

SOPHOS

Sophos Anti-Virus per UNIX manuale utente

Versione prodotto: 7

Data documento: gennaio 2011



Sommario

1	Informazioni sul manuale.....	3
2	Info su Sophos Anti-Virus per UNIX	4
3	Scansione su richiesta.....	6
4	Rilevamento virus.....	10
5	Rimozione virus.....	11
6	Visualizzazione del log di Sophos Anti-Virus	14
7	Aggiornamento immediato di Sophos Anti-Virus	15
8	Appendice A: codici di ritorno della scansione su richiesta.....	16
9	Appendice B: configurazione basata sulla CID.....	18
10	Appendice C: configurazione delle scansioni pianificate.....	23
11	Appendice D: Configurazione degli allarmi e-mail.....	27
12	Appendice E: configurazione log.....	29
13	Appendice F: configurazione aggiornamenti.....	30
14	Risoluzione dei problemi.....	33
15	Glossario.....	37
16	Supporto tecnico.....	39
17	Note legali.....	40

1 Informazioni sul manuale

Questo manuale spiega come configurare ed eseguire Sophos Anti-Virus per UNIX.

In questo manuale si presuppone che Sophos Anti-Virus venga installato e aggiornato da una cartella condivisa creata da Sophos Enterprise Console.

Per *installare* Sophos Anti-Virus, consultare la Guida di avvio di *Sophos Endpoint Security and Control per Linux, NetWare, and UNIX*.

La documentazione Sophos è reperibile online su www.sophos.it/support/docs/.

2 Info su Sophos Anti-Virus per UNIX

2.1 Operato di Sophos Anti-Virus

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

2.2 Protezione del computer da parte di Sophos Anti-Virus

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

Sophos Anti-Virus ha un'interfaccia della riga di comando. Ciò consente di accedere a tutte le funzionalità di Anti-Virus e di eseguire tutte le configurazioni.

Nota: 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 di Sophos Anti-Virus

Se i computer UNIX sono gestiti da Sophos Enterprise Console, configurare Sophos Anti-Virus eseguendo la procedura riportata di seguito:

- Configurare **scansioni pianificate, allarmi, log e aggiornamenti** centralmente da Enterprise Console. Per ulteriori informazioni, consultare la guida in linea di Enterprise Console.

Nota: queste funzioni comprendono anche alcuni parametri che non possono essere impostati tramite Enterprise Console. Per impostarli localmente utilizzare l'interfaccia della riga di comando di Sophos Anti-Virus in ciascun computer UNIX. Enterprise Console li ignora.

- Configurare la **scansione su richiesta** localmente, dall'interfaccia della riga di comando di Sophos Anti-Virus in ciascun computer UNIX.

Se in presenza di una rete di computer UNIX *non* gestita da Enterprise Console, configurare Sophos Anti-Virus eseguendo la procedura seguente:

- Configurare **scansioni pianificate, allarmi, log e aggiornamenti** centralmente modificando un file di configurazione nella directory di installazione centrale (CID) da cui i computer vengono aggiornati. Questa è la configurazione basata sulla CID.
- Configurare la **scansione su richiesta** localmente, dall'interfaccia della riga di comando di Sophos Anti-Virus in ciascun computer.

Nota: non usare la configurazione basata sulla CID a meno che non venga consigliata dal supporto tecnico, altrimenti non si potrà utilizzare Enterprise Console. Non è possibile eseguire la configurazione di Enterprise Console e quella basata sulla CID insieme.

Se in presenza di un computer UNIX autonomo *non* gestito da Enterprise Console, configurare tutte le funzionalità di Sophos Anti-Virus dall'interfaccia della riga di comando di Sophos Anti-Virus.

3 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, consultare l'[Appendice C: configurazione delle scansioni pianificate](#) a pagina 23.

3.1 Esecuzione delle scansioni su richiesta

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

3.1.1 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 Enterprise Console.

3.1.2 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.

3.1.3 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.

3.2 Configurazione della scansione su richiesta

In questa sezione, laddove *path* 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

3.2.1 Scansione di tutti i tipi di file

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

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

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

3.2.2 Scansione di un determinato tipo di file

Per impostazione dpredefinita, Sophos Anti-Virus esegue la scansione solo di eseguibili. Per visualizzare l'elenco completo di tutti i tipi di file che Sophos Anti-Virus sottopone a scansione per impostazione predefinita, digitare **savscan -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.

3.2.3 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**.

- ❖ Per sottoporre a scansione tutti i tipi di archivio, utilizzare l'opzione **-archive**. Tipo:
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.

3.2.4 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**.

- ❖ 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.

3.2.5 Scansione dei computer remoti

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

- ❖ Per sottoporre a scansione i computer remoti, utilizzare l'opzione **--no-stay-on-machine**. Tipo:

savscan percorso --no-stay-on-machine

3.2.6 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**. Tipo: **savscan percorso --no-follow-symlinks**

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

3.2.7 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**. Tipo:

savscan percorso --stay-on-filesystem

3.2.8 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
```

3.2.9 Scansione di tipi di file che UNIX definisce come eseguibili

Per impostazione predefinita, Sophos Anti-Virus non sottopone 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**. Tipo:

```
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**.

4 Rilevamento virus

Se durante la scansione su richiesta viene rilevato un virus, 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](#) a pagina 14).
- Invia un allarme a Enterprise Console, se gestito da Enterprise Console.
- Invia un allarme e-mail a root@localhost.
- visualizza un allarme da riga di comando. Il virus viene riportato nella riga che comincia con >>> seguite dalla dicitura Virus o Frammento di virus:

```
Utility SAVScan per la rilevazione dei virus
Versione 4.50.0 [Linux/Intel]
Versione virus data 4.50, febbraio 2010
Rileva 1375239 virus, cavalli di Troia e worm
Copyright (c) 1989-2010 Sophos Group. Tutti i diritti
riservati.

Ora di sistema 13:43:32, Data di sistema 02 marzo 2010

La directory dei file IDE è: /opt/sophos-av/lib/sav

Uso di IDE file nystate-d.ide
. . . . .
Uso di IDE file injec-lz.ide

Scansione rapida

>>> Virus "EICAR-AV-Test" rilevato nel file
/usr/mydirectory/eicar.src

33 file esaminati in 2 secondi.
1 virus rilevato.
1 file su 33 era infetto.
Vi preghiamo di inviare i campioni infetti a Sophos per
l'analisi.
Per suggerimenti e consigli, consultare www.sophos.it oppure
e-mail\nsupport@sophos.it\n
Fine scansione.
```

Per informazioni sulla rimozione dei virus, consultare la sezione [Rimozione virus](#) a pagina 11.

5 Rimozione virus

5.1 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 (www.sophos.it/security/analyses).
2. Cercare l'analisi del virus utilizzando il nome rilevato da Sophos Anti-Virus.

5.2 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](#) a pagina 12) 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 *path* compare in un comando, fa riferimento al percorso da sottoporre a scansione.

5.2.1 Specificazione della messa in quarantena

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

5.2.2 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 `<tt>-r-----</tt>` (0400).

Se lo si preferisce, è possibile modificare la proprietà 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=nome utente
gid=nnn
group=nome gruppo
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.

5.3 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 scansione e registrate nel log di Sophos Anti-Virus. Per impostazione predefinita, la disinfezione è disabilitata.

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

5.3.1 Disinfezione di un determinato file infetto

- ❖ Per disinfettare un determinato file infetto, utilizzare l'opzione **-di**. Tipo:
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](#) a pagina 11 per sapere come visualizzare, sul sito web di Sophos, i dettagli sugli effetti secondari dei virus.

5.3.2 Disinfezione di tutti i file infetti 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](#) a pagina 11 per sapere come visualizzare, sul sito web di Sophos, i dettagli sugli effetti secondari dei virus.

5.3.3 Eliminazione di un determinato file infetto

- ❖ Per rimuovere un determinato file infetto, utilizzare l'opzione **-remove**. Tipo:

savscan percorso -remove

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

5.3.4 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.

5.4 Rimozione degli effetti secondari dei virus

La rimozione degli effetti secondari 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. Per assistenza rivolgersi al supporto tecnico di Sophos, consultare la sezione [Technical support](#) a pagina 39.

6 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 nel prompt dei comandi, 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

7 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.

8 Appendice A: 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

8.1 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

Codice di ritorno esteso	Descrizione
32	Si è verificato un problema durante il controllo integrità
36	Si è verificato un errore irreversibile
40	Scansione interrotta

9 Appendice B: configurazione basata sulla CID

La configurazione basata sulla directory di installazione centrale (CID) è un'alternativa a quella eseguita da Sophos Enterprise Console. È possibile utilizzarla per configurare tutte le funzioni, eccezion fatta per la scansione su richiesta, per cui si consiglia di consultare la sezione [Configurazione della scansione su richiesta](#) a pagina 6.

Nota: non usare la configurazione basata sulla CID a meno che non venga consigliata dal supporto tecnico, altrimenti non si potrà utilizzare Enterprise Console. Non è possibile eseguire la configurazione di Enterprise Console e quella basata sulla CID insieme.

La configurazione basata sulla CID non richiede l'utilizzo di un computer Windows. Consiste nell'effettuare modifiche a un file di configurazione memorizzato nella CID, impostando i valori dei parametri tramite il comando **savconfig** (consultare la sezione [comando di configurazione savconfig](#) a pagina 21). Quando i computer si aggiornano dalla CID, utilizzano tale configurazione.

I parametri sono anche bloccabili, in modo che non possano essere modificati nei computer client. In questo modo è possibile eseguire la configurazione di Sophos Anti-Virus in tutti i computer, evitando che le impostazioni vengano modificate dall'utente del computer.

I file di configurazione sono due: il file di configurazione online situato nella CID e quello offline, memorizzato altrove. Quando si desidera cambiare il file online, modificare il file offline e sostituire il file online con quest'ultimo. Le seguenti sezioni trattano questo argomento.

9.1 Creazione di una configurazione basata sulla CID

1. Utilizzare il comando **savconfig** per impostare il valore di ciascun parametro si desideri comprendere nel file di configurazione offline.

Utilizzare la seguente sintassi:

```
/opt/sophos-av/bin/savconfig -f file-config -c valore parametro operazione
```

in cui:

- **-f** indica che l'impostazione deve essere applicata al file offline.
- *config-file* è il percorso del file offline, che si può trovare in qualsiasi directory esclusa la CID. **savconfig** crea il file.
- **-c** indica che si desidera accedere al livello Corporate del file offline (per ulteriori informazioni sui livelli, consultare la sezione *Livelli di configurazione* a pagina 21).
- *operation* può essere **set**, **update**, **add**, **remove** o **delete**.
- *parameter* è il parametro che si desidera impostare.
- *value* è il valore su cui si desidera impostare il parametro.

Per esempio, per creare un file denominato CIDconfig.cfg nella directory ./config e disabilitare gli allarmi e-mail, digitare:

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c set EmailNotifier Disabled
```

Per ulteriori informazioni sull'utilizzo di **savconfig**, consultare la sezione *comando di configurazione savconfig* a pagina 21.

2. Per visualizzare i valori del parametro, utilizzare l'operazione **query**. È possibile visualizzare il valore di un singolo parametro o di tutti. Per esempio, per visualizzare i valori di tutti i parametri impostati, digitare:

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c query
```

3. Completata l'impostazione dei parametri, aggiornare Sophos Anti-Virus:

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

4. Eseguire il comando **addcfg** con l'opzione **-f** e il percorso del file di configurazione offline:

```
/opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f config-file
```

5. Copiare nella CID la directory /opt/sophos-av/update/cache/Primary-unpacked/config.

La nuova configurazione è ora disponibile e i computer la potranno scaricare durante il prossimo aggiornamento.

9.2 Aggiornamento di una configurazione basata su CID

1. Utilizzare il comando **savconfig** per impostare il valore di ciascun parametro che si desidera includere nel file di configurazione offline.

Usare la seguente sintassi:

```
/opt/sophos-av/bin/savconfig -f file-config -c valore parametro operazione
```

in cui:

- **-f** indica che l'impostazione deve essere applicata al file offline.
- *config-file* è il percorso del file offline.
- **-c** indica che si desidera accedere al livello Corporate del file offline (per ulteriori informazioni sui livelli, consultare la sezione [Livelli di configurazione](#) a pagina 21).
- *operation* può essere **set**, **update**, **add**, **remove** o **delete**.
- *parameter* è il parametro che si desidera impostare.
- *value* è il valore su cui si desidera impostare il parametro.

Per esempio, per aggiornare un file denominato CIDconfig.cfg nella directory ./config e disabilitare gli allarmi e-mail, digitare:

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c set EmailNotifier Disabled
```

Nota: è necessario impostare *tutti* i parametri che si desidera conservare nel livello Corporate del file online e non solo quelli che si desidera aggiornare. Per utilizzare una copia del file di configurazione online corrente come file offline, copiare CorporateLayer.cfg in qualsiasi directory esclusa la CID. CorporateLayer.cfg si trova nella directory config nella CID.

Per informazioni su come utilizzare **savconfig**, consultare la sezione [comando di configurazione savconfig](#) a pagina 21.

2. Per visualizzare i valori del parametro, utilizzare l'operazione **query**. È possibile visualizzare il valore di un singolo parametro o di tutti. Per esempio, per visualizzare i valori di tutti i parametri impostati, digitare:

```
/opt/sophos-av/bin/savconfig -f ./config/CIDconfig.cfg -c query
```

3. Completata l'impostazione dei parametri, aggiornare Sophos Anti-Virus:
/opt/sophos-av/bin/savupdate
4. Eseguire il comando **addcfg** con l'opzione **-f** e il percorso del file di configurazione offline:
/opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f config-file
5. Copiare nella CID la directory /opt/sophos-av/update/cache/Primary-unpacked/config.
La nuova configurazione è ora disponibile e i computer la potranno scaricare durante il prossimo aggiornamento.

9.3 Livelli di configurazione

Ogni installazione di Sophos Anti-Virus include un file di configurazione locale in cui si trovano le impostazioni relative a tutte le funzioni di Sophos Anti-Virus, eccezion fatta per quelle riguardanti le scansioni su richiesta.

Ogni file di configurazione locale contiene diversi livelli:

- Sophos: livello sempre presente nel file. Include le impostazioni predefinite, che vengono modificate solo da Sophos.
- Corporate: livello presente se l'installazione viene configurata dalla CID.
- Corporate: livello presente se viene eseguita una configurazione a livello locale. Include le impostazioni che vengono applicate solamente all'installazione nel computer dell'utente.

Ogni livello utilizza gli stessi parametri, in modo che ciascuno di essi possa essere impostato in più di un livello. Tuttavia, quando Sophos Anti-Virus verifica il valore di un parametro, lo fa rispettando la gerarchia dei livelli:

- per impostazione predefinita il livello Corporate sovrascrive il livello User
- i livelli Corporate e User sovrascrivono il livello Sophos.

Per esempio, se un parametro è impostato in entrambi i livelli User e Corporate, viene utilizzato il valore del livello Corporate. Tuttavia è possibile sbloccare i valori di singoli parametri nel livello Corporate, in modo che possano essere sovrascritti.

Quando il file di configurazione locale viene aggiornato dal file di configurazione nella CID, il livello Corporate nel file locale viene sostituito da quello del file nella CID.

9.4 comando di configurazione savconfig

savconfig è il comando utilizzato per la configurazione di tutte le funzioni di Sophos Anti-Virus, eccezion fatta per la scansione su richiesta. Il percorso di questo comando è `/opt/sophos-av/bin`. L'utilizzo di questo comando per la configurazione di funzioni specifiche di Sophos Anti-Virus viene spiegato nel riepilogo di questa guida. Questa sottosezione spiega la sintassi.

La sintassi di **savconfig** è:

```
savconfig [opzione] ... [operazione] [parametro] [valore] ...
```

Per visualizzare l'elenco completo di opzioni, operazioni e parametri, digitare:

```
man savconfig
```

9.4.1 opzione

È possibile specificare una o più opzioni. Le opzioni sono principalmente associate ai *livelli* dei file di configurazione locale in ciascuna installazione. Per informazioni sui livelli, consultare la sezione [Livelli di configurazione](#) a pagina 21. Per impostazione predefinita, il comando accede al livello User. Se per esempio si desidera accedere al livello Corporate, utilizzare l'opzione `-c` o `--corporate`.

Per impostazione predefinita, i valori dei parametri nel livello Corporate sono bloccati, in modo che sovrascrivano quelli nel livello User. Se si desidera consentire la sovrascrittura, da parte degli utenti, di un'impostazione aziendale, utilizzare l'opzione **--nolock**. Per esempio, per impostare il valore di **LogMaxSizeMB** e consentirne la sovrascrittura, digitare:

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

Se si sta eseguendo Enterprise Console, è possibile visualizzare solo i valori relativi ai parametri del criterio anti-virus utilizzando l'opzione **--consoleav**. Digitare:

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

È possibile visualizzare solo i valori relativi al criterio di aggiornamento di Enterprise Console utilizzando l'opzione **--consoleupdate**. Digitare:

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

9.4.2 operazione

È possibile specificare una sola operazione. Le operazioni sono principalmente associate al modo in cui si desidera accedere a un parametro. Alcuni parametri possono avere un solo valore mentre altri ne possono avere diversi. Le operazioni consentono di aggiungere o rimuovere valori da un elenco. Per esempio, il parametro **Email** contiene un *elenco* di destinatari e-mail.

Per visualizzare i valori dei parametri, utilizzare l'operazione **query**. Per esempio, per visualizzare il valore del parametro **EmailNotifier**, digitare:

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

Se si sta eseguendo Enterprise Console, quando **savconfig** genera i valori dei parametri, quelli in conflitto con il relativo criterio di Enterprise Console sono chiaramente contrassegnati dalla dicitura "Conflict".

9.4.3 parametro

È possibile specificare un solo parametro. Per elencare tutti i parametri di base che sono impostabili, digitare:

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

Per alcuni parametri è necessario specificare parametri secondari.

9.4.4 valore

È possibile specificare uno o più valori che saranno assegnati a un parametro. Se un valore contiene degli spazi, è necessario racchiuderli entro apostrofi.

10 Appendice C: configurazione delle scansioni pianificate

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

Nota: Per eseguire la scansione dei computer a un orario prestabilito, è possibile utilizzare anche Enterprise Console o il comando **crontab**. Per informazioni, consultare la guida in oinea di Enterprise Console o l'[articolo 12176 della knowledge base del supporto Sophos](#) (in inglese). Le scansioni pianificate aggiunte tramite Enterprise Console vengono visualizzate con nomi che hanno come prefisso “SEC.” e possono essere aggiornate o rimosse solo utilizzando 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 un giorno 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 il percorso del file nel quale si desidera 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 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 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 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 Enterprise Console.

10.7 Aggiornamento di una scansione pianificata da un file

Nota: Non è possibile aggiornare le scansioni pianificate aggiunte tramite 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](#) a pagina 24.
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 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 un giorno e un orario.

3. Per completare la definizione, premere CTRL+D.

10.9 Rimozione di una scansione pianificata

Nota: Non è possibile rimuovere le scansioni pianificate aggiunte tramite 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
```

10.10 Rimozione di tutte le scansioni pianificate

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

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

11 Appendice D: Configurazione degli allarmi e-mail

Nota: quando si configura un singolo computer in rete, la configurazione potrebbe venire sovrascritta se il computer ne scarica una nuova basata sulla console o sulla CID.

È possibile configurare Sophos Anti-Virus in modo tale che invii allarmi e-mail nel caso in cui vengano rilevati virus o si verifichino errori di scansione, o di qualsiasi altro tipo. Gli allarmi e-mail possono essere inviati sia in inglese che giapponese.

11.1 Disattivazione allarmi e-mail

Per impostazione predefinita gli allarmi e-mail sono attivati.

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

11.2 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 Specificazione della lingua

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

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

Nota: questa selezione della lingua è applicabile solo al messaggio di allarme e non a quello personalizzato incluso in ogni e-mail di allarme e che si aggiunge al messaggio di allarme stesso.

11.4 Specificazione dei destinatari e-mail

Per impostazione predefinita, Sophos Anti-Virus invia allarmi e-mail a root@localhost.

- ❖ Per aggiungere un indirizzo all'elenco dei destinatari degli allarmi e-mail, utilizzare il parametro **Email** congiuntamente all'operazione **add**. 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`

11.5 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`

11.6 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 'Contact IT'`

12 Appendice E: configurazione log

Nota: quando si configura un singolo computer in rete, la configurazione potrebbe essere sovrascritta se il computer ne scarica una nuova basata sulla console o sulla CID.

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 F: configurazione aggiornamenti

Importante: Se si gestisce Sophos Anti-Virus tramite Sophos Enterprise Console, è necessario configurare gli aggiornamenti utilizzando Enterprise Console. Per informazioni su come svolgere questa operazione, consultare la guida in linea di 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 modalità 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. Possono servire delle credenziali di accesso.

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. Possono servire delle credenziali di accesso.

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 **Display update configuration** per visualizzare la configurazione corrente.

13.4 Configurazione di computer di aggiornamento multipli perché si aggiornino da un server di aggiornamento

Nota: se si desidera modificare la configurazione per un client di aggiornamento singolo, invece che questa sezione consultare [Configurazione di un singolo client di aggiornamento perché si aggiorni da un server di aggiornamento](#) a pagina 32.

Nel server di aggiornamento, aggiornare il file di configurazione offline, quindi applicare le modifiche al file di configurazione online, in modo che i client di aggiornamento eseguano il download al loro successivo aggiornamento. Nella procedura riportata qui di seguito, *config-file* rappresenta il percorso del file di configurazione offline.

Questa sezione presuppone che si desideri configurare la fonte degli aggiornamenti *primaria*. Se invece si desidera configurare la fonte degli aggiornamenti *secondaria*, utilizzare i relativi parametri. Per esempio, utilizzare **SecondaryUpdateSourcePath** invece di **PrimaryUpdateSourcePath**.

Per configurare client di aggiornamento multipli perché si aggiornino da un server di aggiornamento:

1. Impostare l'indirizzo della fonte di aggiornamento primaria sul percorso della CID, utilizzando il parametro **PrimaryUpdateSourcePath**. È possibile specificare un indirizzo HTTP o un percorso UNC, a seconda di come è stato impostato il server di aggiornamento. Per esempio, digitare:

```
/opt/sophos-av/bin/savconfig -f config-file -c set PrimaryUpdateSourcePath "http://www.mywebcid.com/cid"
```
2. Se la fonte di aggiornamento primaria richiede l'autenticazione, impostare nome utente e password utilizzando rispettivamente i parametri **PrimaryUpdateUsername** e **PrimaryUpdatePassword**. Per esempio, digitare:

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

```
/opt/sophos-av/bin/savconfig -f config-file -c set PrimaryUpdatePassword 'j23rjfwj'
```
3. Se si accede alla fonte di aggiornamento primaria tramite proxy, impostare indirizzo, nome utente e password del server proxy, utilizzando rispettivamente i parametri **PrimaryUpdateProxyAddress**, **PrimaryUpdateProxyUsername** e **PrimaryUpdateProxyPassword**. Per esempio, digitare:

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

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

```
/opt/sophos-av/bin/savconfig -f config-file -c set PrimaryUpdateProxyPassword 'fj202jrjf'
```
4. Completata l'impostazione dei parametri, aggiornare Sophos Anti-Virus:

```
/opt/sophos-av/bin/savupdate
```
5. Eseguire il comando **addcfg** con l'opzione **-f** e il percorso del file di configurazione offline:

```
/opt/sophos-av/update/cache/Primary-unpacked/addcfg.sh -f config-file
```

6. Copiare nella CID la directory `/opt/sophos-av/update/cache/Primary-unpacked/config`.
La nuova configurazione è ora disponibile e i computer la potranno scaricare durante il prossimo aggiornamento.

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

Nota: se si desidera modificare la configurazione per client di aggiornamento multipli, invece che questa sezione consultare [Configurazione di computer di aggiornamento multipli perché si aggiornino da un server di aggiornamento](#) a pagina 31.

1. Nel computer che si desidera configurare digitare:
`/opt/sophos-av/bin/savsetup`
savsetup chiede di scegliere quale operazione si desidera intraprendere.
2. Selezionare l'opzione per configurare la fonte degli aggiornamenti primaria (o secondaria) in modo che funga da server.
savsetup chiede di inserire i dati della fonte di aggiornamento.
3. Inserire l'indirizzo della fonte e il nome utente e password, se necessari.
È possibile 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.
4. Se è necessario un proxy, premere Y e digitarne i dati.

14 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 A: codici di ritorno della scansione su richiesta](#) a pagina 16.

14.1 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.

Risoluzione del problema

Accedere al computer come utente root.

14.2 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.

Risoluzione 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.

14.3 Sophos Anti-Virus non ha sufficiente spazio su disco

Sintomi

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.

Risoluzione 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`.

14.4 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.

Risoluzione 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 un determinato tipo di file](#) a pagina 7.

14.5 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.

Risoluzione del problema

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

14.6 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.

Risoluzione 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.

14.7 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.

Risoluzione 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](#) a pagina 12.
3. Se continuano ad essere rilevati frammenti di virus, rivolgersi al supporto tecnico di Sophos per ricevere assistenza [Supporto tecnico](#) a pagina 39.

15 Glossario

CID	V. "directory di installazione centrale".
Client di aggiornamento	Computer in cui è stato installato Sophos Anti-Virus e che non deve aggiornarsi da altri computer.
configurazione basata sulla CID	Configurazione che modifica il file di configurazione basato sulla CID impostando i valori dei parametri tramite il comando savconfig . Quando i computer si aggiornano dalla CID, utilizzano questo tipo di configurazione. In precedenza denominata "configurazione corporate".
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.
fonte degli aggiornamenti primaria	Posizione degli aggiornamenti cui un computer solitamente accede. Possono servire delle credenziali di accesso.
fonte degli aggiornamenti secondaria	Posizione degli aggiornamenti cui un computer accede quando la fonte primaria non è disponibile. Possono servire delle credenziali di accesso.
layer	Una delle tre sezioni del file di configurazione locale contenente impostazioni di particolare rilievo. Le impostazioni del Corporate layer sovrascrivono quelle contenute nello User layer che, a loro volta, sovrascrivono quelle del Sophos layer.
scansione pianificata	Scansione del computer, o di parti di esso, eseguita ad orari fissi.
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.
server di aggiornamento	Componente che scarica gli aggiornamenti da Sophos e aggiorna un insieme di posizioni di aggiornamento condivise nella rete. Sophos Update Manager and EM Library are update servers.
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.

16 Supporto tecnico

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

- Visitando la community SophosTalk su <http://community.sophos.com/> e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su <http://www.sophos.com/support/>.
- Scaricando la documentazione del prodotto su <http://www.sophos.com/support/docs/>.
- Inviando un'e-mail a support@sophos.com, indicando il o i numeri di versione del software Sophos in vostro possesso, i sistemi operativi e relativi livelli di patch, ed il testo di ogni messaggio di errore.

17 Note legali

Copyright © 2008-2011 Sophos Limited. Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la registrazione e altri mezzi, salvo che da un licenziatario autorizzato a riprodurre la documentazione in conformità con i termini della licenza, oppure previa autorizzazione scritta del titolare dei diritti d'autore.

Sophos e Sophos Anti-Virus sono marchi registrati di Sophos Limited. Tutti gli altri nomi citati di società e prodotti sono marchi o marchi registrati dei rispettivi titolari.

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993–2005, all rights reserved.

Since DOC software is open-source, free software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us¹⁰ know so we can promote your project in the DOC software success stories¹¹.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹² around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly,

and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, 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. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me²¹ know.

Douglas C. Schmidt²²

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. mailto:doc_group@cs.wustl.edu
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~schmidt/>

GNU General Public License

Some software programs are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or similar Free Software licenses which, among other rights, permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires for any software licensed under the GPL, which is

distributed to a user in an executable binary format, that the source code also be made available to those users. For any such software which is distributed along with this Sophos product, the source code is available by submitting a request to Sophos via email to savlinuxgpl@sophos.com. A copy of the GPL terms can be found at www.gnu.org/copyleft/gpl.html

libmagic – file type detection

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

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

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

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

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

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

OpenSSL cryptographic toolkit

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

OpenSSL license

Copyright © 1998–2006 The OpenSSL Project. Tutti i diritti riservati.

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

Original SSLeay license

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

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

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

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

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

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

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

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

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

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

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

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

The 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.]

pycrypto

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

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

--amk (www.amk.ca)

Python

PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, worldwide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright © 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009

Python Software Foundation; All Rights Reserved” are retained in Python alone or in any derivative version prepared by Licensee.

3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.
4. PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

TinyXML XML parser

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 compression tools

© 1995–2002 Jean-loup Gailly and Mark Adler

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

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

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

If you use the zlib library in a product, we would appreciate **not** receiving lengthy legal documents to sign. The sources are provided for free but without warranty of any kind. The library has been entirely written by Jean-loup Gailly and Mark Adler; it does not include third-party code.

If you redistribute modified sources, we would appreciate that you include in the file ChangeLog history information documenting your changes.

Indice

A

- aggiornamento
 - configurazione 30
 - immediato 15
- allarmi
 - e-mail 27
 - riga di comando 10
- allarmi da riga di comando 10
- allarmi e-mail 27
- analisi dei virus 11
- archivi
 - scansioni su richiesta 7

B

- backup dei file esaminati 35

C

- CLI (interfaccia riga di comando) 4
- codici di errore 16
- codici di ritorno 16
- computer remoti, scansioni su richiesta 8
- computer, scansioni su richiesta 6
- configurazione basata sulla CID 4, 18
- configurazione di Sophos Anti-Virus. 4, 18

D

- directory, scansioni su richiesta 6
- disinfezione
 - file infetti 12
- disinfezione di file infetti 12

E

- effetti secondari dei virus 13
- Enterprise Console 4
- esclusione di oggetti
 - scansioni su richiesta 8
- eseguibili di UNIX, scansioni su richiesta 9

F

- file infetti
 - disinfezione 12
 - messa in quarantena 11
 - rimozione 12, 13
- file, scansioni su richiesta 6
- filesystem, scansione su richiesta 6
- filesystem, scansioni su richiesta 8

I

- informazioni sulla disinfezione 11
- interfaccia riga di comando (CLI) 4

L

- livelli, nel file di configurazione 21
- log di Sophos Anti-Virus
 - configurazione 29
 - visualizzazione 14
- log, Sophos Anti-Virus
 - configurazione 29
 - visualizzazione 14

M

- man page not found 33
- messa in quarantena dei file infetti 11

N

- No manual entry for ... 33

O

- oggetti collegati da link simbolici, scansioni su richiesta 8

R

- rimozione di file infetti 12, 13

S

- savconfig 21
- savsetup 30
- scansione su richiesta lenta 34
- scansioni pianificate 23

scansioni su richiesta 6
 archivi 7
 computer 6
 computer remoti 8
 directory 6
 esclusione di oggetti 8
 eseguibili di UNIX 9
 file 6
 filesystem 6, 8
 oggetti collegati da link simbolici 8
 scansioni pianificate 23
 tipi di file 7, 9
Segnalato frammento, virus 36

spazio su disco insufficiente 34

T

tipi di file, scansioni su richiesta 7, 9

V

virus
 analisi 11
 effetti secondari 13
 frammento segnalato 36
 non rimosso 35
 rilevati 10, 28