

SOPHOS



sophos **anti-virus**

Guida di avvio

UNIX o Linux

Versione documento 1.0



Informazioni sulla guida

Questa guida spiega come eseguire le seguenti operazioni su un singolo computer con sistema operativo UNIX:

- installazione di Sophos Anti-Virus
- aggiunta dei file di identità dei virus più recenti
- scansione antivirus del computer
- rimozione dei virus
- aggiornamento di Sophos Anti-Virus
- disinstallazione di Sophos Anti-Virus.

Inoltre spiega come eseguire

- l'installazione di Sophos Anti-Virus su molteplici computer con sistema operativo UNIX
- impostare la reportistica centralizzata dalle workstation con sistema operativo diverso da UNIX
- specificare le opzioni di installazione non predefinite

Ulteriori dettagli su tutte le altre opzioni di configurazione si possono trovare in *Sophos Anti-Virus UNIX user manual* (inglese).

- ❗ Se si desidera installare e aggiornare Sophos Anti-Virus automaticamente utilizzando EM Library, consultare la *Guida di avvio di Sophos Anti-Virus* disponibile sul CD Sophos Anti-Virus Network Install.

La documentazione di Sophos viene pubblicata su www.sophos.it/support/docs/ e sui CD Sophos.

Sommario

1 Installazione di Sophos Anti-Virus	3
2 Aggiunta dei file di identità dei virus (IDE) più recenti	7
3 Scansione antivirus del computer	9
4 Rimozione dei virus	10
5 Aggiornamento di Sophos Anti-Virus	11
6 Disinstallazione di Sophos Anti-Virus	15

Appendici

Appendice 1 Installazione su molteplici computer con sistema operativo UNIX	17
Appendice 2 Installazione delle funzioni di reportistica centralizzata	18
Appendice 3 Opzioni di installazione non predefinite	20

1 Installazione di Sophos Anti-Virus

Se si dispone di molteplici computer con sistema operativo UNIX collegati alla rete, e si desidera installare e aggiornare Sophos Anti-Virus da una directory centrale, anziché eseguire l'installazione su ogni computer separatamente, passare all'[appendice 1](#).

- ❗ InterCheck Server è un daemon che viene eseguito sul server UNIX, ed elabora gli allarmi virus inviati dalle workstation con sistema operativo Windows, Macintosh e OS/2. Non è essenziale per il funzionamento e l'aggiornamento di Sophos Anti-Virus. Per utilizzarlo, è necessario impostare un utente e un gruppo per il daemon, e le autorizzazioni su una directory comune. Consultare l'[appendice 2](#).

Il processo di installazione di Sophos Anti-Virus comprende tre fasi:

- Estrazione dei file di installazione (sezione 1.1).
- Installazione di Sophos Anti-Virus (sezione 1.2).
- Verifica delle impostazioni di sistema (sezione 1.3).

1.1 Estrazione dei file di installazione

Estrarre i file di installazione dal CD Supplementare Sophos Anti-Virus nel modo seguente:

1. Aprire una sessione sul computer con privilegi di root, ovvero di Superuser, e inserire il CD Supplementare Sophos Anti-Virus.
2. Montare il CD Supplementare Sophos Anti-Virus e inserire il comando `list` per visualizzare il contenuto della subdirectory `unix`.
3. Selezionare il file di archivio per la propria versione di UNIX.

Per gli utenti di Linux su Intel:

Se si dispone di un sistema nuovo libc6 con glibc 2.2 o superiore, come RedHat 7 o superiore, è necessario


```
linux.intel.libc6.glibc.2.2.tar
```

Se si dispone di un vecchio sistema libc6, come RedHat 6, SUSE 6, o Slackware 7, è necessario

```
linux.intel.libc6.tar
```

Se non si dispone di un sistema libc6, è necessario

```
linux.intel.libc5.tar
```

-  Per verificare il tipo di sistema in uso, controllare se nella directory `/lib` è presente un file o un link chiamato `libc.so.6` o simile. La presenza del file indica che si tratta di un sistema libc6.

Per gli utenti di Linux su Alpha:

È necessario

```
linux.alpha.tar
```

4. Copiare il file di archivio appropriato nella directory `/tmp`.

5. Decomprimere il file di archivio e salvarlo in /tmp nel modo seguente

```
cd /tmp
tar xvf linux.intel.libc6.glibc.2.2.tar
```

oppure

```
cd /tmp
tar xvf linux.intel.libc6.tar
```

oppure

```
cd /tmp
tar xvf linux.intel.libc5.tar
```

oppure

```
cd /tmp
tar xvf linux.alpha.tar
```

Viene creata una directory `sav-install` all'interno della directory /tmp, che contiene i file di installazione estratti.

Ora installare Sophos Anti-Virus (sezione 1.2).

1.2 Installazione di Sophos Anti-Virus

Per installare Sophos Anti-Virus **senza** InterCheck Server (installazione consigliata), eseguire lo script di installazione nel modo seguente:

```
cd sav-install
./install.sh
```

Per installare Sophos Anti-Virus **con** InterCheck Server, eseguire lo script di installazione con l'opzione `-i` (è necessario aver seguito già le istruzioni contenute nell'[appendice 2.1](#)):

```
cd sav-install
./install.sh -i
```

Per informazioni su tutte le opzioni con le quali è possibile eseguire lo script di installazione, consultare l'[appendice 3](#).

Ora potrebbe essere visualizzato un avviso relativo alla variabile di ambiente MANPATH. Tuttavia, l'installazione verrà eseguita correttamente.

Lo script di installazione colloca

- i file binari in `/usr/local/bin`
- la library condivisa in `/usr/local/lib`
- i virus data in `/usr/local/sav`
- il manuale in `/usr/local/man`

Ora verificare le impostazioni di sistema (sezione 1.3).

1.3 Verifica delle impostazioni di sistema

Accertarsi che le variabili di ambiente nello script o profilo di accesso includano le directory utilizzate da Sophos Anti-Virus.

PATH deve includere `/usr/local/bin`

MANPATH deve includere `/usr/local/man`

Se una di queste variabili non è inclusa, aggiungerla alla variabile (o alle variabili) di ambiente, come esemplificato qui sotto. Non modificare alcuna delle impostazioni esistenti.

Se si esegue la shell sh, ksh, o bash, inserire

```
PATH=$PATH:/usr/local/bin
export PATH
```

Se si esegue la shell csh o tcsh, inserire

```
setenv PATH <values>:/usr/local/bin
```

in cui `<values>` sono le impostazioni esistenti.

Se Sophos Anti-Virus verrà eseguito da più utenti, è necessario rendere disponibili queste variabili a tutto il sistema. A questo scopo, modificare `/etc/login` oppure `/etc/profile`.

💡 Se non si dispone di uno script di accesso, sarà necessario resettare i valori ad ogni avvio del computer.

Ora aggiungere i file di identità dei virus (IDE) più recenti nel computer (sezione 2).

2 Aggiunta dei file di identità dei virus (IDE) più recenti

❓ Un **file di identità del virus (IDE)** è un file che consente a Sophos Anti-Virus di rilevare un determinato virus. I file IDE sono necessari per proteggere il computer dai virus scoperti dopo il rilascio della propria versione di Sophos Anti-Virus.

1. Aprire la pagina dei download sul sito web di Sophos (www.sophos.it/downloads/ide).
2. Scaricare il file compresso contenente i file IDE per la propria versione di Sophos Anti-Virus.
3. Estrarre i file IDE e salvarli nella directory `usr/local/sav`.



- ❗ Se lo si preferisce, scorrere la pagina verso il basso e scaricare i file IDE uno alla volta, nella suddetta posizione.
- ❗ Per assistenza per il download dei file IDE, consultare la knowledge base del supporto tecnico di Sophos (www.sophos.it/support/knowledgebase). Se si utilizza Internet Explorer 5.0, leggere l'articolo che spiega il motivo per cui i file IDE possono prendere un'estensione aggiuntiva al momento del download.

Per ulteriore assistenza per il download dei file IDE, contattare il [supporto tecnico](#) di Sophos.

Ora Sophos Anti-Virus è installato e aggiornato sul computer.

Se si *installa* Sophos Anti-Virus con le funzioni di reportistica centralizzata, ora è necessario attivare InterCheck Server ([appendice 2.2](#)). Se si *aggiorna* Sophos Anti-Virus con le funzioni di reportistica centralizzata, l'aggiornamento è terminato.

Per maggiori informazioni, consultare le seguenti sezioni della presente guida:

- La [sezione 3](#) spiega come effettuare una scansione antivirus del computer.
- La [sezione 4](#) spiega come rimuovere i virus.
- La [sezione 5](#) spiega come eseguire l'aggiornamento di Sophos Anti-Virus.
- La [sezione 6](#) spiega come disinstallare Sophos Anti-Virus.

3 Scansione antivirus del computer

Per eseguire una scansione sul computer locale, inserire

```
sweep /
```

Per eseguire la scansione di una directory o di un file particolare, utilizzare il percorso dell'oggetto da esaminare, per esempio

```
sweep /usr/mydirectory/myfile
```

Dopo la scansione, viene visualizzato un messaggio simile a quello che appare qui sotto

Se Sophos Anti-Virus ha rilevato un virus, lo segnala nella riga che inizia con >>> seguito da Virus o Frammento di virus:

```
Utilità per la rilevazione dei virus SWEEP
Versione 3.90.0 [Linux/Intel]
Virus data versione 3.90, Febbraio 2005
Rilevazione di 99603 virus, trojan e worm
Copyright (c) 1989-2005 Sophos Plc, www.sophos.com

Ora di sistema 09:35:55, Data di sistema 16 febbraio 2005

Scansione rapida

>>> Virus 'EICAR-AV-Test' rilevato nel file /home/source/eicar.src

33 file esaminati in 2 secondi.
1 virus scoperto.
1 file su 33 era infetto.
Inviare i campioni infetti a Sophos per l'analisi.
Per maggiori consigli, consultare www.sophos.com, inviare un'e-mail
a support@sophos.it o telefonare al numero +39 02 6628100
Fine di Sweep.
```

Per assistenza nell'utilizzo di Sophos Anti-Virus, inserire

```
sweep -h
```

4 Rimozione dei virus

Il metodo utilizzato per eliminare un virus con Sophos Anti-Virus varia a seconda che l'oggetto infetto sia un file dati (per esempio, un documento o un foglio elettronico) oppure un programma.

4.1 Rimozione di un virus da un file dati

Per eliminare un virus da un file dati, inserire

```
sweep <object> -di
```

in cui <object> è il percorso del file dati infetto.

In alternativa, per rilevare e rimuovere i virus da un file dati sul computer, inserire

```
sweep / -di
```

In ambedue i casi, Sophos Anti-Virus richiede la conferma prima di rimuovere il virus (o i virus).

- ❗ Quindi, verificare attentamente il file (o i file) dati. Sophos Anti-Virus rimuove il virus, ma non ne elimina gli effetti secondari. Per maggiori informazioni, controllare l'analisi del virus sul sito web di Sophos.

4.2 Rimozione di un virus da un programma

Per eliminare un virus da un programma, rimuovere il programma e sostituirlo con una copia di backup, oppure reinstallarlo dal disco originale.

Per rimuovere un programma infetto, inserire

```
sweep <object> -remove
```

in cui <object> è il programma infetto.

In alternativa, per rilevare e rimuovere i programmi infetti sul sistema, inserire

```
sweep / -remove
```

In ambedue i casi, Sophos Anti-Virus richiede la conferma prima di rimuovere il programma (o i programmi).

5 Aggiornamento di Sophos Anti-Virus

È necessario aggiornare Sophos Anti-Virus regolarmente per consentirgli di rilevare tutti i virus più recenti. Eseguire l'aggiornamento

- ogni mese, quando viene rilasciata la nuova versione di Sophos Anti-Virus (sezione 5.1)
- ogni volta che viene creato un nuovo e preoccupante virus che rappresenta un rischio per il proprio computer (sezione 5.2).

5.1 Aggiornamento mensile di Sophos Anti-Virus

Ogni mese viene rilasciata una nuova versione di Sophos Anti-Virus. Per scoprire le date di rilascio di Sophos Anti-Virus, visitare la pagina del sito web di Sophos (www.sophos.it/downloads/release_dates/).

Non appena viene rilasciata la nuova versione, procedere come segue:

- Scaricare ed estrarre i file di installazione (sezione 5.1.1).
- Aggiornare Sophos Anti-Virus (sezione 5.1.2).
- Scaricare il file compresso contenente i file IDE più recenti (sezione 2).

5.1.1 Download ed estrazione dei file di installazione

Scaricare ed estrarre i file di installazione dal sito web di Sophos nel seguente modo:

1. Cancellare tutti i file *.ide da `/usr/local/sav`.
2. Aprire una sessione sul computer con privilegi di root, ovvero di Superuser.

3. Andare alla pagina del sito web di Sophos dalla quale si possono scaricare i prodotti (www.sophos.it/support/updates). Salvare il file di archivio per la propria versione di UNIX nella directory `/tmp`.

Per gli utenti di Linux su Intel:

Se si dispone di un nuovo sistema libc6 con glibc 2.2 o superiore, come RedHat 7 o superiore, è necessario


Linux su Intel con libc6 (glibc 2.2)

Se si dispone di un vecchio sistema libc6, come RedHat 6, SUSE 6, o Slackware 7, è necessario

Linux su Intel con libc6

Se non si dispone di un sistema libc6, è necessario

Linux su Intel con libc5

-  Per verificare il tipo di sistema in uso, controllare se nella directory `/lib` è presente un file o un link chiamato `libc.so.6` o simile. La presenza del file indica che si tratta di un sistema libc6.

Per gli utenti di Linux su Alpha:

È necessario

Linux su Alpha

4. Decomprimere il file di archivio e salvarlo nella directory `/tmp` nel seguente modo

```
cd /tmp
uncompress linux.intel.libc6.glibc.2.2.tar.Z
tar xvf linux.intel.libc6.glibc.2.2.tar
```

oppure

```
cd /tmp
uncompress linux.intel.libc6.tar.Z
tar xvf linux.intel.libc6.tar
```

oppure

```
cd /tmp
uncompress linux.intel.libc5.tar.Z
tar xvf linux.intel.libc5.tar
```

oppure

```
cd /tmp
uncompress linux.alpha.tar.Z
tar xvf linux.alpha.tar
```

Viene creata una directory `sav-install` all'interno della directory `/tmp`, che contiene i file di installazione estratti.

Ora aggiornare Sophos Anti-Virus (sezione 5.1.2).

5.1.2 Aggiornamento di Sophos Anti-Virus

Per aggiornare Sophos Anti-Virus **senza** InterCheck Server (aggiornamento consigliato), eseguire lo script di installazione come segue:

```
cd sav-install
./install.sh
```

Per aggiornare Sophos Anti-Virus **con** InterCheck Server, eseguire lo script di installazione con l'opzione `-i`:

```
cd sav-install
./install.sh -i
```

Per informazioni su tutte le opzioni con le quali è possibile eseguire lo script di installazione, consultare l'[appendice 3](#).

Ora potrebbe essere visualizzato un avviso relativo alla variabile di ambiente `MANPATH`. Tuttavia, l'aggiornamento verrà eseguito correttamente.

Lo script di installazione colloca

- i file binari in `/usr/local/bin`
- la library condivisa in `/usr/local/lib`
- i virus data in `/usr/local/sav`
- il manuale in `/usr/local/man`

Ora scaricare il file compresso contenente i file IDE più recenti ([sezione 2](#)), che proteggeranno il computer dai virus scoperti dopo il rilascio della nuova versione di Sophos Anti-Virus.

5.2 Aggiornamento nel caso di un nuovo e preoccupante virus

Questo tipo di aggiornamento viene eseguito tra un aggiornamento principale e l'altro di Sophos Anti-Virus.

Ogni volta che compare un nuovo e preoccupante virus che mette a rischio il proprio computer, andare all'area download del sito web di Sophos (www.sophos.it/downloads/ide), scaricare il file IDE per il virus in questione e salvarlo nella cartella `usr/local/sav`.

- 🔔 Per ricevere le notifiche via e-mail sui file IDE e altri allarmi, registrarsi all'indirizzo www.sophos.com/virusinfo/notifications.

6 Disinstallazione di Sophos Anti-Virus

1. Rimuovere il programma `sweep` da `/usr/local/bin`.
 2. Rimuovere le library di Sophos Anti-Virus (`libsavi.*`) da `/usr/local/lib`.
 3. Rimuovere la directory di Sophos Anti-Virus `/usr/local/sav` e tutto il suo contenuto.
 4. Rimuovere il file di configurazione `/etc/sav.conf`.
 5. Rimuovere il manuale `/usr/local/man/man1/sweep.1`.
- Sophos Anti-Virus è stato rimosso dal computer.

Appendici

Installazione su molteplici computer con sistema operativo UNIX

Installazione delle funzioni di reportistica centralizzata

Opzioni di installazione non predefinite

Appendice 1 Installazione su molteplici computer con sistema operativo UNIX

Se si dispone di molteplici computer con sistema operativo UNIX collegati alla rete, è probabile che si desideri installare e aggiornare Sophos Anti-Virus da una directory centrale, anziché eseguire l'installazione su ogni computer separatamente.

- ❗ Questa procedura presuppone che tra i computer esista una trust relationship.
- 1. Su un computer con sistema operativo UNIX, impostare un'area condivisa disponibile per tutti gli altri computer.
- 2. Decomprimere l'archivio o gli archivi di distribuzione di Sophos Anti-Virus per UNIX e salvarli in quest'area.

Se si dispone di computer sulla rete che utilizzano più di un sistema operativo UNIX (per esempio, Linux e FreeBSD), decomprimere l'archivio di distribuzione per ogni sistema in una directory separata.

- 3. Utilizzare ssh per eseguire lo script `install.sh` su ogni computer con sistema operativo UNIX connesso alla rete, dall'area condivisa. Per esempio, inserire

```
ssh -l [nome utente] [nome host] / .install.sh
```

in cui `[nome utente]` è l'ID dell'utente e `[nome host]` è il computer sul quale si desidera installare Sophos Anti-Virus.

In ogni caso, accertarsi di eseguire `install.sh` dal gruppo corretto di file di distribuzione per il sistema operativo del computer.

- ❗ Sui vecchi computer con sistema operativo UNIX, ssh potrebbe non essere disponibile. È possibile utilizzare invece rsh, sebbene sia meno sicuro.
- ❗ Il punto 3 può essere inserito in uno script, eseguito da uno dei computer con sistema operativo UNIX.

Appendice 2 Installazione delle funzioni di reportistica centralizzata

InterCheck Server è un daemon che viene eseguito sul server UNIX, ed elabora gli allarmi virus inviati dalle workstation con sistema operativo Windows, Macintosh e OS/2. Per utilizzarlo, è necessario impostare un utente e un gruppo per il daemon, e le autorizzazioni su una directory comune.

La procedura di installazione di Sophos Anti-Virus con InterCheck Server comprende sei fasi:

- Preparazione all'installazione (appendice 2.1)
- Estrazione dei file di installazione ([sezione 1.1](#))
- Installazione di Sophos Anti-Virus ([sezione 1.2](#))
- Verifica delle impostazioni di sistema ([sezione 1.3](#))
- Aggiunta dei file di identità dei virus più recenti ([sezione 2](#))
- Attivazione delle funzioni di reportistica centralizzata (appendice 2.2).

Appendice 2.1 Preparazione all'installazione

Prima di installare Sophos Anti-Virus per UNIX, è necessario:

- creare un gruppo di utenti chiamato 'sweep'
- creare un utente chiamato 'sweep'. Il gruppo primario di questo utente deve essere 'sweep', e all'utente non deve essere consentito di aprire una sessione sul terminal. Se si desidera impostare la shell su `/bin/false`, consultare la documentazione di UNIX per informazioni sulla procedura.

Ora estrarre i file di installazione ([sezione 1.1](#)).

Appendice 2.2 Attivazione delle funzioni di reportistica centralizzata

Per utilizzare InterCheck Server, procedere nel modo seguente:

1. Esportare la directory `/var/spool/intercheck`, affinché sia visibile alle workstation con sistema operativo diverso da UNIX.
2. Avviare InterCheck Server. Inserire

```
icheckd
```

Per maggiori informazioni sul controllo e sulla configurazione della reportistica centralizzata, consultare *Sophos Anti-Virus UNIX user manual* (inglese).

Appendice 3 Opzioni di installazione non predefinite

È possibile specificare i file di Sophos Anti-Virus installati, e le directory nelle quali sono installati.

Per eseguire un'installazione non predefinita, eseguire lo script di installazione, `install.sh`, con una delle seguenti opzioni.

-d [prefisso]

Installa i programmi, la library, i virus data e il manuale in `[prefisso]/bin`, `[prefisso]/lib`, `[prefisso]/sav` e `[prefisso]/man`.

Non è necessario installare tutti questi file nella stessa directory. Vedere le opzioni `-b`, `-l`, `-m` e `-s`.

-b [directory]

Installa i programmi di scansione antivirus in `[directory]`.

Gli altri file vengono installati nella directory predefinita, salvo diversamente specificato con le opzioni `-l`, `-m` o `-s`.

-l [directory]

Installa la library di Sophos Anti-Virus in `[directory]`.

Gli altri file vengono installati nella directory predefinita, salvo diversamente specificato con le opzioni `-b`, `-m` o `-s`.

-m [directory]

Installa il manuale in `[directory]`.

Gli altri file vengono installati nella directory predefinita, salvo diversamente specificato con le opzioni `-b`, `-l` o `-s`.

-s [directory]

Installa i virus data in `[directory]`.

Gli altri file vengono installati nella directory predefinita, salvo diversamente specificato con le opzioni `-b`, `-l` o `-m`.

-i [directory]

Installa i file di InterCheck Server in `[directory]`. Se non è stata specificata alcuna directory, viene utilizzato il valore in `/etc/ichckd.conf`, o il

valore predefinito `/var/spool/intercheck`. Inoltre vengono installati il file binario `icheckd` e il manuale.

-ni

Non installa affatto InterCheck Server.

-ssi

Arresta e avvia InterCheck Server dopo l'installazione (impostazione predefinita, implica `-i`).

-nssi

Non arresta e avvia InterCheck Server dopo l'installazione.

-h

Stampa l'help.

-v

Funzionamento in modalità "verbose". Visualizza il percorso di ogni file dopo che è stato installato.

Supporto tecnico

Per informazioni sul supporto tecnico, visitare

www.sophos.it/support

Se si contatta il supporto tecnico, è necessario fornire il maggior numero possibile di informazioni: il numero (o i numeri) di versione del software Sophos, il sistema operativo (o i sistemi operativi), e la (o le) patch, nonché il testo esatto di tutti i messaggi di errore.

Copyright © 2005 by Sophos Plc

Tutti i diritti riservati. Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero di informazioni, o trasmessa in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la registrazione ed 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.