per Linux sia stato installato nel percorso predefinito `/opt/sophos-av`. Se non è questo il caso, quando si esegue un comando, è necessario inserire il percorso della directory di installazione che si sta utilizzando.

3.1 Verifica che la scansione in accesso sia attiva

- Per verificare che la scansione in accesso sia attiva digitare: `/opt/sophos-av/bin/savdstatus`.

3.2 Verifica che la scansione in accesso sia impostata per cominciare automaticamente all'avvio

Per eseguire questa procedura, è necessario accedere al computer come utente root.

1. Verificare che `savd` venga avviato automaticamente all'avvio del sistema: `chkconfig --list`.

   Nota
   Se questo comando non funziona nella propria distribuzione Linux, utilizzare la relativa utilità per visualizzare i servizi configurati per essere avviati al momento dell'avvio del sistema.

   Se l'elenco include una voce per sav-protect con 2:on, 3:on, 4:on e 5:on, la scansione in accesso verrà lanciata automaticamente all'avvio del sistema. In caso contrario, digitare: `/opt/sophos-av/bin/savdctl enableOnBoot savd`.
2. Verificare che la scansione in accesso venga avviata automaticamente tramite `savd`: `/opt/sophos-av/bin/savconfig query EnableOnStart`.

   Se il comando restituisce il valore `true`, la scansione in accesso verrà lanciata automaticamente con `savd`, all'avvio del sistema. In caso contrario, digitare: `/opt/sophos-av/bin/savconfig set EnableOnStart true`.

3.3 Avvio della scansione in accesso

Per avviare la scansione in accesso, eseguire una delle seguenti operazioni:

- Digitare: `/opt/sophos-av/bin/savdctl enable`.
- Utilizzare il tool adeguato per avviare il servizio sav-protect installato. Per esempio, digitare: `/etc/init.d/sav-protect start` o `service sav-protect start`.

3.4 Blocco della scansione in accesso

Importante
Se si interrompe la scansione in accesso, Sophos Anti-Virus non esegue la scansione dei file a cui si accede alla ricerca di virus. Ciò espone a rischi il proprio computer e tutti quelli a cui si è collegati.

- Per bloccare la scansione in accesso, digitare: `/opt/sophos-av/bin/savdctl disable`.

4 Scansione su richiesta

La scansione su richiesta è una scansione avviata dall'utente. È possibile eseguire la scansione di qualsiasi elemento, da un solo file a tutto ciò che è contenuto nel proprio computer e per cui si dispone di autorizzazione per la lettura. È possibile eseguire la scansione su richiesta sia manualmente che automaticamente.

Per pianificare una scansione su richiesta, eseguire il comando `crontab`. Per informazioni, consultare l'articolo 12176 della knowledge base del supporto Sophos.

4.1 Esecuzione delle scansioni su richiesta

Il comando da digitare per eseguire una scansione su richiesta è `savscan`.

4.1.1 Scansione del computer

- Per sottoporre a scansione il computer, digitare: `savscan /`.

Nota
Per sottoporre a scansione completa uno o più computer, si può anche utilizzare Sophos Enterprise Console. Per dettagli, consultare la Guida in linea di Sophos Enterprise Console.

4.1.2 Scansione di una determinata directory o file

- Per sottoporre a scansione una directory o un file in particolare, specificare il percorso dell'elemento. Per esempio, digitare: `savscan /usr/mydirectory/myfile`.

  Nello stesso comando è possibile digitare più di una directory o file.

4.1.3 Scansione di un filesystem

- Per sottoporre a scansione un filesystem, specificarne il nome. Per esempio, digitare: `savscan /home`.

  Nello stesso comando è possibile digitare più di un filesystem.

4.1.4 Scansione di un settore di avvio

Nota
Ciò è applicabile solo a sistemi operativi Linux e FreeBSD.

Per eseguire la scansione di un settore di avvio, accedere come superuser. Ciò consente di avere i permessi sufficienti per accedere ai dispositivi del disco.

È possibile eseguire la scansione del settore di avvio sia di un'unità logica che fisica.

- Per eseguire la scansione del settore di avvio di una determinata unità logica, digitare: `savscan -bs=unità, unità, ...`, in cui *unità* è il nome dell'unità, per esempio `/dev/fd0` o `/dev/hda1`.
- Per eseguire la scansione del settore di avvio di tutte le unità logiche, digitare: `savscan -bs`.
- Per eseguire la scansione del record di avvio principale tutte le unità fisiche fisse presenti nel computer, digitare: `savscan -mbr`.

4.2 Configurazione delle scansioni su richiesta

In questa sezione, laddove *percorso* compare in un comando, fa riferimento al percorso da sottoporre a scansione.

Per visualizzare l'elenco completo delle opzioni utilizzabili con una scansione su richiesta, digitare:

```
man savscan
```

4.2.1 Scansione di tutti i tipi di file

Per impostazione dredefinita, Sophos Anti-Virus esegue la scansione solo di eseguibili. Per visualizzare l'elenco completo di tutti i tipi di file che Sophos Anti-Virus sottopne a scansione per impostazione predefinita, digitare `savscan -vvsweep -vv`.

- Per sottoporre a scansione tutti i tipi di file, non solo quelli esaminati per impostazione predefinita, utilizzare l'opzione -all. Digitare: `savscan percorso -all`.

> **Nota**
> Ciò rende la scansione più lunga, può avere un impatto sul rendimento dei server e può causare falsi positivi.

4.2.2 Scansione di un determinato tipo di file

Per impostazione dredefinita, Sophos Anti-Virus esegue la scansione solo di eseguibili. Per visualizzare l'elenco completo di tutti i tipi di file che Sophos Anti-Virus sottopne a scansione per impostazione predefinita, digitare `savscan -vvsweep -vv`.

- Per eseguire la scansione di un determinato tipo di file, utilizzare l'opzione -ext con l'estensione adeguata. Per esempio, per abilitare la scansione dei file con estensione `.txt`, digitare: `savscan percorso -ext=txt`.
- Per disabilitare la scansione di un determinato tipo di file, utilizzare l'opzione -next con l'estensione adeguata.

> **Nota**
> Per specificare più di un tipo di file, separare ogni estensione da una virgola.

4.2.3 Scansione di tutti i tipi di archivio

È possibile configurare Sophos Anti-Virus in modo tale che esegua la scansione di tutti i tipi di archivio. Per visualizzare un elenco di tutti i tipi di archivio disponibili, digitare `savscan -vv`.

Nota
Il motore di rilevamento delle minacce effettua la scansione dei file di archivio solamente quando non superano gli 8GB (se decompressi). Ciò è perché supporta il formato di archivio ustar POSIX, che non permette l'uso di file di dimensioni superiori a questo limite.

- Per sottoporre a scansione tutti i tipi di archivio, utilizzare l'opzione -archive. Digitare: `savscan *percorso* -archive`.

  Gli archivi "annidati" all'interno di altri (per esempio, un archivio TAR all'interno di un archivio ZIP) vengono esaminati in modo ricorsivo.

  In caso di numerosi archivi complessi, la scansione può impiegare più tempo. Tenerlo a mente prima di pianificare delle scansioni automatiche.

4.2.4 Scansione all'interno di un particolare tipo di archivio

È possibile configurare Sophos Anti-Virus in modo tale che esegua di un determinato tipi di archivio. Per visualizzare un elenco di tutti i tipi di archivio disponibili, digitare `savscan -vv`.

Nota
Il motore di rilevamento delle minacce effettua la scansione dei file di archivio solamente quando non superano gli 8GB (se decompressi). Ciò è perché supporta il formato di archivio ustar POSIX, che non permette l'uso di file di dimensioni superiori a questo limite.

- Per sottoporre a scansione un particolare tipo di archivio, utilizzare l'opzione mostrata nell'elenco. Per esempio, per eseguire una scansione all'interno degli archivi TAR e ZIP, digitare: `savscan *percorso* -tar -zip`.

  Gli archivi "annidati" all'interno di altri (per esempio, un archivio TAR all'interno di un archivio ZIP) vengono esaminati in modo ricorsivo.

  In caso di numerosi archivi complessi, la scansione può impiegare più tempo. Tenerlo a mente prima di pianificare delle scansioni automatiche.

4.2.5 Scansione dei computer remoti

Per impostazione predefinita, Sophos Anti-Virus non esegue la scansione di oggetti presenti su computer remiti (vale a dire che non attraversa punti di montaggio remoti).

- Per sottoporre a scansione i computer remoti, utilizzare l'opzione --no-stay-on-machine. Digitare: `savscan *percorso* --no-stay-on-machine`.

4.2.6 Disabilitazione della scansione di oggetti collegati da link simbolici

Per impostazione predefinita, Sophos Anti-Virus sottopone a scansione gli oggetti collegati da link simbolici.

- Per disabilitare la scansione di tali oggetti, utilizzare l'opzione --no-follow-symlinks. Digitare: `savscan *percorso* --no-follow-symlinks`.

  Per evitare di esaminare un oggetto più di una volta, utilizzare l'opzione --backtrack-protection.

4.2.7 Scansione solamente del filesystem di avvio

Sophos Anti-Virus è configurabile per non sottoporre a scansione gli oggetti che sono oltre il filesystem di avvio (vale a dire, per non attraversare i punti di montaggio).

- Per sottoporre a scansione solamente il filesystem di avvio, utilizzare l'opzione --stay-on-filesystem. Digitare: `savscan *percorso* --stay-on-filesystem`.

4.2.8 Esclusione di oggetti dalla scansione

È possibile configurare Sophos Anti-Virus in modo tale che escluda determinati oggetti (file, directory o file system) dalla scansione tramite l'opzione -exclude. Sophos Anti-Virus esclude tutti gli oggetti che seguono, nella stringa di comando, l'opzione sopracitata. Per esempio, per eseguire la scansione di oggetti quali `fred` e `harry`,ma non di `tom` o `peter`, digitare: `savscan fred harry -exclude tom peter`

È possibile escludere directory e file che si trovano *in* una particolare directory. Per esempio, per sottoporre a scansione tutta la directory home di Fred, escludendo la directory `games` (e tutte le directory e i file in essa contenuti), digitare: `savscan /home/fred -exclude /home/fred/games`.

È inoltre possibile configurare Sophos Anti-Virus in modo tale che includa gli oggetti posizionati dopo -include. Per esempio. per eseguire la scansione di oggetti quali `fred`, `harry` e `bill`,ma non di `tom` o `peter`, digitare: `savscan fred harry -exclude tom peter -include bill`.

4.2.9 Scansione di tipi di file che UNIX definisce come eseguibili

Per impostazione predefinita, Sophos Anti-Virus non sottopne a scansione i tipi di file che UNIX definisce come eseguibili.

- Per sottoporre a scansione i tipi di file che UNIX definisce come eseguibili, utilizzare l'opzione --examine-x-bit. Digitare: `savscan *percorso* --examine-x-bit`.

  Sophos Anti-Virus continua ad eseguire la scansione dei file le cui estensioni, indicate nel nome file, sono incluse anche nel suo elenco. Per visualizzare l'elenco di tali estensioni, digitare `savscan -vv`.

5 Cosa accade se i virus vengono rilevati in accesso

Sia che i virus vengano rilevati dalla scansione in accesso che da quella su richiesta, per impostazione predefinita Sophos Anti-Virus:

- Registra l'evento in syslog e nel log di Sophos Anti-Virus (consultare la sezione Visualizzazione del log di Sophos Anti-Virus (pagina 15)).
- Invia un allarme a Sophos Enterprise Console, se gestito da Sophos Enterprise Console.
- Invia un avviso e-maila a root@localhost.

Per impostazione predefinita, Sophos Anti-Virus visualizza avvisi anche in base a se i virus siano stati rilevati tramite scansione in accesso o su richiesta, come indicato qui di seguito.

Scansione in accesso

Se durante la scansione in accesso vine rilevato un virus, Sophos Anti-Virus nega l'accesso al file e, per impostazione predefinita, visualizza nel desktop allarmi pop-up simili a quello riportato qui sotto.

Se non è possibile visualizzare allarmi pop-up nel desktop, vengono invece visualizzati allarmi da riga di comando.

Per informazioni sulla rimozione dei virus, consultare la sezione Rimozione virus (pagina 12).

Scansioni su richiesta

Se durante la scansione su richiesta viene rilevato un virus, per impostazione predefinita Sophos Anti-Virus visualizza allarmi da riga di comando. Il virus viene riportato nella riga che comincia con >>> seguite dalla dicitura `Virus` o `Frammento di virus`:

```
SAVScan virus detection utility
Version 4.69.0 [Linux/Intel]
Virus data version 4.69
Includes detection for 2871136 viruses, Trojans and worms
Copyright (c) 1989-2012 Sophos Limited. All rights reserved.

System time 13:43:32, System date 22 September 2012

IDE directory is: /opt/sophos-av/lib/sav

Using IDE file nyrate-d.ide
. . . . . .
Using IDE file injec-lz.ide

Quick Scanning

>>> Virus 'EICAR-AV-Test' found in file /usr/mydirectory/eicar.src

33 files scanned in 2 seconds.
1 virus was discovered.
1 file out of 33 was infected.
Please send infected samples to Sophos for analysis.
For advice consult www.sophos.com or email support@sophos.com
End of Scan.
```

6 Rimozione virus

6.1 Informazioni sulla disinfezione

Se vengono segnalati virus, è possibile ottenere informazioni e consigli per la loro rimozione dal sito web di Sophos.

Per informazioni sulla disinfezione:

1. Visitare la pagina web con le analisi della sicurezza (http://www.sophos.com/it-it/threat-center/threat-analyses/viruses-and-spyware.aspx).
2. Cercare l'analisi del virus utilizzando il nome rilevato da Sophos Anti-Virus.

6.2 Messa in quarantena dei file infetti

È possibile configurare la scansione su richiesta in modo tale da poter mettere in quarantena i file infetti, evitando in questo modo che vi si acceda. Ciò è realizzabile cambiando la proprietà e le autorizzazioni per tali file.

Nota
se si specifica la disinfezione (consultare la sezione Disinfezione di file infetti (pagina 13)) oltre che la messa in quarantena, Sophos Anti-Virus cerca di disinfettare i file infetti e nel caso questa operazione non riesca li mette in quarantena.

In questa sezione, laddove *percorso* compare in un comando, fa riferimento al percorso da sottoporre a scansione.

6.2.1 Specificazione della messa in quarantena

- Per specificare la messa in quarantena, utilizzare l'opzione --quarantine. Digitare: `savscan` *percorso* `--quarantine`.

6.2.2 Specificazione della proprietà e delle autorizzazioni da applicare

Per impostazione predefinita, Sophos Anti-Virus cambia:

- L'utente proprietario di un file infetto con l'utente che esegue Sophos Anti-Virus.
- Il gruppo proprietario del file con il gruppo cui appartiene l'utente.
- Le autorizzazioni del file con `-r--------(0400)`.

Se lo si preferisce, è possibile modificare la prorietà utente o gruppo e le autorizzazioni file applicate da Sophos Anti-Virus ai file infetti. A tale scopo, utilizzare i seguenti parametri:

```
uid=nnn
user=username
gid=nnn
group=group-name
mode=ppp
```

Non è possibile specificare più di un parametro per proprietà utente o gruppo. Per esempio, non è possibile specificare contemporaneamente un parametro uid e user.

Per ogni parametro che non si specifica, viene utilizzata l'impostazione predefinita (citata in precedenza).

Per esempio:

`savscan fred --quarantine:user=virus,group=virus,mode=0400` modifica la proprietà utente di un file infetto in "virus", la proprietà gruppo in "virus" e le autorizzazioni dei file in `-r---------`. Ciò significa che il file è di proprietà dell'utente "virus" e del gruppo "virus", ma solo l'utente "virus" può accedervi (e solo in lettura). Nessuno (eccezion fatta per l'utente root) può eseguire alcuna operazione riguardante questo file.

Per impostare proprietà e autorizzazioni può essere necessario connettersi come utente speciale o superuser.

6.3 Disinfezione di file infetti

È possibile configurare una scansione su richiesta per disinfettare (disinfetta o cancella) i file infetti. Tutte le azioni svolte da Sophos Anti-Virus in file infetti sono elencate nel riepilogo della scansioe e registrate nel log di Sophos Anti-Virus. Per impostazione predefinita, la disinfezione è disabilitata.

In questa sezione, laddove *`percorso`* compare in un comando, fa riferimento al percorso da sottoporre a scansione.

6.3.1 Disinfezione di un determinato file infetto

- Per disinfettare un determinato file infetto, utilizzare l'opzione -di. Digitare: `savscan` *`percorso`* `-di`.

  Sophos Anti-Virus chiede conferma prima di procedere alla disinfezione.

  Nota
  La disinfezione dei documenti infetti non annulla le modifiche che il virus può aver apportato al documento. Consultare Informazioni sulla disinfezione (pagina 12) per sapere come visualizzare, sul sito web di Sophos, i dettagli sugli effetti secondari dei virus.

6.3.2 Disinfezione di tutti i file infetti presenti nel computer

- Per disinfettare tutti i file infetti presenti nel computer, digitare: `savscan / -di`.

  Sophos Anti-Virus chiede conferma prima di procedere alla disinfezione.

Nota
La disinfezione dei documenti infetti non annulla le modifiche che il virus può aver apportato al documento. Consultare Informazioni sulla disinfezione (pagina 12) per sapere come visualizzare, sul sito web di Sophos, i dettagli sugli effetti secondari dei virus.

6.3.3 Eliminazione di un determinato file infetto

- Per rimuovere un determinato file infetto, utilizzare l'opzione -remove. Digitare: `savscan` *`percorso`* `-remove`.

  Sophos Anti-Virus chiede conferma prima di procedere all'eliminazione.

6.3.4 Eliminazione di tutti i file infetti nel computer

- Per rimuovere tutti i file dal computer, digitare: `savscan / -remove`.

  Sophos Anti-Virus chiede conferma prima di procedere all'eliminazione.

6.3.5 Disinfezione di un settore di avvio infetto

Nota
Ciò è applicabile solo a sistemi operativi Linux e FreeBSD.

- Per eseguire la disinfezione di un settore di avvio infetto, utilizzare l'opzione di disinfezione -di e quella relativa al settore di avvio -bs. Per esempio, digitare: `savscan -bs=/dev/fd0 -di`.

  in cui `/dev/fd0` è il nome dell'unità in cui si trova il settore di avvio infetto.

  Sophos Anti-Virus chiede conferma prima di procedere alla disinfezione.

6.4 Rimozione degli effetti collaterali dei virus

La rimozione degli effetti collaterali dei virus dipende dal modo in cui il virus ha infettato il computer. Alcuni virus non provocano effetti secondari, altri possono averne di così gravi da comportare il ripristino dell'hard disk.

Alcuni virus alterano i dati gradualmente. Questo tipo di alterazione può essere difficile da rilevare. È molto importante leggere l'analisi del virus sul sito web di Sophos e verificare con attenzione i documenti dopo aver effettuato la disinfezione.

È essenziale disporre di copie di backup attendibili. Se non si disponeva di tali copie prima dell'infezione, è necessario cominciare a crearle e conservarle in caso di future infezioni.

Talvolta è possibile recuperare i dati dai dischi danneggiati da un virus. Sophos fornisce delle utilità per la riparazione dei danni causati da alcuni virus. Rivolgersi al supporto tecnico di Sophos per ricevere assistenza.

7 Visualizzazione del log di Sophos Anti-Virus

Sophos Anti-Virus registra i dati relativi alle attività di scansione in syslog e nel log di Sophos Anti-Virus. Anche virus ed eventi vengono registrati nel log di Sophos Anti-Virus.

- Per visualizzare il log di Sophos Anti-Virus, utilizzare il comando `savlog`. Quest'ultimo può essere eseguito applicando diverse opzioni che consentono di limitare i risultati solo a determinati messaggi e di controllare la visualizzazione. Per esempio, per visualizzare i messaggi registrati nel log di Sophos Anti-Virus nelle ultime 24 e la data e l'ora in formato UTC/ISO 8601 digitare: `/opt/sophos-av/bin/savlog --today --utc`.
- Per visualizzare l'elenco completo delle opzioni che si possono utilizzare con `savlog`, digitare: `man savlog`.

8 Aggiornamento immediato di Sophos Anti-Virus

Se è stata abilitata la funzione di aggiornamento automatico, Sophos Anti-Virus verrà aggiornato automaticamente. È comunque possibile aggiornare Sophos Anti-Virus immediatamente, senza dover attendere il prossimo aggiornamento automatico.

- Per aggiornare Sophos Anti-Virus immediatamente, nel computer in cui si desidera eseguire l'aggiornamento digitare: `/opt/sophos-av/bin/savupdate`.

Nota
è possibile aggiornare i computer immediatamente anche da Sophos Enterprise Console.

9 Supporto kernel

Nota
Questa sezione riguarda solo gli utenti che utilizzano Talpa come metodo di intercettazione della scansione in accesso. Per ulteriori informazioni, consultare la sezione Modifica del metodo di intercettazione dei file della scansione in accesso (pagina 31).

9.1 Supporto per nuovi rilasci di kernel

Quando un dei vendor di Linux supportato da Sophos Anti-Virus rilascia un aggiornamento del kernel Linux, Sophos rilascerà un aggiornamento del modulo dell'interfaccia del kernel (Talpa) di Sophos per poterlo supportare. Se viene applicato un aggiornamento del kernel Linux prima di applicare il relativo aggiornamento Talpa, Sophos Anti-Virus avvia la compilazione locale di Talpa. Se questa operazione non riesce, Sophos Anti-Virus proverà ad utilizzare Fanotify come metodo di intercettazione alternativo. Se anche Fanotify non è disponibile, verrà bloccata la scansione in accesso e rilevato un errore.

Per evitare di incorrere in questo problema, è necessario verificare che l'aggiornamento di Talpa corrispondente sia stato rilasciato prima di applicare l'aggiornamento del kernel di Linux. L'elenco delle distribuzioni e aggiornamenti di Linux supportati è disponibile consultando l'articolo 14377 della knowledge base di Sophos (http://www.sophos.com/it-it/support/knowledgebase/14377.aspx).

Se l'aggiornamento di Talpa richiesto è incluso nell'elenco, significa che è disponibile per il download. Se è stata abilitata la funzione di aggiornamento automatico, Sophos Anti-Virus scaricherà l'aggiornamento automaticamente.

È anche possibile aggiornare Sophos Anti-Virus immediatamente, senza dover attendere il prossimo aggiornamento automatico, digitare: `/opt/sophos-av/bin/savupdate`.

Sarà quindi possibile applicare l'aggiornamento del kernel di Linux.

9.2 Supporto per kernel personalizzati

Se si personalizzano kernel di Linux, in questa guida non è spiegato come configurare gli aggiornamenti in questa particolare situazione. Consultare l'articolo 13503 della knowledge base del supporto tecnico di Sophos (http://www.sophos.com/it-it/support/knowledgebase/13503.aspx).

10 Appendice: creazione di una scansione pianificata

Sophos Anti-Virus può memorizzare le definizioni di una o più scansioni pianificate.

Nota
Le scansioni pianificate aggiunte tramite Sophos Enterprise Console vengono visualizzate con nomi che hanno come prefisso “SEC:” e possono essere aggiornate o rimosse solo utilizzando Sophos Enterprise Console.

10.1 Aggiunta di una scansione pianificata da un file

1. Se inizialmente si desidera utilizzare un modello per le definizioni delle scansioni, aprire il file `/opt/sophos-av/doc/namedscan.example.en`.

   Per creare da zero una definizione di scansione, aprire un nuovo file di testo.
2. Definire cosa sottoporre a scansione e quando, oltre a qualsiasi altra opzione, utilizzando solo i parametri elencati nel modello.

   Per pianificare la scansione, è necessario includere almeno una data e un orario.
3. Salvare il file in una posizione a propria scelta, facendo attenzione a non sovrascrivere il modello.
4. Aggiungere la scansione pianificata a Sophos Anti-Virus tramite il comando `savconfig` scegliendo l'opzione add e il parametro NamedScans. Specificare il nome della scansione e il percorso del file della definizione. Per esempio, per aggiungere la scansione Quotidiana e memorizzarla in `/home/fred/ScansioneQuotidiana`, digitare: `/opt/sophos-av/bin/savconfig add NamedScans Daily /home/fred/DailyScan`.

10.2 Aggiunta di una scansione pianificata dall'input standard

1. Aggiungere la scansione pianificata a Sophos Anti-Virus tramite il comando `savconfig` scegliendo l'opzione add e il parametro NamedScans. Specificare il nome della scansione utilizzando un trattino per indicare che la definizione deve venire letta dall'immissione standard. Per esempio, per aggiungere la scansione Quotidiana, digitare: `/opt/sophos-av/bin/savconfig add NamedScans Daily -`.
   Premendo INVIO, Sophos Anti-Virus attende che venga digitata la definizione della scansione pianificata.
2. Definire cosa sottoporre a scansione e quando, oltre a qualsiasi altra opzione, utilizzando solo i parametri elencati nella definizione di scansione del modello: `/opt/sophos-av/doc/namedscan.example.en`. Dopo aver digitato ogni parametro e il relativo valore, premere INVIO.

   Per pianificare la scansione, è necessario includere almeno un giorno e un orario.
3. Per completare la definizione, premere CTRL+D.

10.3 Esportazione di una scansione pianificata in un file

- Per esportare una scansione pianificata da Sophos Anti-Virus in un file, utilizzare il comando `savconfig` con l'opzione query e il parametro NamedScans.
- Specificare il nome della scansione e del percorso del file in cui esportare la scansione. Per esempio, per esportare la scansione Quotidiana nel file `/home/fred/ScansioneQuotidiana`, digitare: `/opt/sophos-av/bin/savconfig query NamedScans Daily > /home/fred/DailyScan`.

10.4 Esportazione dei nomi di tutte le scansioni pianificate in un file

- Per esportare i nomi di tutte le scansioni pianificate (compreso quelle create tramite Sophos Enterprise Console) da Sophos Anti-Virus in un file, utilizzare il comando `savconfig` e scegliere l'opzione query e il parametro NamedScans. Specificare il percorso del file nel quale si desidera esportare i nomi delle scansioni. Per esempio, per esportare i nomi di tutte le scansioni pianificate nel file `/home/fred/AllScans`, digitare: `/opt/sophos-av/bin/savconfig query NamedScans > /home/fred/AllScans`.

  Nota
  `SEC:FullSystemScan` è una scansione sempre definita se il computer è gestito da Sophos Enterprise Console.

10.5 Esportazione di una scansione pianificata nell'output standard

- Per esportare una scansione pianificata da Sophos Anti-Virus a output standard, utilizzare il comando `savconfig` con l'opzione query e il parametro NamedScans. Specificare il nome della scansione. Per esempio, per esportare la scansione Quotidiana nell'output standard, digitare: `/opt/sophos-av/bin/savconfig query NamedScans Daily`.

10.6 Esportazione dei nomi di tutte le scansioni pianificate nell'output standard

- Per esportare i nomi di tutte le scansioni pianificate (compreso quelle create tramite Sophos Enterprise Console) da Sophos Anti-Virus a output standard, utilizzare il comando `savconfig` e scegliere l'opzione query e il parametro NamedScans. Per esempio, per esportare i nomi di tutte le scansioni pianificate nell'output standard, digitare: `/opt/sophos-av/bin/savconfig query NamedScans`.

Nota
`SEC:FullSystemScan` è una scansione sempre definita se il computer è gestito da Sophos Enterprise Console.

10.7 Aggiornamento di una scansione pianificata da un file

Nota
Non è possibile aggiornare le scansioni pianificate aggiunte tramite Sophos Enterprise Console.

1. Aprire il file che definisce la scansione pianificata da aggiornare.

   Se la scansione non è ancora definita in un file, è possibile esportarla in un file, secondo quanto descritto nella sezione Esportazione di una scansione pianificata in un file (pagina 19).
2. Modificare la definizione secondo necessità, utilizzando solo i parametri elencati nella definizione della scansione del modello: `/opt/sophos-av/doc/namedscan.example.en`. È necessario definire la scansione in modo completo, anziché specificare solo cosa aggiornare.
3. Salvare il file.
4. Aggiornare la scansione pianificata in Sophos Anti-Virus tramite il comando `savconfig` scegliendo l'opzione update e il parametro NamedScans. Specificare il nome della scansione e il percorso del file della definizione. Per esempio, per aggiornare la scansione Quotidiana e memorizzarla in `/home/fred/ScansioneQuotidiana`, digitare: `/opt/sophos-av/bin/savconfig update NamedScans Daily /home/fred/DailyScan`.

10.8 Aggiornamento di una scansione pianificata dall'input standard

Nota
Non è possibile aggiornare le scansioni pianificate aggiunte tramite Sophos Enterprise Console.

1. Aggiornare la scansione pianificata in Sophos Anti-Virus tramite il comando `savconfig` scegliendo l'opzione update e il parametro NamedScans. Specificare il nome della scansione utilizzando un trattino per indicare che la definizione deve venire letta dall'immissione standard. Per esempio, per aggiornare la scansione quotidiana, digitare: `/opt/sophos-av/bin/savconfig update NamedScans Daily -`.
   Premendo INVIO, Sophos Anti-Virus attende che venga digitata la definizione della scansione pianificata.
2. Definire cosa sottoporre a scansione e quando, oltre a qualsiasi altra opzione, utilizzando solo i parametri elencati nella definizione di scansione del modello: `/opt/sophos-av/doc/namedscan.example.en`. Dopo aver digitato ogni parametro e il relativo valore, premere INVIO. È necessario definire la scansione in modo completo, anziché specificare solo cosa aggiornare.

   Per pianificare la scansione, è necessario includere almeno una data e un orario.

3. Definire cosa sottoporre a scansione e quando, oltre a qualsiasi altra opzione, utilizzando solo i parametri elencati nella definizione di scansione del modello: `/opt/sophos-av/doc/namedscan.example.en`. Dopo aver digitato ogni parametro e il relativo valore, premere INVIO.

   Per pianificare la scansione, è necessario includere almeno una data e un orario.

10.9 Visualizzazione del log della scansione pianificata

- Per visualizzare il log di una scansione pianificata, utilizzare il comando `savlog` e l'opzione namedscan. Specificare il nome della scansione. Per esempio, per visualizzare il log della scansione giornaliera, digitare: `/opt/sophos-av/bin/savlog --namedscan=Daily`.

10.10 Rimozione di una scansione pianificata

Nota
Non è possibile rimuovere le scansioni pianificate aggiunte tramite Sophos Enterprise Console.

- Per rimuovere una scansione pianificata da Sophos Anti-Virus, utilizzare il comando `savconfig` con l'opzione remove e il parametro NamedScans. Specificare il nome della scansione. Per esempio, per rimuovere la scansione Quotidiana, digitare: `/opt/sophos-av/bin/savconfig remove NamedScans Daily`.

10.11 Rimozione di tutte le scansioni pianificate

Nota
Non è possibile rimuovere le scansioni pianificate aggiunte tramite Sophos Enterprise Console.

- Per rimuovere tutte le scansioni pianificate da Sophos Anti-Virus, digitare: `/opt/sophos-av/bin/savconfig delete NamedScans`.

11 Appendice: configurazione degli allarmi

Nota
Quando si configura un singolo computer in rete, la configurazione potrebbe essere sovrascritta se il computer scarica una nuova configurazione per Enterprise Console.

È possibile configurare Sophos Anti-Virus in modo tale che invii allarmi nel caso in cui vengano rilevati virus o si verifichino errori di scansione, o di qualsiasi altro tipo. Gli allarmi possono essere inviati nei seguenti modi:

- Pop-up nel desktop (solo per la scansione in accesso).
- Riga di comando (solo per la scansione in accesso).
- E-mail (scansione in accesso e su richiesta).

Gli allarmi pop-up e da riga di comando vengono inviati nella lingua del computer in cui è stato rilevato l'allarme. Gli allarmi e-mail possono essere inviati sia in inglese che giapponese.

11.1 Configurazione di allarmi pop-up nel desktop

11.1.1 Disattivazione degli allarmi pop-up nel desktop

Per impostazione predefinita gli allarmi pop-up sono attivati

.

- Per disattivare gli allarmi pop-up, digitare: `/opt/sophos-av/bin/savconfig set UIpopupNotification disabled`
- Per disattivare sia allarmi pop-up nel desktop sia quelli da riga di comando, digitare: `/opt/sophos-av/bin/savconfig set UINotifier disabled`.

11.1.2 Specificare messaggi personalizzati

È possibile specificare un messaggio personalizzato che verrà aggiunto a tutti gli avvisi della riga di comando e a tutte le notifiche pop-up visualizzate sul desktop.

Nota
Il messaggio di avviso principale può essere visualizzato in lingue diverse (a seconda delle impostazioni di sistema), ma il testo personalizzato rimarrà nella lingua utilizzata nel momento in cui è stato specificato.

- Per specificare il messaggio personalizzato, utilizzare il parametro UIContactMessage. Per esempio, digitare: `/opt/sophos-av/bin/savconfig set UIContactMessage 'Contattare il supporto'`.

11.2 Configurazione degli allarmi da riga di comando

11.2.1 Disattivazione degli allarmi da riga di comando

Per impostazione predefinita gli allarmi da riga di comando sono attivati.

- Per disattivarli digitare gli allarmi da riga di comando, digitare: `/opt/sophos-av/bin/savconfig set UIttyNotification disabled`.
- Per disattivare sia allarmi pop-up nel desktop sia quelli da riga di comando, digitare: `/opt/sophos-av/bin/savconfig set UINotifier disabled`.

11.2.2 Specificare messaggi personalizzati

È possibile specificare un messaggio personalizzato che verrà aggiunto a tutti gli avvisi della riga di comando e a tutte le notifiche pop-up visualizzate sul desktop.

Nota
Il messaggio di avviso principale può essere visualizzato in lingue diverse (a seconda delle impostazioni di sistema), ma il testo personalizzato rimarrà nella lingua utilizzata nel momento in cui è stato specificato.

- Per specificare il messaggio personalizzato, utilizzare il parametro UIContactMessage. Per esempio, digitare: `/opt/sophos-av/bin/savconfig set UIContactMessage 'Contattare il supporto'`.

11.3 Configurazione degli allarmi e-mail

11.3.1 Disattivazione allarmi e-mail

Per impostazione predefinita gli allarmi e-mail sono attivati.

- Per disattivarli digitare: `/opt/sophos-av/bin/savconfig set EmailNotifier disabled`.

11.3.2 Specificazione del nome host o dell'indirizzo IP del server SMTP

Per impostazione predefinita, il nome host e la porta del server SMTP sono localhost:25.

- Per specificare il nome host o l'indirizzo IP del server SMTP, utilizzare il parametro EmailServer. Per esempio, digitare: `/opt/sophos-av/bin/savconfig set EmailServer 171.17.31.184`.

11.3.3 Specificazione della lingua

Per impostazione predefinita, i messaggi di allarme sono in lingua inglese.

- Per specificare la lingua da utilizzare nei messaggi di allarme, modificare il parametro EmailLanguage. Solo `English` o `Japanese` sono attualmente valori validi. Per esempio, digitare: `/opt/sophos-av/bin/savconfig set EmailLanguage Japanese`.

  Nota
  La lingua selezionata con questa opzione è applicabile solo al messaggio di allarme e non a quello personalizzato che viene aggiunto al messaggio di allarme e incluso in ogni e-mail di allarme.

11.3.4 Specificazione dei destinatari e-mail

Per impostazione predefinita gli allarmi e-mail vengono inviati a root@localhost.

- Per aggiungere un indirizzo all'elenco dei destinatari degli allarmi e-mail, utilizzare il parametro Email insieme all'operazione aggiungi. Per esempio, digitare: `/opt/sophos-av/bin/savconfig add Email admin@localhost`.

  Nota
  nello stesso comando è possibile specificare più destinatari, separandoli con uno spazio.

- Per eliminare un indirizzo dall'elenco, utilizzare il parametro Email congiuntamente all'operazione remove. Per esempio, digitare: `/opt/sophos-av/bin/savconfig remove Email admin@localhost`.

  Importante
  Non è possibile rimuovere root@localhost con questo comando. Per svolgere questa operazione occorre sovrascrivere completamente l'elenco con il seguente comando: `/opt/sophos-av/bin/savconfig set Email <indirizzo e-mail>`.

11.3.5 Indirizzo e-mail Sender

Per impostazione predefinita gli allarmi e-mail vengono inviati da root@localhost.

- Per indicare un indirizzo e-mail Sender, utilizzare il parametro EmailSender. Per esempio, digitare: `/opt/sophos-av/bin/savconfig set EmailSender admin@localhost`.

11.3.6 Indirizzo e-mail ReplyTo

- Per indicare un indirizzo e-mail ReplyTo, utilizzare il parametro EmailReplyTo. Per esempio, digitare: `/opt/sophos-av/bin/savconfig set EmailReplyTo admin@localhost`.

11.3.7 Indicare cosa accade se i virus vengono rilevati in accesso

Per impostazione predefinita, Sophos Anti-Virus invia allarmi e-mail nel caso in cui la scansione in accesso abbia rilevato un virus. Ciascun messaggio di allarme include anche un messaggio personalizzato aggiuntivo in inglese. Il testo del messaggio personalizzato può essere modificato ma non viene tradotto.

- Per disattivare l'invio di allarmi email nel caso vengano rilevati virus, digitare: `/opt/sophos-av/bin/savconfig set SendThreatEmail disabled`.
- Per specificare il messaggio personalizzato, utilizzare il parametro ThreatMessage. Per esempio, digitare: `/opt/sophos-av/bin/savconfig set ThreatMessage 'Contattare il supporto'`.

11.3.8 Indicare cosa accade se si verifica errore di scansione in accesso

Per impostazione predefinita, Sophos Anti-Virus invia un allarme e-mail nel caso si verifichi un errore della scansione in accesso. Ciascun messaggio di allarme include anche un messaggio personalizzato aggiuntivo in inglese. Il testo del messaggio personalizzato può essere modificato ma non viene tradotto.

- Per disattivare l'invio di allarmi e-mail nel caso in cui si sia verificato un errore della scansione in accesso, digitare: `/opt/sophos-av/bin/savconfig set SendErrorEmail disabled`.
- Per specificare il messaggio personalizzato, utilizzare il parametro ScanErrorMessage. Per esempio, digitare: `/opt/sophos-av/bin/savconfig set ScanErrorMessage 'Contattare il supporto'`.

11.3.9 Disattivazione degli allarmi e-mail su richiesta

Per impostazione predefinita, Sophos Anti-Virus invia un'e-mail riassuntiva relativa alla scansione su richiesta eseguita se, e solo se, durante tale scansione sono stati rilevati virus.

- Per disattivare la funzione di invio di un'e-mail riassuntiva nel caso di rilevamento virus durante una scansione su richiesta, digitare: `/opt/sophos-av/bin/savconfig set EmailDemandSummaryIfThreat disabled`.

11.3.10 Evento registrato nel log

Per impostazione predefinita, Sophos Anti-Virus invia un'e-mail di allarme non appena un evento viene registrato nel log di Sophos Anti#Virus. Oltre al messaggio di allarme, l'e-mail di allarme include un messaggio personalizzato in lingua inglese. È possibile modificare il testo di tale messaggio personalizzato, ma non è possibile tradurlo in altre lingue.

- Per specificare il messaggio personalizzato, utilizzare il parametro LogMessage. Per esempio, digitare: `/opt/sophos-av/bin/savconfig set LogMessage 'Contattare il supporto'`.

12 Appendice: configurazione log

Nota
Quando si configura un singolo computer in rete, la configurazione potrebbe essere sovrascritta se il computer scarica una nuova configurazione per Sophos Enterprise Console.

Per impostazione predefinita, le attività di scansione vengono registrate nel log di Sophos Anti-Virus: `/opt/sophos-av/log/savd.log`. Quando raggiunge 1 MB di dimensioni, ne viene eseguito automaticamente il backup nella stessa directory e viene avviato un nuovo log.

- Per vedere il numero predefinito dei log che vengono conservati, digitare: `/opt/sophos-av/bin/savconfig -s query LogMaxSizeMB`.
- Per specificare il numero massimo di log che sono conservati, utilizzare il parametro LogMaxSizeMB. Per esempio, se si desidera che il numero massimo di log sia 50, digitare: `/opt/sophos-av/bin/savconfig set LogMaxSizeMB 50`.

13 Appendice: configurazione aggiornamenti

Importante
Se si gestisce Sophos Anti-Virus tramite Sophos Enterprise Console, è necessario configurare gli aggiornamenti utilizzando Sophos Enterprise Console. Per informazioni su come svolgere questa operazione, consultare la guida in linea di Sophos Enterprise Console invece che questa sezione.

13.1 Concetti di base

Server di aggiornamento

Il server di aggiornamento corrisponde al computer in cui è installato Sophos Anti-Virus e che funge da fonte di aggiornamento per altri computer. Tali computer possono essere sia server che client di aggiornamento, a seconda della mpdalità di distribuzione di Sophos Anti-Virus nella rete.

Client di aggiornamento

Il client di aggiornamento corrisponde al computer in cui è installato Sophos Anti-Virus e che non è fonte di aggiornamento per altri computer.

Fonte di aggiornamento primaria

La *fonte di aggiornamento primaria* corrisponde al percorso di aggiornamento cui un computer solitamente accede. È possibile che vengano richieste credenziali.

Fonte di aggiornamento secondaria

La *fonte di aggiornamento secondaria* corrisponde al percorso di aggiornamento cui un computer accede quando la fonte primaria non è disponibile. È possibile che vengano richieste credenziali.

13.2 Comando di configurazione savsetup

`savsetup` è un comando che consente la configurazione degli aggiornamenti. Utilizzarlo solo per eseguire le operazioni specifiche descritte nelle seguenti sottosezioni.

Benché consenta di accedere solo ad alcuni dei parametri cui si può accedere con `savconfig`, è più facile da utilizzare. Richiede all'utente i valori dei parametri, cui bisogna rispondere selezionando o digitando i valori. Per eseguire `savsetup`, digitare: `/opt/sophos-av/bin/savsetup`.

13.3 Verifica della configurazione dell'aggiornamento automatico per un computer

1. Nel computer che si desidera verificare, digitare: `/opt/sophos-av/bin/savsetup`.
   `savsetup` chiede di scegliere quale operazione si desidera intraprendere.
2. Selezionare **Auto-updating configuration**.
   `savsetup` chiede di scegliere quale operazione si desidera intraprendere.
3. Selezionare **Display update configuration** per visualizzare la configurazione corrente.

13.4 Configurazione del server degli aggiornamenti

È possibile utilizzare una qualsiasi installazione autonoma di Sophos Anti-Virus come server di aggiornamento per i computer in rete.

Nota
Il server di aggiornamento deve essere un computer a 64 bit, se utilizzato per tenere aggiornati client a 64 bit. Se il server di aggiornamento è un computer a 32 bit, non potrà scaricare aggiornamenti a 64 bit e, di conseguenza, non potrà tenere aggiornati i client.

1. Nel server di aggiornamento, digitare: `/opt/sophos-av/bin/savsetup`.
   `savsetup` chiede di scegliere quale operazione si desidera intraprendere.
2. Scegliere un'opzione e utilizzare i prompt per configurare il server degli aggiornamenti.

   Durante la configurazione degli aggiornamenti, se si esegue l'aggiornamento da Sophos, inserire nome il utente e la password presenti nel contratto di licenza. Se si eseguono gli aggiornamenti da un server degli aggiornamenti, specificare un indirizzo HTTP o un percorso UNC, a seconda di come è stato impostato il server di aggiornamento.
3. Per eseguire aggiornamenti per altri client di Sophos Anti-Virus:
   a) Copiare la directory cache locale (/opt/sophos-av/update/cache/) in un percorso diverso del filesystem.
      Questa operazione può essere automatizzata utilizzando uno script.
   b) Pubblicare tale percorso negli altri computer in rete tramite HTTP, SMB, NFS o altro. Questo percorso diventerà la directory di installazione centrale (CID)da cui i client scaricheranno gli aggiornamenti.

13.5 Configurazione di un singolo client di aggiornamento perché si aggiorni da un server di aggiornamento

Per configurare un singolo client di aggiornamento perché si aggiorni da un server di aggiornamento

1. Nel computer che si desidera configurare digitare: `/opt/sophos-av/bin/savsetup`.
   `savsetup` chiede di scegliere quale operazione si desidera intraprendere.
2. Selezionare **Auto-updating configuration**.
   `savsetup` chiede di scegliere quale operazione si desidera intraprendere.

3. Selezionare l'opzione per configurare la fonte degli aggiornamenti primaria (o secondaria) in modo che funga da server.
   `savsetup` chiede i dati della fonte di aggiornamento.
4. Inserire l'indirizzo della fonte e il nome utente e password, se necessari.

   Specificare un indirizzo HTTP o un percorso UNC, a seconda di come è stato impostato il server di aggiornamento.

   `Savsetup` chiede se sia necessario un proxy per accedere al server di aggiornamento.
5. Se si richiede un proxy, premere Y e immetterne i dati.

14 Appendice: configurazione di Sophos Live Protection

Nota
Quando si configura un singolo computer in rete, la configurazione potrebbe essere sovrascritta se il computer scarica una configurazione nuova di Sophos Enterprise Console.

Sophos Live Protection decide se un file sospetto rappresenta una minaccia e, quando ciò accade, agisce immediatamente secondo quanto specificato nella configurazione disinfezione di Sophos Anti-Virus.

Live Protection migliora il rilevamento di nuovo malware, senza il rischio di rilevamenti indesiderati. Questo avviene mediante ricerca istantanea in base alle più aggiornate versioni di malware conosciute. Quando viene identificato un nuovo malware, Sophos è in grado di inviare aggiornamenti entro pochi secondi.

Se la scansione antivirus su un computer ha identificato un file come sospetto, ma non riesce poi a determinare se sia pulito o malevolo, in base ai file di identità delle minacce (IDE) memorizzati nel computer, alcuni dati del file (come il checksum e altri attributi) vengono inviati a Sophos per un'ulteriore analisi.

La verifica “in-the-cloud” esegue la ricerca istantanea di un file sospetto nel database di SophosLabs. Se il file viene identificato come pulito o malevolo, la decisione viene inviata al computer e lo stato del file viene automaticamente aggiornato.

14.1 Verifica di Sophos Live Protection

Se è stata eseguita l'installazione di Sophos Anti-Virus per la prima volta, Sophos Live Protection sarà attivo per impostazione predefinita. Se invece è stato eseguito l'upgrade da una versione precedente di Sophos Anti-Virus, non sarà attivo.

- Per verificare le impostazioni di Live Protection, digitare: `/opt/sophos-av/bin/savconfig query LiveProtection`.

14.2 Attivazione e disattivazione di Sophos Live Protection

- Per attivare Live Protection, digitare: `/opt/sophos-av/bin/savconfig set LiveProtection true`.
- Per disattivare Live Protection, digitare: `/opt/sophos-av/bin/savconfig set LiveProtection false`.

15 Appendice: configurazione della scansione in accesso

Nota
Quando si configura un singolo computer in rete, la configurazione potrebbe essere sovrascritta se il computer scarica una nuova configurazione per Sophos Enterprise Console.

15.1 Modifica del metodo di intercettazione dei file della scansione in accesso

Se si effettua l'upgrade a una versione di kernel Linux che non supporta Talpa, è possibile effettuare Fanotify come metodo di intercettazione per i file della scansione in accesso.

Importante
L'utilizzo di Fanotify da parte di Sophos Anti-Virus è una funzionalità della versione beta non completamente supportata.

- Per utilizzare Fanotify come metodo di intercettazione per i file della scansione in accesso, digitare: `/opt/sophos-av/bin/savconfig set DisableFanotify false`.

15.2 Esclusione di file e directory dalla scansione

È possibile escludere directory e file dalla scansione in due modi:

- Utilizzando i nomi di file o directory.
- Utilizzando caratteri jolly.

Se si desidera escludere file e directory i cui nomi sono codificati non utilizzando UTF-8, consultare la sezione Indicare la codifica dei caratteri per i nomi di directory e file (pagina 32).

15.2.1 Utilizzo di nomi di file o directory

Nota
Quando si configura un singolo computer in rete, la configurazione potrebbe essere sovrascritta se il computer scarica una nuova configurazione per Sophos Enterprise Console.

- Per escludere un determinato file o directory, utilizzare il parametro ExcludeFilePaths con operatore add. Indicare una directory utilizzando la barra finale. Per esempio, per aggiungere il file `/tmp/report` all'elenco dei file e directory da escludere, digitare: `/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/report`.
  a) Per aggiungere il file `/tmp/report` all'elenco dei file e directory da escludere, digitare: `/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/report/`.

- Per rimuovere esclusioni dall'elenco, utilizzare il parametro ExcludeFilePaths con l'operatore remove. Per esempio, digitare: `/opt/sophos-av/bin/savconfig remove ExcludeFilePaths /tmp/report`.

15.2.2 Utilizzo di carattere jolly

Nota
Quando si configura un singolo computer in rete, la configurazione potrebbe essere sovrascritta se il computer scarica una configurazione nuova di Sophos Enterprise Console.

- Per escludere file e directory utilizzando caratteri jolly, utilizzare il parametro ExcludeFileOnGlob con l'operatore add. Caratteri jolly validi sono `*`, corrispondente a qualsiasi numero di caratteri e `?`, corrispondente a un carattere qualsiasi, Per esempio, per aggiungere tutti i file di testo presenti nella directory `/tmp` all'elenco dei file e directory da escludere, digitare: `/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob '/tmp/*.txt'`.

  Nota
  Se si utilizza ExcludeFileOnGlob per escludere una directory, è necessario aggiungere il carattere jolly `*` alla fine del percorso. Per esempio: `/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob '/tmp/report/*'`.

- Se l'espressione non viene racchiusa dalle virgolette, Linux espande l'espressione e passa l'elenco dei file a Sophos Anti-Virus. Ciò è utile per escludere solo i file già esistenti e per abilitare la scansione dei file che sono stati creati in un secondo tempo. Per esempio, per aggiungere tutti i file di testo già presenti nella directory `/tmp` all'elenco dei file e directory da escludere, digitare: `/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob /tmp/*.txt`.
- Per rimuovere esclusioni dall'elenco, utilizzare il parametro ExcludeFileOnGlob con l'operatore remove. Per esempio, digitare: `/opt/sophos-av/bin/savconfig remove ExcludeFileOnGlob '/tmp/notes.txt'`.

15.2.3 Indicare la codifica dei caratteri per i nomi di directory e file

Linux consente di attribuire nomi a directory e file utilizzando qualsiasi codifica dei caratteri si desideri (per es. UTF-8 o EUC_jp). Sophos Anti-Virus memorizza però le esclusioni solo in UTF-8. Di conseguenza, se si desidera escludere dalla scansione directory e file non codificati in UTF-8, specificare le esclusioni in UTF-8, quindi specificare le codifiche utilizzando il parametro ExclusionEncodings. I nomi delle directory e dei file esclusi verranno quindi valutati in base alla codifica specificata, procedendo così ad escludere directory e file corrispondenti. Ciò è applicabile per le esclusioni specificate utilizzando i parametri ExcludeFilePaths e ExcludeFileOnGlob. Per impostazione predefinita, UTF-8, EUC_jp e ISO-8859-1 (Latin-1) sono specificati.

Per esempio, se si desidera escludere directory e file il cui nome è codificato in EUC_cn, specificare i nomi di tali directory e file utilizzando il parametro ExcludeFilePaths e/o ExcludeFileOnGlob. Quindi aggiungere EUC_cn all'elenco delle codifiche: `/opt/sophos-av/bin/savconfig add ExclusionEncodings EUC_cn`.

Sophos Anti-Virus valuta quindi in UTF-8, EUC_jp, ISO-8859-1 (Latin-1) e EUC_cn tutti i nomi di directory e file specificati. Esclude quindi i nomi delle directory e file che corrispondono.

15.3 Esclusione di un tipo di filesystem dalla scansione

Per impostazione predefinita, non è escluso nessun tipo di filesystem.

- Per escludere un tipo di filesystem, utilizzare il parametro ExcludeFilesystems con operatore add. I tipi di filesystem validi sono elencati nel file /proc/filesystems. Per esempio, per aggiungere nfs all'elenco di tipi di filesystem da escludere, digitare: `/opt/sophos-av/bin/savconfig add ExcludeFilesystems nfs`.
- Per rimuovere esclusioni dall'elenco, utilizzare il parametro ExcludeFilesystems con l'operatore remove. Per esempio, digitare: `/opt/sophos-av/bin/savconfig remove ExcludeFilesystems nfs`.

15.4 Scansione degli archivi

Per impostazione predefinita, la scansione in accesso degli archivi è disattivato. Si consiglia però di attivarla nel caso cui si lavori con più file di archivio contemporaneamente, dal momento che, in una situazione di questo tipo, il mancato rilevamento di un virus potrebbe comportare danni gravi. Si potrebbe per esempio dover inviare un file di archivio a un contatto importante.

Nota
Si consiglia di non abilitare questa opzione, per le seguenti ragioni:

- La scansione degli archivi rallenta notevolmente le operazioni di scansione.
- Sia che questa opzione sia abilitata o meno, quando si apre un file estratto da un archivio, tale file viene sottoposto a scansione.

Nota
Il motore di rilevamento delle minacce effettua la scansione dei file di archivio solamente quando non superano gli 8GB (se decompressi). Ciò è perché supporta il formato di archivio ustar POSIX, che non permette l'uso di file di dimensioni superiori a questo limite.

- Per attivare la scansione degli archivi, digitare: `/opt/sophos-av/bin/savconfig set ScanArchives enabled`.
- Per disattivare la scansione degli archivi, digitare: `/opt/sophos-av/bin/savconfig set ScanArchives disabled`.

15.5 Disinfezione di file infetti

È possibile configurare una scansione in accesso per disinfettare (disinfetta o cancella) i file infetti. Per impostazione predefinita, la disinfezione è disabilitata.

Tutte le azioni compiute da Sophos Anti-Virus contro eventuali file infetti vengono registrate nel log di Sophos Anti-Virus.

Nota
è possibile attivare sia la disinfezione che la cancellazione contemporaneamente, ma si tratta di una scelta non consigliata. Nel caso si desideri procedere comunque, Sophos Anti-Virus effettuerà per prima cosa la disinfezione del file. Nel caso in cui tale operazione non riesca, ne effettuerà la cancellazione.

Nota
Sophos Anti-Virus è in grado di disinfettare o rimuovere i file durante la scansione "all'apertura" (quando i file vengono copiati, spostati o aperti). Non è in grado di fare ciò durante la scansione "alla chiusura" (quando vengono salvati o creati file). Ciò non rappresenta un problema durante l'uso normale, in quanto la scansione "all'apertura" non può essere disattivata centralmente sui computer Linux, e la disinfezione o la rimozione dei file avviene all'accesso successivo.

15.5.1 Disinfezione di file infetti e del settore di avvio

- Per *attivare* la disinfezione in accesso dei file infetti e dei boot sector, digitare: `/opt/sophos-av/bin/savconfig add AutomaticAction disinfect`.

  Importante
  Sophos Anti-Virus non chiede conferma prima di cancellare.

  Nota
  La disinfezione dei documenti infetti non annulla le modifiche che il virus può aver apportato al documento. Consultare Informazioni sulla disinfezione (pagina 12) per sapere come visualizzare, sul sito web di Sophos, i dettagli sugli effetti secondari dei virus.

- Per *disattivare* la disinfezione in accesso dei file infetti e dei boot sector, digitare: `/opt/sophos-av/bin/savconfig remove AutomaticAction disinfect`.

15.5.2 Rimozione di file infetti

Importante
Questa opzione deve essere utilizzata soltanto su consiglio del supporto tecnico di Sophos. Se il file infetto si trova in una casella di posta, Sophos Anti-Virus potrebbe cancellare l'intera casella di posta.

- Per *abilitare* la disinfezione in accesso dei file infetti, digitare: `/opt/sophos-av/bin/savconfig add AutomaticAction delete`.

  Importante
  Sophos Anti-Virus non chiede conferma prima di cancellare.

- Per *disabilitare* la disinfezione in accesso dei file infetti, digitare: `/opt/sophos-av/bin/savconfig remove AutomaticAction delete`.

16 Risoluzione dei problemi

Questa sezione spiega come risolvere i problemi che possono verificarsi durante l'utilizzo di Sophos Anti-Virus.

Per informazioni sui codici restituiti di Sophos Anti-Virus per le scansioni su richiesta, consultare la sezione Appendice: codici di ritorno della scansione su richiesta (pagina 41).

16.1 Impossibile eseguire un comando

Sintomi

Il computer non consente l'esecuzione di uno dei comando di Sophos Anti-Virus.

Causa

Ciò può essere dovuto alla mancanza di sufficienti privilegi.

Soluzione del problema

Accedere al computer come utente root.

16.2 Non è stata applicata la configurazione delle esclusioni

Sintomi

Tal volta, quando si configura Sophos Anti-Virus in modo tale che includa nella scansione in accesso file precedentemente esclusi, i file restano esclusi.

Causa

Probabilmente la cache dei file precedentemente sottoposti a scansione include ancora i file esclusi.

Soluzione del problema

A seconda del metodo di intercettazione della scansione in accesso utilizzato, eseguire una delle seguenti azioni:

- Se si esegue Talpa, provare a scaricare la cache. Per fare ciò, digitare: `echo 'disable' > /proc/sys/talpa/intercept-filters/Cache/status` `echo 'enable' > /proc/sys/talpa/intercept-filters/Cache/status`.

- Se si esegue Fanotify, provare a riavviare il servizio sav-protect già installato. Per fare ciò, digitare: `/etc/init.d/sav-protect restart`.

16.3 Report del computer “No manual entry for …”

Sintomi

Quando si cerca di visualizzare la pagina man di Sophos Anti-Virus, il computer visualizza un messaggio simile al seguente `No manual entry for ...`.

Causa

Ciò è probabilmente dovuto al fatto che la variabile ambientale *`MANPATH`* non include il percorso relativo alla pagina man.

Soluzione del problema

1. Se si esegue la shell sh, ksh o bash, aprire `/etc/profile` per eventuali modifiche.

   Se si esegue la shell csh o tcsh, aprire `/etc/profile` per eventuali modifiche.

   Nota
   Se non si è in possesso dello script di accesso o del profilo, eseguire i seguenti passaggi dal prompt dei comandi. È necessario ripetere questi passaggi ogni qualvolta il computer venga riavviato.

2. Verificare che la variabile ambientale MANPATH includa la directory `/usr/local/man`.
3. Se *`MANPATH`* non include questa directory, aggiungerla eseguendo la procedura riportata qui di seguito. Non modificare nessuna delle impostazioni esistenti.

   Se si esegue la shell sh, ksh o bash, digitare:

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

   Se si esegue la shell csh o tcsh, digitare:

   ```
   setenv MANPATH valori:/usr/local/man
   ```

   in cui la dicitura *`valori`* indica le impostazioni esistenti.
4. Salvare lo script di accesso o il profilo.

16.4 Non ha sufficiente spazio su disco

Sintomo

Sophos Anti-Virus esaurisce lo spazio su disco, probabilmente durante la scansione di archivi complessi.

Cause

Ciò si verifica per una delle ragioni riportate di seguito:

- Quando decomprime gli archivi, Sophos Anti-Virus utilizza la directory `/tmp` per memorizzare i risultati dell'elaborazione. Se questa directory non è molto grande, Sophos Anti-Virus può esaurire lo spazio su disco.
- Sophos Anti-Virus ha superato la quota dell'utente.

Soluzione del problema

Eseguire una delle seguenti operazioni:

- Ingrandire la directory `/tmp`.
- Aumentare la quota dell'utente.
- Cambiare la directory utilizzata da Sophos Anti-Virus per i risultati dell'elaborazione. È possibile svolgere questa operazione impostando la variabile ambientale *SAV_TMP*.

16.5 La scansione su richiesta è lenta

Questo problema può essere dovuto a uno dei seguenti motivi:

Sintomi

Sophos Anti-Virus impiega notevolmente più tempo per eseguire la scansione su richiesta.

Cause

Ciò si verifica per una delle ragioni riportate di seguito:

- Per impostazione predefinita, Sophos Anti-Virus esegue una scansione rapida solo delle parti dei file che hanno maggiori probabilità di contenere virus. Se la scansione è impostata come completa (tramite l'opzione -f), esamina tutto il file.
- Per impostazione predefinita, Sophos Anti-Virus esegue la scansione di determinati tipi di file. Se è configurata per esaminare *tutti* i tipi di file, il processo impiega più tempo.

Soluzione del problema

Eseguire una delle seguenti operazioni a seconda del caso:

- Non eseguire la scansione completa, a meno che non venga espressamente consigliato, per esempio dal supporto tecnico di Sophos.
- Per eseguire la scansione di file aventi estensioni specifiche, aggiungerle all'elenco dei tipi di file di cui Sophos Anti-Virus esegue la scansione per impostazione predefinita. Per ulteriori informazioni, consultare la sezione Scansione di una determinata directory o file (pagina 6).

16.6 Il programma di archiviazione esegue il backup di tutti i file sottoposti alla scansione su richiesta

Sintomi

Il programma di archiviazione esegue sempre il back up di tutti i file sottoposti a scansione su richiesta da parte di Sophos Anti-Virus.

Causa

Ciò è dovuto alle modifiche apportate da Sophos Anti-Virus all'orario “status-changed” dei file. Per impostazione predefinita, Sophos Anti-Virus tenta di reimpostare l'orario di accesso (atime) dei file sincronizzandolo con quello visualizzato prima della scansione. Tuttavia, ciò ha l'effetto di cambiare l'orario "status-changed" dell'inode (ctime). Se il programma di archiviazione utilizza ctime per stabilire se un file è stato modificato, questo esegue il back up di tutti i file sottoposti a scansione da Sophos Anti-Virus.

Soluzione del problema

Eseguire `savscan` con l'opzione --no-reset-atime.

16.7 Virus non rimosso

Sintomi

- Sophos Anti-Virus non ha eseguito la rimozione di un virus.
- Sophos Anti-Virus visualizza la dicitura `Disinfection failed` (disinfezione non riuscita).

Cause

Ciò si verifica per una delle ragioni riportate di seguito:

- La rimozione automatica non è stata abilitata.
- Sophos Anti-Virus non può eseguire la disinfezione di quel determinato tipo di virus.
- Il file infetto si trova su un supporto rimovibile, per es. un floppy disk o CD protetto da scrittura.
- Il file infetto si trova in un file system NTFS.
- Sophos Anti-Virus non esegue la rimozione di un frammento di virus, in quanto non è stato rilevato alcun virus a cui corrisponda perfettamente.

Soluzione del problema

Eseguire una delle seguenti operazioni a seconda del caso:

- Abilitare la rimozione automatica.
- Se possibile, rendere scrivibile il supporto rimovibile.
- Trattare i file che si trovano in un file system NTFS nel computer locale.

16.8 Frammento di virus rilevato

Sintomi

Sophos Anti-Virus segnala il rilevamento di un frammento di virus.

Cause

Ciò indica che parte di un file corrisponde a una parte di un virus. Questo è dovuto a una delle ragioni elencate di seguito:

- Molti virus nuovi si basano su virus già esistenti. Di conseguenza, frammenti di codice propri di un virus già noto possono fare parte di file contaminati da un nuovo virus.
- Molti virus contengono bug nelle loro routine di replicazione che fanno sì che questi virus infettino i file in modo non corretto. Una parte inattiva del virus (anche considerevole) potrebbe apparire all'interno del file che la ospita e venire rilevata da Sophos Anti-Virus.
- Quando si esegue una scansione completa, Sophos Anti-Virus può rilevare la presenza di un frammento di virus in un file di database.

Soluzione del problema

1. Eseguire l'aggiornamento di Sophos Anti-Virus nel computer infetto, in modo tale che sia in possesso dei dati sui virus più recenti.
2. Per eseguire la disinfezione del file, consultare la sezione Disinfezione di un determinato file infetto (pagina 13).
3. Se vengono segnalati ancora frammenti di virus, rivolgersi al supporto tecnico di Sophos per ricevere assistenza:

16.9 Consenso dell'accesso al disco

Sintomi

Impossibile accedere ai file in un disco rimovibile.

Causa

Per impostazione predefinita, Sophos Anti-Virus impedisce l'accesso ai supporti rimovibili i cui settori di avvio sono infetti.

Soluzione del problema

Per consentire l'accesso (per es. per copiare file da un floppy infetto da un virus del boot sector):

1. Digitare: `/opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat enabled`.
2. Una volta terminato l'accesso al disco, digitare: `/opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat disabled`.
3. Rimuovere il disco dal computer in modo tale che non possa tentare di reinfettare il computer al riavvio.

17 Appendice: codici di ritorno della scansione su richiesta

`savscan` genera un codice nella shell che indica il risultato della scansione. Una volta conclusa la scansione è possibile visualizzare il codice eseguendo un comando specifico, per esempio: `echo $?`.

Codice di ritorno	Descrizione
0	Non si è verificato alcun errore e non sono stati rilevati virus.
1	L'utente ha interrotto la scansione premendo CTRL+C.
2	Si è verificato un errore che non consente il completamento della scansione.
3	Rilevato virus.

17.1 Codici di ritorno estesi

`savscan`, se eseguito con l'opzione -eec, genera un codice più dettagliato di quello shell. Una volta conclusa la scansione è possibile visualizzare il codice eseguendo un comando specifico, per esempio: `echo $?`

Codice di ritorno esteso	Descrizione
0	Non si è verificato alcun errore e non sono stati rilevati virus
8	Si è verificato un errore reversibile
16	Rilevato file protetto da password (non ne viene eseguita la scansione)
20	Rilevato e disinfettato un oggetto contenente virus
24	Rilevato, ma non disinfettato un oggetto contenente virus
28	Virus rilevato nella memoria
32	Si è verificato un problema durante il controllo integrità
36	Si è verificato un errore irreversibile

Codice di ritorno esteso	Descrizione
40	Scansione interrotta

18 Appendice: configurazione della funzionalità "phone home"

Sophos Anti-Virus può contattare Sophos ed inviare informazioni relative ai prodotti e alle piattaforme in uso. La funzionalità "phone-home" è molto utile per migliorare i prodotti Sophos e l'esperienza utente.

Quando si effettua l'installazione Sophos Anti-Virus, la funzionalità "phone-home" è attivata per impostazione predefinita. Si consiglia di lasciarla attiva. Questa funzionalità non ha alcun impatto sui livelli di protezione o sulle performance dei computer:

- I dati vengono inviati in formato cifrato a un percorso sicuro dove vengono conservati per un massimo di tre mesi.
- I prodotti Sophos installati inviano, una volta a settimana, solo circa 2 KB di dati. La funzionalità "phone-home" entra in funzione a intervalli casuali, per evitare che più computer la utilizzino simultaneamente.

È possibile disattivare questa funzionalità in qualsiasi momento dopo avere completato l'installazione.

Per disattivare la funzionalità "phone-home", digitare: `/opt/sophos-av/bin/savconfig set DisableFeedback true`.

Per attivare nuovamente la funzionalità "phone-home", digitare: `/opt/sophos-av/bin/savconfig set DisableFeedback false`.

19 Appendice: configurazione dei riavvii per RMS

Se RMS (Remote Management System), responsabile della gestione delle comunicazioni col server, smette di funzionate o non viene avviato correttamente, un adattatore effettua il riavvio dei componenti di RMS: mrouter e magent.

ISe si desidera riavviare RMS periodicamente, aggiungere `RestartIntervalHours=<Ore>` a `$INST/etc/sophosmgmtd.conf`.

20 Glossario

virus del settore di avvio	Tipo di virus che sovverte le fasi iniziali del processo di avvio. Un virus del settore di avvio può attaccare sia il Master Boot Record che il settore di avvio di partizione.
directory di installazione centrale (CID)	Directory in cui vengono posizionati il software Sophos e i relativi aggiornamenti. I computer collegati in rete si aggiornano da tale directory.
disinfezione	La disinfezione rimuove un virus da un file o settore di avvio.
scansione in accesso	Il vostro principale metodo di protezione contro virus. Ogni qual volta si accede a un file (copia, salva, sposta o apri), Sophos Anti-Virus ne esegue la scansione e ne consente l'accesso solo se tale file non costituisce una minaccia per il computer.
scansione su richiesta	Scansione avviata dall'utente. È possibile utilizzare la scansione su richiesta per sottoporre a scansione qualsiasi elemento, da un solo file a tutto ciò che è contenuto nel proprio computer e per cui si dispone di autorizzazione per la lettura.
fonte degli aggiornamenti primaria	Posizione degli aggiornamenti cui un computer solitamente accede. È possibile che vengano richieste credenziali.
scansione pianificata	Scansione del computer, o di parti di esso, eseguita ad orari fissi.
fonte degli aggiornamenti secondaria	Posizione degli aggiornamenti cui un computer accede quando la fonte primaria non è disponibile. È possibile che vengano richieste credenziali.
Sophos Live Protection	Funzione che utilizza la tecnologia "in-the-cloud" per decidere all'istante se un file sospetto rappresenta una minaccia e intraprendere l'azione specificata nella configurazione di disinfezione di Sophos Anti-Virus.
client di aggiornamento	Il client di aggiornamento corrisponde al computer in cui è installato Sophos Anti-Virus e che non è fonte di aggiornamento per altri computer.
server di aggiornamento	Il client di aggiornamento corrisponde al computer in cui è installato Sophos Anti-Virus e che non è fonte di aggiornamento per altri computer. Tali computer possono essere sia server che client di aggiornamento, a seconda della modalità di distribuzione di Sophos Anti-Virus nella rete.
virus	programma che si replica autocopiandosi. Spesso i virus danneggiano i sistemi del computer o i dati

in essi contenuti. Necessitano di un programma host e infettano il computer solo quando tale programma viene eseguito. Alcuni virus si diffondono attraverso le reti autocopiandosi o autoinviandosi via e-mail. Il termine virus viene spesso utilizzato anche per riferirsi a virus, worm e trojan.

21 Supporto

È possibile ricevere supporto tecnico per i prodotti Sophos in ciascuno dei seguenti modi:

- Visitando la Sophos Community su community.sophos.com/ e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su www.sophos.com/it-it/support.aspx.
- Scaricando la documentazione del prodotto da www.sophos.com/it-it/support/documentation.aspx.
- Aprendo un ticket per il nostro supporto tecnico alla pagina https://secure2.sophos.com/it-it/support/contact-support/support-query.aspx.

22 Note legali

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

new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

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

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

Douglas C. Schmidt

GNU General Public License

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

libcap

Unless otherwise *explicitly* stated, the following text describes the licensed conditions under which the contents of this libcap release may be used and distributed:

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

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.
2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU General Public License (v2.0 - see below), in which case the provisions of the GNU GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential conflict between the GNU GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED "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(S) 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.

OpenSSL

OpenSSL copyright

LICENSE ISSUES

==========

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

OpenSSL license

==========

Copyright © 1998–2017 The OpenSSL Project. All rights reserved.

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

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

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

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

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

(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

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

Original SSLeay license

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared 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

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 rouines 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 licence 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 licence [including the GNU Public Licence.]

protobuf

This license applies to all parts of Protocol Buffers except the following:

- Atomicops support for generic gcc, located in src/google/protobuf/stubs/atomicops_internals_generic_gcc.h. This file is copyrighted by Red Hat Inc.

- Atomicops support for AIX/POWER, located in src/google/protobuf/stubs/atomicops_internals_power.h. This file is copyrighted by Bloomberg Finance LP.

Copyright 2014, 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)

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

Copyright (C) 1995-2017 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 Mark Adler

jloup@gzip.org madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files http://tools.ietf.org/html/rfc1950 (zlib format), rfc1951 (deflate format) and rfc1952 (gzip format).