

KASPERSKY LAB

**Kaspersky Anti-Virus[®] 5.5 per Workstation e File
Server Linux e FreeBSD**

**GUIDA
DELL'AMMINISTRATORE**

KASPERSKY ANTI-VIRUS ® 5.5 PER
WORKSTATION E FILE SERVER LINUX E FREEBSD

Guida dell'amministratore

© Kaspersky Lab Ltd.
<http://www.kaspersky.com/>

Data revisione: Novembre, 2006

Sommario

CAPITOLO 1. INTRODUZIONE.....	6
1.1. Virus informatici e software nocivo	7
1.2. Scopo e funzioni principali di Kaspersky Anti-Virus	8
1.3. Novità della versione 5.5.....	8
1.4. Procedura di concessione della licenza	9
1.5. Requisiti hardware e software di sistema.....	9
1.6. Kit retail	11
1.7. Servizi per utenti registrati.....	11
1.8. Convenzioni utilizzate nel presente documento.....	12
CAPITOLO 2. ALGORITMO DELL'APPLICAZIONE.....	14
CAPITOLO 3. INSTALLAZIONE DI KASPERSKY ANTI-VIRUS.....	16
3.1. Installazione dell'applicazione su un computer operante in ambiente Linux	16
3.2. Installazione dell'applicazione su un computer operante in ambiente FreeBSD	17
3.3. Procedura di installazione	17
3.4. Aggiornamento dell'applicazione alla versione 5.5	18
3.5. Installazione della chiave di licenza	18
3.6. Ubicazione dei file dell'applicazione	19
3.7. Completamento dell'installazione	22
CAPITOLO 4. CONFIGURAZIONE DELL'APPLICAZIONE POST- INSTALLAZIONE	23
4.1. Configurazione predefinita dell'applicazione	23
4.2. Installazione del database anti-virus.....	24
4.3. Configurazione per utilizzare Kaspersky Anti-Virus con Webmin	24
CAPITOLO 5. UTILIZZO DI KASPERSKY ANTI-VIRUS.....	26
5.1. Aggiornamento del database anti-virus.....	26
5.1.1. Nuove funzionalità del componente di aggiornamento.....	27
5.1.2. Aggiornamento automatico del database anti-virus.....	28
5.1.3. Aggiornamento a richiesta del database anti-virus	30

5.1.4. Creazione di una cartella di rete per memorizzare e scaricare il database anti-virus.....	31
5.2. Protezione anti-virus dei file system	32
5.2.1. Area di analisi.....	33
5.2.2. Scansione degli oggetti e modalità di disinfezione	34
5.2.3. Possibili azioni sugli oggetti.....	35
5.2.4. Scansione a richiesta di una singola cartella.....	36
5.2.5. Scansione programmata	36
5.2.6. Funzionalità ulteriori: uso dei file script.....	37
5.2.6.1. Disinfezione di oggetti infetti all'interno di un archivio.....	37
5.2.6.2. Invio di notifiche all'amministratore.....	38
5.3. Protezione anti-virus in tempo reale	39
5.4. Gestione delle chiavi di licenza	40
5.4.1. Visualizzazione dei dettagli delle chiavi di licenza	40
5.4.2. Rinnovo della licenza.....	41
CAPITOLO 6. PARAMETRI SUPPLEMENTARI	43
6.1. Ottimizzazione del funzionamento di Kaspersky Anti-Virus	43
6.2. Trasferimento degli oggetti nella cartella Quarantine.....	45
6.3. Modalità di creazione di una copia di backup degli oggetti.....	46
6.4. Formato di data e ora	47
6.5. Impostazioni per la generazione dei report di Kaspersky Anti-Virus	47
CAPITOLO 7. DISINSTALLAZIONE DI KASPERSKY ANTI-VIRUS.....	50
CAPITOLO 8. VERIFICA DEL FUNZIONAMENTO DI KASPERSKY ANTI-VIRUS..	51
APPENDICE B. INFORMAZIONI SUPPLEMENTARI SULL'APPLICAZIONE	53
A.1. File di configurazione di Kaspersky Anti-Virus.....	53
A.2 Tasti modificatori della riga di comando per il componente kavscanner	61
A.3 Codici visualizzati per il componente kavscanner	65
A.4 Tasti modificatori della riga di comando del componente kavmonitor	66
A.5 Tasti modificatori della riga di comando per il componente licensemanager	66
A.6 Codici visualizzati per il componente licensemanager	67
A.7 Tasti modificatori della riga di comando del componente keepup2date	67
B.1.1.68	
A.8 Codici visualizzati per il componente keepup2date	68
APPENDICE C. DOMANDE FREQUENTI.....	70

APPENDICE D. KASPERSKY LAB.....	76
D.1.1. C.1 Altri prodotti Kaspersky Lab.....	77
D.1.2. Recapiti.....	85
APPENDICE E. CONTRATTO DI LICENZA.....	87

CAPITOLO 1. INTRODUZIONE

La costante crescita del numero di utenti di computer e le nuove possibilità di scambio dati attraverso la posta elettronica o Internet ha determinato un aumento della possibilità di contrarre virus e di essere vittima di danneggiamento o sottrazione di dati da parte di programmi informatici nocivi.

Tra le sorgenti di software nocivo che penetrano nei computer dell'utente, le più diffuse sono:

Internet

La rete informatica globale è la sorgente principale di distribuzione del software nocivo di tutti i tipi. In linea generale, i virus e gli altri programmi nocivi si insediano in siti web popolari, mascherandosi da software utile o gratuito. Il software nocivo si può trovare all'interno di numerosi script che si caricano automaticamente nel momento in cui il browser carica un sito web.

Messaggi e-mail

I messaggi e-mail inviati nella casella di posta dell'utente e memorizzati nei database di posta elettronica possono contenere dei virus. Il software nocivo può trovarsi all'interno degli allegati ai messaggi o nel corpo di un messaggio. In generale, le e-mail infette contengono virus o worm di posta. Quando si apre un messaggio e-mail o si salva un file allegato sul disco fisso, è possibile infettare i dati memorizzati nel computer.

Vulnerabilità del software

Nella maggior parte dei casi, gli attacchi degli hacker sfruttano i "buchi del software". Queste vulnerabilità consentono agli hacker di ottenere accesso remoto al computer e quindi ai dati dell'utente, alle risorse sulla LAN e ad altre fonti di informazioni.

Nei sistemi basati su Unix, i virus sono molto meno diffusi rispetto, per esempio, ai sistemi operativi Windows a causa delle peculiarità delle due piattaforme. Tuttavia, questo non significa che gli utenti Unix non siano soggetti a pericoli. Di seguito è illustrata una descrizione dettagliata dei tipi di software nocivo.

1.1. Virus informatici e software nocivo

Per poter essere consapevoli delle potenziali minacce a cui il computer è soggetto, è utile conoscere i tipi di software nocivo ("malware") esistenti e il relativo funzionamento. In generale, i programmi nocivi rientrano in una delle tre seguenti categorie:

- **Worm** – i programmi nocivi che appartengono a questa categoria si distribuiscono attraverso le risorse di rete. Questi programmi sono stati chiamati "worm" a causa della loro capacità di passare da un computer all'altro sfruttando le reti, la posta elettronica ed altri canali. Questa caratteristica, consente loro di proliferare in modo estremamente veloce.

I worm penetrano in un computer, determinano gli indirizzi IP di altri computer e inviano copie di se stessi a questi altri computer. Oltre agli indirizzi di rete, i worm spesso utilizzano i dati contenuti nelle rubriche dei client di posta installati sulla macchina infetta. Talvolta i worm creano file di lavoro sui dischi, ma possono funzionare anche senza utilizzare altre risorse del computer infetto ad eccezione della RAM.

- **Virus** – programmi che infettano altri programmi aggiungendo il loro codice al codice del programma infetto per ottenere il controllo della macchina nel momento in cui sono eseguiti i file infetti. Questa semplice definizione aiuta a stabilire che l'azione principale svolta da un virus è *infettare* i programmi sul computer. I virus si diffondono più lentamente dei worm.
- **Cavalli di troia o Trojan** – eseguono azioni non autorizzate sui computer infetti, per esempio, in funzione di condizioni particolari, possono cancellare dei dati sul disco fisso, "congelare" il sistema, sottrarre informazioni confidenziali, ecc. In senso stretto, I cavalli di troia non sono virus in quanto non infettano i programmi o i dati; non sono in grado di insinuarsi indipendentemente dei computer e pertanto sono distribuiti dagli hacker che li mascherano sotto forma di software "utile". Tuttavia, i Trojan possono infliggere più danni rispetto a un normale attacco di un virus.

Recentemente, *worm* e *Trojan* sono diventati il tipo più diffuso di software nocivo nei sistemi basati su Unix.



Da questo momento, nel presente testo, sarà utilizzato il termine "virus" per indicare virus, Trojan e worm. Il particolare tipo di software nocivo sarà menzionato solo quando necessario.

1.2. Scopo e funzioni principali di Kaspersky Anti-Virus

Kaspersky Anti-virus® per Workstation e File Server Linux e FreeBSD (di seguito definito *Kaspersky Anti-Virus, l'applicazione*) è concepito per proteggere file server e workstation con sistema operativo Linux o FreeBSD.

Kaspersky Anti-Virus per Linux e FreeBSD presenta le seguenti funzioni:

- *Protezione in tempo reale del file system contro codici nocivi:* intercettazione e analisi dei tentativi di accesso ai file, pulizia ed eliminazione degli oggetti infetti.
- *Analisi su richiesta degli oggetti:* ricerca dei file infetti o sospetti (inclusi i file nelle aree di ricerca specificate), analisi dei file, disinfezione o eliminazione degli oggetti infetti.
- *Quarantena degli oggetti sospetti e danneggiati:* i file sospetti vengono salvati in una directory Quarantine.
- Creazione di copie di backup degli oggetti infetti prima di disinfettarli o rimuoverli per consentire il ripristino degli oggetti contenenti dati utili.
- *Aggiornamento dei database anti-virus;* il database viene aggiornato dai server di aggiornamento Kaspersky Lab. L'utente può anche configurare l'applicazione in modo tale da aggiornare il database dalla cartella locale.
- *Controllo e configurazione di Kaspersky Anti-Virus* utilizzando il file di configurazione dell'applicazione e l'interfaccia basata su web Webmin.

1.3. Novità della versione 5.5

Rispetto alla versione 5.0, la versione 5.5 di **Kaspersky Anti-Virus per workstation e file server Linux/FreeBSD** presenta le seguenti migliorie:

- All'applicazione è stato aggiunto un nuovo componente, *kavmonitor*, che consente la protezione anti-virus dei file in tempo reale.
- Sono state implementate nuove tecnologie per scaricare gli aggiornamenti dei database anti-virus e dei moduli dell'applicazione inclusi controlli di integrità e controllo dell'utilizzabilità del data base scaricato. Questo garantisce un notevole snellimento del traffico di rete.
- Possibilità di selezionare il tipo di database anti-virus da scaricare (set standard o esteso). Questa opzione consente di individuare

singolarmente il set di database utilizzato da ogni componente dell'applicazione.

- Le procedure di installazione e rimozione dell'applicazione sono state semplificate.
- Possibilità di importare le impostazioni della versione precedente (5.0). Questo consente di accelerare considerevolmente il processo di configurazione.
- Possibilità di creare un'area di memorizzazione di backup per conservare le copie degli oggetti sospetti o infetti prima della loro disinfezione o rimozione. Questo consente il recupero dei dati originali qualora si verificassero errori durante la disinfezione degli oggetti.
- Introduzione della tecnologia del database iChecker e della cache di secondo livello degli oggetti analizzati per diminuire il sovraccarico della CPU durante l'analisi anti-virus.
- È stata aggiunta un'opzione che consente di limitare il numero di oggetti analizzati contemporaneamente in background per ottimizzare il carico del computer.
- La nuova versione consente di generare l'elenco dei virus rilevati.
- Estensione del set delle possibili azioni da eseguire quando vengono rilevati oggetti in vari stati.
- L'applicazione supporta ora una piattaforma a 64 bit.

Appendice C. Le opzioni di scansione a richiesta sono state perfezionate.

1.4. Procedura di concessione della licenza

La politica di concessione in licenza impone restrizioni sull'uso dell'applicazione in base al periodo di utilizzo (in regola generale, per un periodo di un anno dalla data di acquisto della licenza).

1.5. Requisiti hardware e software di sistema

I requisiti di sistema hardware e software minimi di **Kaspersky Anti-Virus** sono i seguenti:

- Requisiti hardware:
 - Processore classe Intel Pentium® 133 MHz o superiore;
 - 64 Mb di RAM.
 - 100 Mb di spazio libero su disco fisso per l'installazione dell'applicazione e la memorizzazione dei file temporanei.
- Requisiti software:
 - Per la piattaforma a 32 bit, uno dei seguenti sistemi operativi:
 - RedHat Linux versioni 9.0, Fedora Core 2, Advanced Server 3
 - RedHat Enterprise Linux Advanced Server 4 UPD3.
 - RedHat Fedora Core 5.
 - SuSE Linux versioni Enterprise Server 9.0, SP3.
 - Novell Linux Desktop 9.
 - SUSE Linux Professional 10.1.
 - Debian GNU/Linux versione 3.1 R2.
 - Mandrake Linux versione 10.1 2006.
 - FreeBSD versioni 4.11.
 - OpenBSD versione 3.6
 - Mandriva 2006 FreeBSD versione 4.11.
 - FreeBSD versione 5.4.
 - FreeBSD versione 6.1.
 - Per la piattaforma a 64 bit, uno dei seguenti sistemi operativi:
 - RedHat Enterprise Linux Advanced Server 4 UPD3.
 - RedHat Fedora Core 5.
 - SUSE Linux Professional 10.1.
 - SLES 9 SP3.
 - Il programma Webmin (www.webmin.com) per l'amministrazione remota di Kasperky Anti-Virus.
 - Perl versione 5.0 o superiore per l'installazione di Kaspersky Anti-Virus utilizzando *install.sh*. (www.perl.org)
 - Relative utility installate.

- Pacchetti di compilazione software installati (gcc, binutils, glibc-devel, make, ld) e codice kernel del sistema operativo preinstallato, necessari per utilizzare il componente *kavmonitor*.



Si noti che Kaspersky Anti-Virus non supporta il sistema SE Linux. L'utilizzo di SE Linux può causare la comparsa di vari messaggi di avvertenza nel file di sistema del report dell'applicazione.

1.6. Kit retail

Il software può essere acquistato dai nostri rivenditori (versione retail) o in uno dei nostri punti vendita online (per esempio, visitare il sito www.kaspersky.com, sezione **E-Store**).

Il pacchetto della versione retail comprende:

- Una busta sigillata contenente il CD di installazione dei file dell'applicazione software
- La guida dell'utente
- Una chiave di licenza memorizzata in un apposito dischetto
- Una scheda di registrazione (contenente il numero di serie del prodotto);
- Il contratto di licenza.



Prima di rompere il sigillo della busta del CD, leggere con attenzione il Contratto di licenza.

Se si acquista Kaspersky Anti-Virus online, scaricarla dal sito web di Kaspersky Lab. La copia, comprende anche la presente Guida. La chiave di licenza sarà inviata all'utente via posta elettronica dietro pagamento.

Contratto di licenza

Il Contratto di licenza è un contratto con valore legale tra l'utente e Kaspersky Lab che definisce i termini e le condizioni d'uso del prodotto anti-virus acquistato. Leggere attentamente il Contratto di Licenza!

In caso di mancata accettazione dei termini e delle condizioni del Contratto di licenza, l'utente può restituire la versione retail al distributore presso il quale lo aveva acquistato e riceverà il rimborso completo a condizione che la busta contenente il CD di installazione sia rimasta intatta.

L'apertura della busta sigillata contenente il CD di installazione (o i floppy disk) implica l'accettazione dei termini e delle condizioni del contratto di licenza.

1.7. Servizi per utenti registrati

Kaspersky Lab offre un ampio pacchetto di assistenza che consente ai propri utenti registrati di utilizzare con maggiore efficienza il software Kaspersky Anti-Virus.

Acquistando la licenza, si diventa un utente registrato e si ottiene il diritto ai seguenti servizi per tutto il periodo di validità della sottoscrizione:



- Ricevimento di nuove versioni del software acquistato;
- Supporto su aspetti legati a installazione, configurazione e utilizzo del software acquistato; questi servizi sono forniti via telefono o via e-mail.
- Informazioni sull'uscita di nuovi prodotti Kaspersky Lab e sulla comparsa di nuovi virus informatici in tutto il mondo (servizio riservato agli utenti iscritti alla newsletter di Kaspersky Lab).






Kaspersky Lab non fornisce assistenza per aspetti legati alle prestazioni e all'uso di sistemi operativi o altre tecnologie.

1.8. Convenzioni utilizzate nel presente documento

In tutta la presente Guida sono utilizzate varie convenzioni di formattazione in funzione dello scopo e del significato del testo. Tali convenzioni sono spiegate nella tabella sotto riportata.

Caratteristica di formattazione	Significato/Usò
Caratteri in grassetto	Titoli di menu, voci di menu, titoli di finestre, finestre di dialogo e relativi elementi, ecc.
 Nota.	Ulteriori informazioni, note.
 Attenzione!	Informazioni che richiedono particolare attenzione.

Caratteristica di formattazione	Significato/Usò
 <p><i>A tal fine...</i></p> <ol style="list-style-type: none"> 1. Passaggio 1. 2. ... 	<p>Descrizione in sequenza dei passaggi dell'utente e possibili azioni.</p>
 <p>Operazione, esempio</p>	<p>Illustrazione di un problema, esempio dimostrativo delle capacità dell'applicazione</p>
 <p>Soluzione</p>	<p>Implementazione dell'azione</p>
<p>[modificatore] – scopo del modificatore</p>	<p>Tasti modificatori delle righe di comando</p>
<p>Messaggi informativi e testo delle righe di comando</p>	<p>Testo dei file di configurazione, messaggi informative e riga di comando.</p>

CAPITOLO 2. ALGORITMO DELL'APPLICAZIONE

Prima di analizzare le funzioni di Kaspersky Anti-Virus, è opportuno illustrarne l'architettura interna. Questo consentirà di capire appieno l'algoritmo utilizzando nel funzionamento del programma Anti-Virus.

Kaspersky Anti-Virus include:

- Componente di scansione anti-virus su richiesta *kavscanner*,
- Componente di scansione anti-virus in tempo reale *kavmonitor*,
- Modulo di aggiornamento database anti-virus *keepup2date*,
- Utilità di gestione della chiave di licenza *licensemanager*,
- *Modulo di amministrazione remota* utilizzato con l'applicazione Webmin.

Segue una discussione dettagliata sull'algoritmo di funzionamento dell'applicazione, basato su un esempio di protezione in tempo reale (vale a dire, attraverso l'utilizzo del componente *kavmonitor*).

La procedura di funzionamento è la seguente:

1. Quando una qualsiasi applicazione del computer tenta di accedere a un oggetto del file system (richiesta di aprire, eseguire o chiudere un file) questa richiesta viene intercettata dal modulo kernel del componente *kavmonitor* e inviato per la scansione anti-virus.
2. Il file intercettato sarà poi elaborato utilizzando un'applicazione daemon inclusa nel componente *kavmonitor*. Il daemon analizza l'oggetto per verificare la presenza di attuali virus e lo elabora in base alle impostazioni specificate nel file di configurazione (compresa, senza tuttavia ad essa limitarsi, la disinfezione utilizzando il database anti-virus a condizione che questa opzione sia selezionata).
3. Una volta elaborato il file, il modulo kernel invierà a *kavmonitor* il codice di accesso (consentito/negato) che definisce lo stato del file.
4. In funzione dello stato dell'oggetto, il componente *kavmonitor* consente o blocca l'accesso al file (in caso di accesso negato, l'applicazione che richiede l'accesso riceverà un codice di errore (Accesso negato)).

Durante la scansione (e l'elaborazione), al file può essere assegnato uno dei seguenti stati:

- **Clean** – l'oggetto non è infetto.

- **Infected** – l'oggetto è infetto.
- **Cured** – l'oggetto è stato disinfettato con esito positivo.
- **CureFailed** – la disinfezione dell'oggetto non è riuscita.
- **Warning** – il codice dell'oggetto assomiglia a un virus noto.
- **Suspicion** – si sospetta che l'oggetto sia infetto da un virus sconosciuto.
- **Protected** – l'analisi dell'oggetto è impossibile perché è codificato.
- **Corrupted** – l'oggetto è danneggiato.
- **Error** – durante la scansione dell'oggetto si è verificato un errore di sistema.

Le azioni eseguite sull'oggetto in ogni particolare stato sono definite dalle impostazioni del file di configurazione (per i dettagli vedere Appendice A a pagina 53).

CAPITOLO 3. INSTALLAZIONE DI KASPERSKY ANTI-VIRUS

Prima di installare Kaspersky Anti-Virus, si consiglia di effettuare quanto segue sul sistema e di eseguire un controllo di sistema:

- Verificare che il sistema soddisfi i requisiti hardware e software minimi elencati nella sezione 1.5 a pag. 9. Qualora qualche applicazione, per esempio Perl, non sia ancora stata installata, si consiglia di installarla: in caso contrario, una parte delle funzionalità di Anti-Virus risulterà non disponibile.
- Configurare la connessione Internet.
- Collegarsi al sistema come **root**.

3.1. Installazione dell'applicazione su un computer operante in ambiente Linux

Kaspersky Antivirus per sistemi Linux è disponibile in due formati:

- **.rpm** – per sistemi che supportano RPM Package Manager;
- **.deb** – per pacchetti retail Debian.



Per avviare l'installazione di Kaspersky Anti-Virus dal pacchetto .rpm, immettere quanto segue nella riga di comando:

```
# rpm -i <distribution_package_filename>
```



Per avviare l'installazione di Kaspersky Anti-Virus dal pacchetto .deb, immettere quanto segue nella riga di comando:

```
# dpkg -i <distribution_package_filename>
```

3.2. Installazione dell'applicazione su un computer operante in ambiente FreeBSD

Il pacchetto retail di Kaspersky Anti-Virus è fornito in un pacchetto .pkg per computer che operano su sistemi operativi FreeBSD.



Per avviare l'installazione di Kaspersky Anti-Virus dal pacchetto .pkg, immettere la seguente riga di comando:

```
pkg_add <package_name>
```

3.3. Procedura di installazione

L'installazione dell'applicazione è *automatica*, seguire i passaggi sotto riportati:

1. Copiare i file di distribuzione sul computer.
2. Installare una chiave di licenza.

Se la chiave di licenza non è installata, la propria copia di Kaspersky Anti-Virus non funziona.

Se la chiave è temporaneamente non disponibile (per esempio se l'applicazione è stata acquistata via Internet e non si è ancora ricevuta la chiave di licenza via e-mail), è possibile installare la chiave in un secondo momento, ma comunque prima di iniziare effettivamente ad utilizzare l'applicazione (per maggiori informazioni sull'installazione della chiave di licenza, vedere la sezione 4.4. a pagina 39).

3. Configurare il componente di aggiornamento dei database anti-virus *keepup2date*.
4. Installare e aggiornare i database anti-virus.



Verificare che i database anti-virus siano installati prima di iniziare a utilizzare l'applicazione. L'analisi e l'elaborazione dei file non possono essere eseguiti senza i database anti-virus!

5. Installare il modulo Webmin.

Il modulo Webmin di amministrazione remota può essere installato *solo se durante l'installazione del pacchetto Webmin sono stati rispettati i percorsi predefiniti*. In seguito all'installazione, l'utente riceverà istruzioni

dettagliate su come configurare il modulo affinché funzioni con l'applicazione.



Quando si opera su sistemi operativi Linux, ricordare che durante l'aggiornamento del modulo kernel del sistema operativo, occorre aggiornare anche il modulo kernel del componente *kavmonitor*.

3.4. Aggiornamento dell'applicazione alla versione 5.5

Dopo l'installazione dell'applicazione, nel sistema vengono ricercate versioni precedenti di Kaspersky Anti-Virus eventualmente installate sul computer.

Se viene rilevata una versione precedente dell'applicazione, alcune impostazioni della versione esistente verranno importate nel file di configurazione della versione 5.5.



Il tool di installazione non rimuove il pacchetto retail della versione precedente di Kaspersky Anti-Virus. Questa attività deve essere svolta dall'amministratore.

Alcuni parametri standard del file di configurazione (per esempio il percorso alla directory contenente i database anti-virus) *non vengono esportati*, ma bensì determinati durante la procedura di installazione.

Inoltre, nella versione 5.5 rispetto alla 5.0, sono state introdotte alcune modifiche nella logica di funzionamento di determinati componenti. Pertanto, si raccomanda di verificare la correttezza del file di configurazione prima di utilizzare l'applicazione.

3.5. Installazione della chiave di licenza

Durante questa fase di installazione, la cartella corrente cercherà una chiave di licenza, cioè un file (con estensione *.key*) richiesto per il funzionamento di Kaspersky Anti-Virus. Il file consente la funzionalità completa dell'applicazione. È impossibile utilizzare Kaspersky Anti-Virus prima dell'installazione della chiave di licenza.

In caso di rilevamento della chiave di licenza, il tool di installazione riproduce il messaggio corrispondente sulla console e procede alla fase successiva, cioè l'installazione dei database anti-virus.

In caso di mancato rilevamento della chiave di licenza, il tool di installazione richiede di specificarne il percorso completo. Se non è disponibile alcuna chiave, saltare il passaggio della specificazione del percorso della chiave di licenza e proseguire con l'installazione dell'applicazione.

Quando si riceve la chiave di licenza, installarla immediatamente (per dettagli, vedere sezione 4.4 a pagina 39).

3.6. Ubicazione dei file dell'applicazione



Dopo aver installato Kaspersky Anti-Virus su una workstation con sistema operativo Linux, i file del pacchetto retail, come impostazione predefinita sono ubicati come segue:

/etc/opt/kaspersky/ – cartella contenente il file di configurazione di Kaspersky Anti-Virus:

kav4ws.conf – file di configurazione.

/opt/kaspersky/kav4ws/ – cartella principale di Kaspersky Anti-Virus contenente:

/bin/ – cartella contenente i file eseguibili di tutti i componenti di Kaspersky Anti-Virus:

kav4ws-kavscanner – file eseguibile del componente di protezione anti-virus;

kav4ws-keepup2date – file eseguibile del componente di aggiornamento del database anti-virus;

kav4ws-licensemanager – file eseguibile del componente di gestione delle chiavi di licenza.

/lib/ – cartella contenente i file ausiliari di Kaspersky Anti-Virus.

/man/ – cartella che contiene i file man.

/sbin/ – cartella che contiene i servizi ausiliari di Kaspersky Anti-Virus:

kav4ws-kavmonitor – file eseguibile del componente di protezione anti-virus.

/src/ – cartella che contiene il modulo kernel anti-virus dell'applicazione.

/opt/kaspersky/kav4ws/share/contrib/kav4ws.wbm – plugin per l'applicazione Webmin.

/opt/kaspersky/kav4ws/share/contrib/vox.sh – script *vox.sh*, utilizzato per disinfettare gli archivi.

/opt/kaspersky/kav4ws/share/doc/LICENSE – contratto di licenza.

/var/opt/kaspersky/kav4ws/bases – cartella che contiene il database anti-virus

`/var/opt/kaspersky/kav4ws/bases.backup` – cartella che contiene il database anti-virus aggiornato prima dell'ultimo aggiornamento.



Per collegare il sistema della guida di Kaspersky Anti-Virus (pagine del manuale), assegnare il valore `/opt/kaspersky/kav4ws/man` alla variabile ambientale `MANPATH`.



In seguito all'installazione di Kaspersky Anti-Virus su una workstation con sistema operativo FreeBSD, i file del pacchetto retail come impostazione predefinita saranno ubicati come segue:

`/usr/local/etc/kaspersky/` – cartella contenente il file di configurazione di Kaspersky Anti-Virus:

`kav4ws.conf` – file di configurazione.

`/usr/local/bin/` – cartella contenente i file eseguibili di tutti i componenti di Kaspersky Anti-Virus:

`kav4ws-kavscanner` – file eseguibile del componente di protezione anti-virus;

`kav4ws-keepup2date` – file eseguibile del componente di aggiornamento dei database anti-virus;

`kav4ws-licensemanager` – file eseguibile del componente di gestione delle chiavi di licenza.

`/usr/local/sbin/` – cartella che memorizza i servizi ausiliari di Kaspersky Anti-Virus:

`kav4ws-kavmonitor` – file eseguibile del componente di protezione anti-virus.

`/usr/local/man/` – cartella contenente i file man.

`/usr/local/src/kav4ws/` – cartella contenente il modulo kernel anti-virus dell'applicazione.

`/usr/local/share/kav4ws/contrib/kav4ws.wbm` – plugin per l'applicazione Webmin.

`/usr/local/share/kav4ws/contrib/vox.sh` – script `vox.sh`, utilizzato per disinfettare gli archivi.

`/usr/local/share/doc/kav4ws/LICENSE` – contratto di licenza.

`/var/db/kaspersky/kav4ws/bases` – cartella che memorizza il database anti-virus.

`/var/db/kaspersky/kav4ws/bases.backup` – cartella che memorizza il database anti-virus aggiornato prima dell'ultimo aggiornamento.



Dopo aver installato Kaspersky Anti-Virus su una workstation con sistema operativo Linux, i file del pacchetto retail, come impostazione predefinita sono ubicati come segue:

`/etc/opt/kaspersky/` – cartella contenente il file di configurazione di Kaspersky Anti-Virus:

kav4ws.conf – file di configurazione.

/opt/kaspersky/kav4ws/ – cartella principale di Kaspersky Anti-Virus contenente:

/bin/ – cartella contenente i file eseguibili di tutti i componenti di Kaspersky Anti-Virus:

kav4ws-kavscanner – file eseguibile del componente di protezione anti-virus;

kav4ws-keepup2date – file eseguibile del componente di aggiornamento del database anti-virus;

kav4ws-licensemanager – file eseguibile del componente di gestione delle chiavi di licenza.

/lib/ – cartella contenente i file ausiliari di Kaspersky Anti-Virus.

/man/ – cartella che contiene i file man.

/sbin/ – cartella che contiene i servizi ausiliari di Kaspersky Anti-Virus:

kav4ws-kavmonitor – file eseguibile del componente di protezione anti-virus.

/src/ – cartella che contiene il modulo kernel anti-virus dell'applicazione.

/opt/kaspersky/kav4ws/share/contrib/kav4ws.wbm – plugin per l'applicazione Webmin.

/opt/kaspersky/kav4ws/share/contrib/vox.sh – script *vox.sh*, utilizzato per disinfettare gli archivi.

/opt/kaspersky/kav4ws/share/doc/LICENSE – contratto di licenza.

/var/opt/kaspersky/kav4ws/bases – cartella che contiene il database anti-virus

/var/opt/kaspersky/kav4ws/bases.backup – cartella che contiene il database anti-virus aggiornato prima dell'ultimo aggiornamento.



Per collegare il sistema della guida di Kaspersky Anti-Virus (pagine del manuale), assegnare il valore ***/opt/kaspersky/kav4ws/man*** alla variabile ambientale ***MANPATH***.



In seguito all'installazione di Kaspersky Anti-Virus su una workstation con sistema operativo FreeBSD, i file del pacchetto retail come impostazione predefinita saranno ubicati come segue:

/usr/local/etc/kaspersky/ – cartella contenente il file di configurazione di Kaspersky Anti-Virus:

kav4fs.conf – file di configurazione.

/usr/local/bin/ – cartella contenente i file eseguibili di tutti i componenti di Kaspersky Anti-Virus:

kav4fs-kavscanner – file eseguibile del componente di protezione anti-virus;

kav4fs-keepup2date – file eseguibile del componente di aggiornamento dei database anti-virus;

kav4fs-licensemanager – file eseguibile del componente di gestione delle chiavi di licenza.

/usr/local/sbin/ – cartella che memorizza i servizi ausiliari di Kaspersky Anti-Virus:

kav4fs-kavmonitor – file eseguibile del componente di protezione anti-virus.

/usr/local/man/ – cartella contenente i file man.

/usr/local/src/kav4fs/ – cartella contenente il modulo kernel anti-virus dell'applicazione.

/usr/local/share/kav4ws/contrib/kav4fs.wbm – plugin per l'applicazione Webmin.

/usr/local/share/kav4fs/contrib/vox.sh – script *vox.sh*, utilizzato per disinfettare gli archivi.

/usr/local/share/doc/kav4fs/LICENSE – contratto di licenza.

/var/db/kaspersky/kav4fs/bases – cartella che memorizza il database anti-virus.

/var/db/kaspersky/kav4fs/bases.backup – cartella che memorizza il database anti-virus aggiornato prima dell'ultimo aggiornamento.



In futuro, a scopo esemplificativo, useremo i nomi dei componenti accettati per l'installazione su un server con sistema operativo Linux.

3.7. Completamento dell'installazione

Se tutti i passaggi di installazione sopra descritti sono stati completati con successo, sulla console viene visualizzato *un messaggio* che conferma l'esito positivo dell'installazione. Il file di configurazione incluso nel pacchetto retail contiene tutte le impostazioni necessarie per iniziare ad utilizzare l'applicazione. Tuttavia, alcune impostazioni utili per utilizzare appieno le funzionalità di Kaspersky Anti-Virus non vengono determinate durante la procedura di installazione. Pertanto, si raccomanda di eseguire la configurazione solo al termine della procedura di installazione (vedere capitolo 3 a pagina 23).

CAPITOLO 4. CONFIGURAZIONE DELL'APPLICAZIONE POST- INSTALLAZIONE

Il processo di installazione include l'analisi del sistema su cui è in corso l'installazione di Kaspersky Anti-Virus e determina automaticamente alcuni parametri di configurazione, mentre altre impostazioni del file di configurazione vengono configurate nel modo più pratico ai fini del funzionamento dell'anti-virus (vedere sezione 4.2 a pagina 23).

Il presente capitolo illustra le impostazioni predefinite di Kaspersky Anti-Virus e i *parametri che è opportuno che l'amministratore di sistema imposti prima di iniziare a utilizzare l'applicazione.*

4.1. Configurazione predefinita dell'applicazione

Tutte le impostazioni che definiscono il funzionamento di Kaspersky Anti-Virus sono memorizzate nel file di configurazione **kav4fs.conf** utilizzato come impostazione predefinita.

La configurazione di Kaspersky Anti-Virus è la seguente:

- All'avvio del sistema operativo, Kaspersky Anti-Virus si avvia automaticamente. L'applicazione intercetta tutte le richieste al file system e le analizza. Quando vengono rilevati oggetti infetti, sospetti o danneggiati, Kaspersky Anti-Virus riporta i messaggi corrispondenti nel file report **kavmonitor.log**.
- Se si avvia una scansione a richiesta senza utilizzare tasti modificatori supplementari della riga di comando, la scansione anti-virus delle cartelle e del file system del computer sarà eseguita a partire dalla cartella corrente. Messaggi contenenti l'esito della scansione saranno visualizzati sullo schermo e riportati nel file report **kavscanner.log**.



Si noti che gli oggetti infetti scoperti non vengono disinfettati o trasferiti nella cartella quarantene come impostazione predefinita!

4.2. Installazione del database anti-virus

L'applicazione rileva i virus e disinfetta gli oggetti infetti avvalendosi dei record dei propri database anti-virus, che contengono descrizioni di tutti i programmi nocivi correntemente noti e dei metodi da usare per la loro disinfezione. Pertanto, è fondamentale tenere aggiornati i database antivirus.



Ogni giorno compaiono nuovi virus. Si raccomanda di aggiornare il database anti-virus subito dopo l'installazione dell'applicazione in quanto il database incluso nel pacchetto retail sarà già obsoleto al momento dell'installazione.

Kaspersky Anti-Virus aggiorna il database anti-virus utilizzando il componente *keepup2date*. Per avviare il processo di aggiornamento, immettere quanto segue nella riga di comando:

```
/path/to/kav4fs-keepup2date
```

I database anti-virus saranno scaricati dai server di aggiornamento Kaspersky Lab in una directory speciale specificata nel file di configurazione.

4.3. Configurazione per utilizzare Kaspersky Anti-Virus con Webmin

Se si intende utilizzare il tool di amministrazione remota di Kaspersky Anti-Virus, si raccomanda di configurarlo per renderlo operativo con il pacchetto Webmin.

Per esempio, Webmin può essere utilizzato per limitare l'accesso al programma attraverso un sistema di password utenti.

Come impostazione predefinita, tutte le impostazioni dell'applicazione configurate in remoto da Webmin vengono salvate nel file di configurazione predefinito dell'applicazione.



Se si desidera creare un file di configurazione alternativo utilizzando Webmin, procedere come segue:

1. Copiare i dati dal file di configurazione esistente in un nuovo salvandolo con un altro nome. Dopodiché, modificare il nuovo file di configurazione (alternativo) come richiesto.

2. Specificare il nome del file di configurazione alternativo nel campo di immissione del parametro **Full path to KAV config** della scheda **Config edit**.



Consultare la documentazione di **Webmin** per ulteriori informazioni sulle sue impostazioni. Utilizzare la guida online di Webmin per informazioni sull'amministrazione remota dell'applicazione.

Di seguito, nell'ambito della descrizione delle impostazioni dell'applicazione e del relativo lancio, la presente guida **non** descriverà nel dettaglio la procedura per le operazioni remote via Webmin!

CAPITOLO 5. UTILIZZO DI KASPERSKY ANTI-VIRUS

Kaspersky Anti-Virus crea un sistema di protezione anti-virus per il computer che copre l'intera gamma di oggetti, dai singoli file all'intero file system.

Le funzionalità dell'applicazione comprendono operazioni che l'amministratore può eseguire utilizzando Kaspersky Anti-Virus. Queste operazioni possono essere suddivise nei seguenti gruppi :

- Aggiornamento dei database anti-virus utilizzati per l'analisi e la pulizia degli oggetti infetti (per i dettagli, vedere la sezione 5.1 a pagina 26).
- Protezione anti-virus dei file system su un computer, attraverso l'analisi programmata e/o su richiesta (per i dettagli, vedere la sezione 5.2 on page 32).
- Costante protezione anti-virus, vale a dire protezione in tempo reale .

Il presente capitolo contiene la descrizione di attività specifiche dell'applicazione, che l'amministratore può combinare o elaborare per un particolare contesto aziendale.

5.1. Aggiornamento del database anti-virus

L'aggiornamento del database anti-virus eseguito dal componente *keepup2date* dell'applicazione è un fattore integrato della protezione completa anti-virus. La sorgente utilizzata per l'aggiornamento del database sono i server di aggiornamento Kaspersky Lab. La lista di questi server comprende:

<http://downloads1.kaspersky-labs.com/updates/>

<http://downloads2.kaspersky-labs.com/updates/>

<ftp://downloads1.kaspersky-labs.com/updates/> e altri server.

Un elenco completo degli indirizzi da cui è possibile scaricare gli aggiornamenti è indicato nel file *updcfg.xml* incluso nel pacchetto dell'applicazione.

Durante la procedura di aggiornamento, il componente *keepup2date* seleziona un indirizzo e tenta di scaricare i database anti-virus dal server corrispondente. Se un tentativo di aggiornamento fallisce, *keepup2date* ripete il processo utilizzando l'indirizzo successivo.



Gli aggiornamenti del database anti-virus sono caricati sui server Kaspersky Lab a cadenza oraria.

Dopo un aggiornamento eseguito con successo, viene eseguito un comando specificato nel valore del parametro **PostUpdateCmd**, sezione **[updater.options]** del file di configurazione. Come impostazione predefinita, il comando avvia un ricaricamento automatico del database anti-virus. In caso di modifica non valida della suddetta impostazione, l'applicazione potrebbe non riuscire ad usare il database aggiornato o non funzionare correttamente.



Tutte le impostazioni del componente *keepup2date* sono raggruppate nelle opzioni **[updater.*]** del file di configurazione.

Se la struttura della LAN (rete locale) di cui si dispone è piuttosto complicata, si consiglia di scaricare gli aggiornamenti dei database anti-virus a cadenza oraria su una directory di rete e di configurare gli altri computer collegati in rete affinché copino gli aggiornamenti da quella directory. Per dettagli sulla creazione di una cartella di rete, vedere la sezione 5.1.4 on page 31.

La procedura di aggiornamento può essere programmata utilizzando la utility **cron** (vedere sezione 5.1.2 a pagina 28; in alternativa l'amministratore può scegliere di eseguirla manualmente (dalla riga di comando) (vedere sezione 5.1.3 a pagina 30).



Si raccomanda fortemente di configurare gli aggiornamenti del database in modo che vengano eseguiti a cadenza oraria!

5.1.1. Nuove funzionalità del componente di aggiornamento

Il componente di aggiornamento dei database anti-virus nella versione 5.5 di Kaspersky Anti-Virus è stato aggiornato rispetto alla versione precedente. Il nuovo componente presenta funzioni perfezionate e alcune nuove proprietà:

- L'opzione di selezione automatica del server di aggiornamento geograficamente più vicino, in base alla nazione specificata nel file di configurazione;
- L'opzione di scaricare e installare aggiornamenti incrementali quando si rendono disponibili aggiornamenti cumulativi, che può essere utile per l'economia del traffico;
- La capacità di ripristinare l'aggiornamento al punto in cui era stato interrotto in caso di caduta del collegamento durante lo scaricamento dei

database anti-virus o di modifica del server di aggiornamento. Dopo il ripristino del collegamento, il componente scarica solo la porzione residua dei database anti-virus anziché ricominciare da capo;

- Un controllo di integrità dei database scaricati;
- L'analisi della completezza del database anti-virus e la possibilità di scaricare solo gli aggiornamenti che sono stati modificati o recentemente aggiunti. Anche questa opzione contribuisce a snellire il traffico di rete;
- L'opzione di lanciare un comando definito dall'utente per ricaricare i database anti-virus immediatamente dopo un aggiornamento eseguito con esito positivo;
- L'opzione di tornare alla versione precedente dei database anti-virus;
- Il programma *wget* non è più richiesto per il funzionamento del nuovo componente;
- Capacità di selezionare il tipo di database anti-virus da scaricare (set standard o esteso).

Database standard– database anti-virus che contiene la descrizione dettagliata di tutti i virus esistenti al momento e i metodi utilizzati per il loro rilevamento e la loro pulizia. Come impostazione predefinita è utilizzato questo tipo di database.

Database esteso – database anti-virus che, oltre alle informazioni sui virus, contiene informazioni RiskWare e AdWare.

I programmi RiskWare contengono vulnerabilità che possono essere sfruttate dagli hacker, per l'installazione non autorizzata di software, ecc.

I programmi AdWare sono installati insieme ad altro software e visualizzano messaggi pubblicitari, aprono pop-up contenenti pubblicità o costringono l'utente a visitare il sito web dell'inserzione pubblicitaria. Oltre a questi messaggi pubblicitari indesiderati, questi programmi sovraccaricano considerevolmente i canali di comunicazione e aumentano il traffico.

Per la modalità di funzionamento regolare, è sufficiente selezionare il database anti-virus standard. Il database esteso garantisce un livello di protezione dei dati maggiore. L'uso di set di database più completi aumenta le risorse utilizzate durante l'operazione di scansione.

5.1.2. Aggiornamento automatico del database anti-virus

È possibile pianificare aggiornamenti automatici a cadenza regolare del database anti-virus modificando il file di configurazione.



Attività: programmazione dell'aggiornamento automatico del database anti-virus ogni 3 ore. Il registro del sistema deve essere aggiornato solo con gli errori dell'applicazione. Un registro generale deve elencare tutte le attività iniziate, senza produzione di informazioni sullo schermo.



Soluzione: per eseguire questa operazione, procedere come segue:

1. Impostare i valori appropriati nel file di configurazione dell'applicazione:

```
[updater.options]
KeepSilent=yes
[updater.report]
Append=yes
ReportLevel=1
```

2. Modificare il file che definisce le regole di funzionamento del processo **cron (crontab -e)**, immettendo la seguente riga:

```
0 0-23/3 * * * /opt/kaspersky/bin/kav4fs-keepup2date
```



Attività: configurazione dell'applicazione in modo che scarichi gli aggiornamenti dei database anti-virus dai server di aggiornamento Kaspersky Lab. L'indirizzo del server di aggiornamento dovrebbe essere selezionato automaticamente dall'elenco fornito con il componente *keepup2date*.



Soluzione: per eseguire l'attività, procedere come segue:

Assegnare il valore **No** al parametro **UseUpdateServerUri** nella sezione **[updater.options]**.



Attività: configurazione dell'applicazione in modo che scarichi gli aggiornamenti dei database anti-virus dall'indirizzo specificato dall'amministratore. Il processo deve essere terminato qualora lo scaricamento dall'indirizzo specificato non riuscisse.



Soluzione: per eseguire l'attività, procedere come segue:

Assegnare il valore **Yes** ai parametri **UseUpdateServerUri** e **UseUpdateServerUriOnly** nella sezione **[updater.options]**. Inoltre, il parametro **UpdateServerUri** deve contenere l'indirizzo del server di aggiornamento.



Attività: configurazione dell'applicazione in modo che scarichi gli aggiornamenti dei database anti-virus dall'indirizzo specificato dall'amministratore. Qualora lo scaricamento dall'indirizzo specificato non riuscisse, i database devono essere aggiornati utilizzando un altro indirizzo dall'elenco dei server interno del componente dell'updater.



Soluzione: per eseguire l'attività, procedere come segue:

Assegnare il valore **Yes** al parametro **UseUpdateServerUrl** nella sezione **[updater.options]** e **No** al parametro **UseUpdateServerUrlOnly**. Inoltre, il parametro **UpdateServerUrl** deve contenere l'indirizzo del sever di aggiornamento.

5.1.3. Aggiornamento a richiesta del database anti-virus

La procedura per l'aggiornamento dei database anti-virus può essere avviata in qualsiasi momento dalla linea di comando.



Attività: avvio della procedura di aggiornamento dei database anti-virus e riepilogo dei risultati nel file `/tmp/updatesreport.log`.



Soluzione: immettere quanto segue nella riga di comando:

```
# kav4fs-keepup2date -l /tmp/updatesreport.log
```

Se si intende aggiornare i database anti-virus su più computer è generalmente più pratico scaricare i database su un computer e salvarli su una directory di rete e quindi aggiornare tutti i computer da quella directory, piuttosto che scaricare i file per ogni singolo computer.



Attività: configurazione dell'aggiornamento dei database anti-virus utilizzando i file nella directory di rete **/home/bases**. Se la directory è inaccessibile o vuota, la procedura di aggiornamento deve utilizzare i server di aggiornamento Kaspersky Lab. I risultati del lavoro vengono raccolti sul file del report **report.txt**.



Soluzione: eseguire l'attività:

1. Impostare i valori appropriati nel file di configurazione dell'applicazione:

```
[updater.options]  
UpdateServerUrl=/home/bases
```

```
UseUpdateServerUrl=yes  
UseUpdateServerUrlOnly=no
```

2. Immettere quanto segue nella riga di comando:

```
# kav4fs-keepup2date -l /tmp/report.txt
```

5.1.4. Creazione di una cartella di rete per memorizzare e scaricare il database anti-virus

Per garantire la corretta esecuzione degli aggiornamenti del database anti-virus dalla cartella di rete, la struttura dei file in tale cartella deve essere identica alla struttura dei server di aggiornamento di Kaspersky Lab. Questa operazione è illustrata di seguito.



Attività: creazione di una cartella di rete da cui gli aggiornamenti del database anti-virus vengono copiati sui computer locali all'interno della rete.



Soluzione: per eseguire l'operazione, procedere come segue:

1. Creare una cartella locale.
2. Avviare il componente *keepup2date* come segue:

```
# kav4fs-keepup2date -u <dir>
```

dove <dir> rappresenta un percorso completo alla cartella creata.

3. Garantire ai computer locali compresi nella rete l'accesso di sola lettura a quella cartella.



Attività: configurazione dell'aggiornamento dei database anti-virus attraverso un server proxy.



Soluzione: per eseguire questa operazione, procedere come segue:

1. Assegnare il valore **Yes** all'impostazione **UseProxy** nella sezione **[updater.options]**.

2. Verificare che l'impostazione **ProxyAddress** nella sezione **[updater.options]** del file di configurazione contenga l'URL del server proxy. L'indirizzo deve essere specificato nel seguente formato: **http://username:password@ip_address:port**. I valori **ip_address** e **port** sono obbligatori, mentre **username** e **password** devono essere specificati solo se il server proxy richiede l'autorizzazione.

oppure:

1. Assegnare il valore **Yes** all'impostazione **UseProxy** nella sezione **[updater.options]**.
2. Specificare la variabile ambientale **http_proxy** utilizzando il seguente formato: **http://username:password@ip_address:port**.

5.2. Protezione anti-virus dei file system

I file system del computer sono protetti dai virus attraverso il componente *kavscanner*, che analizza ed elabora gli oggetti infetti e sospetti in base alle relative impostazioni.



Tutte le impostazioni del componente *kavscanner* sono raggruppate nella sezione **[scanner.*]** del file di configurazione dell'applicazione.



Come impostazione predefinita, solo l'utente **root** può lanciare la scansione su richiesta.

È possibile eseguire la scansione dell'intero file system o di una singola cartella o oggetto. Tutte le impostazioni di protezione possono essere suddivise in gruppi che definiscono:

Area di scansione (vedere sezione 5.2.1 a pagina 33).

- Gli oggetti analizzati e la modalità di disinfezione (vedere sezione 5.2.2 a pagina 34)
- Le azioni da eseguire sugli oggetti (vedere sezione 5.2.2 a pagina 34)
- Le impostazioni utilizzate per la generazione del report sul risultato dell'operazione (vedere sezione 6.5 a pagina 47).

La scansione del file system del computer può essere iniziata:

- Come attività manuale, dalla riga di comando (vedere sezione 5.2.4 a pagina 36).

- Come attività programmata utilizzando l'applicazione **cron** (vedere sezione 5.2.5 a pagina 36).



La scansione anti-virus di un intero computer è un'attività che richiede molte risorse. Si ricorda che durante l'analisi, il livello di prestazione di tutto il computer diminuisce, per cui si raccomanda di non eseguire altri processi contemporaneamente. Per evitare questi problemi, si consiglia invece di analizzare singole cartelle.

5.2.1. Area di analisi

Per praticità, l'area di analisi può essere suddivisa in due parti:

- *Percorso di analisi* indica un elenco di directory e oggetti di destinazione sui quali eseguire l'analisi anti-virus;
- *Oggetti sottoposti ad analisi* indica il tipo di oggetti sottoposti ad analisi per identificare l'eventuale presenza di virus (archivi, ecc.).

Come impostazione predefinita, vengono analizzati tutti gli oggetti accessibili del file system, a partire dalla directory corrente.



L'analisi di tutti i file system del computer necessita come prima cosa dell'immissione della radice o dell'indicazione / come area di analisi nella riga di comando.

Il percorso di analisi può essere ridefinito utilizzando i seguenti metodi:

- Enumerando le cartelle e i file con percorsi assoluti o relativi (rispetto alla cartella corrente), separandoli da spazi sulla riga di comando, all'avvio del componente.
- Specificando i percorsi di analisi in un file di testo, con il comando successivo per utilizzare il file emesso dall'opzione **-@ <file_name>**. Ciascun oggetto nel file viene elencato su una nuova riga con il percorso assoluto corrispondente.



Se la riga di comando contiene sia il percorso di analisi che il file di testo con un elenco di oggetti da analizzare, l'applicazione elabora solo gli oggetti elencati nel file. Il percorso specificato sulla riga di comando verrà ignorato.

- Restringendo i parametri accettati come impostazione predefinita (tutti quelli che iniziano con la cartella corrente), o i percorsi elencati sulla riga di comando; questa operazione può essere effettuata immettendo nel file di configurazione **kav4fs.conf** delle maschere per i file e le cartelle da escludere dall'area di analisi, utilizzando i parametri **ExcludeMask** e **ExcludeDirs** nella sezione **[scanner.options]**.

- Disabilitando l'*analisi ricorrente delle cartelle* (sezione **[scanner.options]**, parametro **Recursion** o tasto **-r**).
- Creando un file di configurazione alternativo, con un comando successivo per utilizzarlo, emesso attraverso l'opzione **-c <file_name>** all'avvio del componente.

Gli oggetti da analizzare come impostazione predefinita sono specificati anche nel file di configurazione **kav4fs.conf** (sezione **[scanner.options]**) e possono essere ridefiniti:

- Direttamente in quel file;
- Attraverso le opzioni della riga di comando quando il componente è avviato;
- Quando si utilizza un file di configurazione alternativo.

5.2.2. Scansione degli oggetti e modalità di disinfezione

Queste impostazioni sono essenziali per l'analisi in quanto determinano se l'applicazione debba tentare di pulire i file infetti.

L'opzione di disinfezione è disabilitata come impostazione predefinita, pertanto, durante l'analisi, l'applicazione invierà solo notifica del l'eventuale presenza di virus, oggetti sospetti o danneggiati, inviando un messaggio alla console e al relativo file report (vedere sezione 6.5 a pagina 47

In seguito alla procedura di analisi, a ciascun oggetto viene assegnato uno dei seguenti valori di stato:

- **Clean** – non è stato rilevato alcun virus (l'oggetto non è infetto)
- **Infected** – l'oggetto è infetto
- **Warning** – il codice dell'oggetto assomiglia a un virus noto
- **Suspicious** – l'oggetto è potenzialmente affetto da un virus sconosciuto
- **Corrupted** – l'oggetto è danneggiato
- **Protected** – l'oggetto non può essere analizzato perché è codificato (protetto da password).

Quando la modalità di disinfezione è abilitata (sezione **[scanner.options]**, parametro **Cure=yes**) solo gli oggetti nello stato **Infected** sono inviati per essere sottoposti all'elaborazione anti-virus. In seguito alla disinfezione, a un file viene assegnato uno dei seguenti valori di stato:

- **Cured** – l'oggetto è stato disinfettato con esito positivo.
- **CureFailed** – la disinfezione dell'oggetto non è riuscita. Questi file saranno trattati in base alle regole definite per gli oggetti infetti.
- **Error** – si è verificato un errore durante la scansione di un oggetto.

5.2.3. Possibili azioni sugli oggetti

È possibile applicare determinate azioni agli oggetti in funzione del loro stato (vedere Capitolo 2 a pagina 14). Tuttavia, possono essere definite alcune azioni specificamente per i file con stato **Infected** (infecto), **Suspicious** (sospetto), **Warning** (avvertenza) o **Corrupted** (danneggiato), **Error**, **Protected** come:

- *Trasferimento a una directory specificata* – riposizionamento dei file con un dato stato in una *directory specificata*; è possibile il trasferimento regolare o ricorrente;
- *Rimozione del file dal file system*;
- *Esecuzione di un determinato comando* – elaborazione dei file utilizzando i comandi, gli script, ecc. Unix standard.

Si noti che Kaspersky Anti-Virus distingue tra un oggetto semplice (file) e un oggetto composito (costituito da più oggetti, per esempio un archivio). Anche le azioni da eseguire su questi due tipi di oggetti sono diverse, e sono localizzate in sezioni separate del file di configurazione. La sezione **[scanner.object]** è dedicata agli oggetti semplici, mentre la sezione **[scanner.container]** agli oggetti composti.



Per gli archivi autodecompressibili sono possibili varie operazioni: se è l'archivio stesso ad essere infetto, viene trattato come un oggetto semplice, se invece sono gli oggetti archiviati all'interno dello stesso a contenere virus, viene trattato come un oggetto composito. Queste due operazioni separate sull'archivio sono determinate da parametri impostati in sezioni diverse del file di configurazione!

Per selezionare un'azione da compiere su un determinato file, possono essere utilizzati i seguenti metodi:

- Specificare le azioni nel file di configurazione **kav4fs.conf** se devono essere utilizzate come azioni predefinite (sezioni **[scanner.object]** e **[scanner.container]**).
- Indicare le azioni nel file di configurazione alternativo e utilizzarlo all'avvio del componente.



Se nella riga di comando non è indicato alcun file di configurazione, i parametri funzionali sono presi dal file predefinito **kav4fs.conf**. L'uso di questo file all'avvio non deve essere necessariamente specificato!

- Definire le azioni per la sessione corrente utilizzando le opzioni della riga di comando all'avvio del componente *kavscanner*.

Le azioni di definizione della sintassi sono simili sia per gli oggetti semplici che per quelli composti (sezioni **[scanner.object]** e **[scanner.container]**).

5.2.4. Scansione a richiesta di una singola cartella

Una delle attività più frequentemente usate in Kaspersky Anti-Virus è la scansione anti-virus e la pulizia di una singola cartella.



Attività: avviare l'analisi della directory **/tmp** disinfettando automaticamente tutti gli oggetti infetti. Gli oggetti che non possono essere disinfettati devono essere eliminati.

Creare i file *infected.lst*, *suspicion.lst*, *corrupted.lst* e *warning.lst* nella stessa directory, registrando rispettivamente i nomi degli oggetti infetti, sospetti o danneggiati rilevati dalla procedura di analisi.

Memorizzare i risultati dell'attività del componente (data di avvio, informazioni dettagliate su tutti i file tranne quelli non contenenti virus) in un file rapporto *kavscanner-<<current_date>>-pid.log* nella stessa directory.



Soluzione: per eseguire l'attività, immettere quanto segue nella riga di comando:

```
#kavscanner -rlq -pi/tmp/infected.lst
-ps/tmp/suspicion.lst -pc/tmp/corrupted.lst
-pw/tmp/warning.lst -o /tmp/kavscanner-`date
"+%Y-%m-%d-%s"`.log -i3 -ePASBMe -j3 -mCn /tmp
```

5.2.5. Scansione programmata

L'avvio della scansione programmata, incluse le attività di Kaspersky Anti-Virus, avviene attraverso l'applicazione **cron**.



Attività: programmazione dell'analisi giornaliera per rilevare la presenza di eventuali virus, in modo che inizi alle ore 0:00 per la directory **/home**, utilizzando i parametri di analisi definiti nel file di configurazione `/etc/kav/scanhome.conf`.



Soluzione: per eseguire l'attività, procedere come segue:

1. Creare il file di configurazione `/etc/kav/scanhome.conf` e registrare tutti i parametri di analisi richiesti nello stesso.
2. Modificare il file che definisce le attività per **cron**, immettendo **crontab -e** nella riga di comando, e aggiungere la seguente riga:

```
0 0 * * * /path/to/kav4fs-kavscanner -c
/etc/kav/scanhome.conf /home
```

5.2.6. Funzionalità ulteriori: uso dei file script

Kaspersky Anti-Virus consente l'ulteriore elaborazione degli oggetti che sono già stati sottoposti ad analisi anti-virus utilizzando i comandi e gli script Unix standard. Questi strumenti consentono agli amministratori esperti di estendere la funzionalità di Kaspersky Anti-Virus definendo varie azioni da eseguire su oggetti dallo stato diverso.

5.2.6.1. Disinfezione di oggetti infetti all'interno di un archivio

Kaspersky Anti-Virus non esegue la disinfezione di file infetti compressi; si limita a rilevare gli oggetti sospetti e infetti all'interno degli archivi. Tuttavia, questa capacità può essere implementata utilizzando uno script supplementare come lo script `vox.sh`, utilizzato per disinfettare gli archivi `tar` e `zip`, incluso nel pacchetto retail di Kaspersky Anti-Virus.

Quando viene lanciato, lo script decompime l'archivio correntemente sottoposto a scansione, esegue la scansione antivirus e l'elaborazione dei singoli oggetti, e successivamente comprime i file analizzati. Pertanto devono essere installate nel sistema le necessarie utility di compressione file.



Attività: analisi di tutti gli archivi `tar` e `zip` utilizzando lo script `vox.sh` .



Soluzione: per eseguire l'attività, procedere come segue:

Immettere nella riga di comando:

```
# /opt/kaspersky/kav4fs/share/contrib/vox.sh <archive-
path>
```

5.2.6.2. Invio di notifiche all'amministratore

Kaspersky Anti-Virus consente di configurare gli strumenti standard Unix in modo che notifichino l'amministratore relativamente agli oggetti infetti, sospetti o danneggiati rilevati all'interno dei file system del computer.



Attività: configurazione della notifica all'amministratore su file e archivi infetti scoperti nel file system del computer durante ogni analisi eseguita in base ai parametri definiti nel file di configurazione **kav4fs.conf**. Abilitare la modalità di apertura symlinks.



Soluzione: per eseguire l'attività, procedere come segue:

Definire le regole per l'elaborazione di oggetti semplici e oggetti contenitori nel file di configurazione **kav4fs.conf**:

```
[scanner.options]
FollowSymlinks=yes
[scanner.object]
OnInfected=exec echo %FULLPATH%/%FILENAME% is
infected by %VIRUSNAME% |
mail -s kav4fs-kavscanner admin@localhost.ru
[scanner.container]
OnInfected=exec echo archive %FULLPATH%/%FILENAME% is
infected, viruses list is in the attached file %LIST%
| mail -s kav4fs-kavscanner -a %LIST% admin@localhost.ru
```



Prima di lanciare l'esempio l'utente deve assicurarsi che la utility **di posta elettronica** si trovi nella posizione indicata dal percorso di installazione standard di questa utility nel sistema operativo.

5.3. Protezione anti-virus in tempo reale

La protezione anti-virus in tempo reale del file system del computer è eseguita dal componente *kavmonitor*.



Tutte le impostazioni del componente *kavmonitor* sono contenute nella sezione **[monitor.*]** del file di configurazione dell'applicazione.

Il componente *kavmonitor* è configurato in modo tale che quando si esegue un'azione che richiede l'accesso a un file (apertura, chiusura o esecuzione), il componente *kavmonitor* esegue una scansione anti-virus (quando è chiuso, il file viene analizzato solo se è stato modificato). Come impostazione predefinita, tutti gli oggetti richiesti dall'utente saranno sottoposti all'analisi anti-virus e alla ricerca di software nocivo, inclusi:

- File compressi;
- Archivi;
- Archivi ad estrazione automatica;
- Database di posta elettronica;
- Messaggi di posta elettronica.

Sulla base dei risultati della scansione anti-virus, gli oggetti verranno elaborati utilizzando le impostazioni specificate nel file di configurazione dell'applicazione.



Come impostazione predefinita, la disinfezione degli oggetti infetti è disabilitata! Per configurare questa opzione, assegnare il valore **Yes** all'impostazione **Cure** nella sezione **[monitor.options]** del file di configurazione dell'applicazione.

Per gli oggetti con stato **Infected**, **Suspicious**, **Warning**, **Error**, **Protected** e **CureFailed**, possono essere configurate alcune azioni, tra le quali:

- *Trasferimento in una cartella* – spostamento degli oggetti con un determinato stato in una cartella; è possibile il trasferimento *semplice* e *ricorrente* (con il ripristino dell'intero percorso).
- *Eliminazione dell'oggetto* dal file system;

Le regole per l'elaborazione degli oggetti possono essere definite nel file di configurazione dell'applicazione (sezione **[monitor.actions]**).

È inoltre possibile configurare parametri supplementari:

- I parametri **ExcludeDirs** e **ExcludeMask** definiscono le cartelle che devono essere escluse dalla scansione.
- Utilizzare l'analizzatore euristico di codici e le tecnologie iChecker.

Appendice C. Ridurre il carico del server definendo il numero massimo di oggetti che possono essere analizzati contemporaneamente.

5.4. Gestione delle chiavi di licenza

Una chiave di licenza dà il diritto di utilizzare l'applicazione e contiene inoltre dati relativi alla licenza acquistata, come il tipo di licenza, la data di scadenza, informazioni sui distributori, ecc.

Inoltre, durante il periodo di validità della licenza, l'utente ha diritto di usufruire dei seguenti servizi:

- Supporto tecnico 24 ore su 24, 7 giorni alla settimana;
- Aggiornamenti dei database anti-virus a cadenza oraria;
- Aggiornamenti dell'applicazione (patch);
- Nuove versioni dell'applicazione (upgrade);
- Notifiche tempestive su nuovi virus.

Quando la licenza scade, questi servizi vengono sospesi automaticamente. Kaspersky Anti-Virus continuerà ad analizzare i file ma utilizzerà unicamente database anti-virus che risalgono al periodo di validità della licenza, in quanto la funzione di aggiornamento dei database anti-virus risulterà disabilitata.

È pertanto fondamentale controllare periodicamente i file del report contenenti le informazioni sulla chiave di licenza e controllarne la data di scadenza.

5.4.1. Visualizzazione dei dettagli delle chiavi di licenza

Le informazioni sulle chiavi di licenza installate possono essere controllate nei registri prodotti dai componenti *kavscanner*, *kavmonitor* e *keepup2date*, poiché ciascuno di loro carica le informazioni dalle chiavi di licenza quando vengono lanciati.

Inoltre, Kaspersky Anti-Virus contiene uno speciale componente *licensemanager* che consente di visualizzare informazioni più dettagliate sulle chiavi oltre ad alcuni dati analitici.

Tutte le informazioni possono essere visualizzate sullo schermo del terminale.



Per controllare le informazioni sulle chiavi di licenza installate,

Immettere la seguente riga di comando:

```
kav4fs-licensemanager -s
```

Informazioni sulle licenze installate, simili alle seguenti, saranno visualizzate sul terminale:

```
Kaspersky license manager Version 5.5
Copyright (C) Kaspersky Lab. 1997-2006.
License file 0003D3EA.key, serial 0038-000419-
0003D3EA, "Kaspersky Anti-Virus for Unix", expires 04-
07-2003 in 28 days
License file 0003E3E8.key, serial 011E-000413-
0003E3E8, "Kaspersky Anti-Virus for Linux File Srv
(licence per e-mail address)", expires 25-01-2004 in
234 days
```



Per controllare le informazioni su una specifica chiave di licenza,

Immettere la seguente riga di comando:

```
kav4fs-licensemanager -k 0003D3EA.key
```

La console visualizzerà informazioni simili alle seguenti:

```
Kaspersky license manager Version 5.5
Copyright (C) Kaspersky Lab. 1997-2006.
Portions Copyright (C) Lan Crypto
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus for
Linux", expires 04-07-2003 in 28 days
```

5.4.2. Rinnovo della licenza

Il rinnovo della licenza per utilizzare Kaspersky Anti-Virus prolunga o ripristina la funzionalità di tutta l'applicazione, l'aggiornamento dei database anti-virus e il prolungamento dei servizi supplementari elencati nella sezione 5.4 on page 40 .

Il periodo di validità della licenza dipende dal tipo di licenza selezionata durante la procedura di acquisto dell'applicazione.



Per estendere la licenza di utilizzo di Kaspersky Anti-Virus occorre:

Contattare il distributore presso il quale è stata acquistata l'applicazione e rinnovare la licenza d'uso di Kaspersky Anti-Virus.

oppure:

estendere la durata della licenza direttamente attraverso Kaspersky Lab inviando una e-mail all'ufficio acquisti (sales@kaspersky.com), oppure compilando il modulo corrispondente nella sezione **E-Store** → **Renew Your License** del nostro sito (www.kaspersky.com). Dopo pagamento, l'utente riceverà una chiave di licenza che sarà inviata all'indirizzo e-mail indicato nel modulo d'ordine.



Periodicamente, Kaspersky Lab Ltd. Lancia campagne promozionali che prevedono notevoli sconti per il rinnovo della licenza sui nostri prodotti. Per essere sempre informati sulle nostre offerte, visitate il sito Kaspersky Lab e andate alla sezione **Products** → **Sales and special offers**.

La chiave di licenza acquistata deve essere installata.



Per installare la nuova chiave di licenza,

Immettere la riga di comando:

```
kav4fs-licensemanager -a <key filename>
```

Successivamente, si raccomanda di aggiornare il proprio database anti-virus (vedere sezione **5.1** a pagina 26).



Per rimuovere una chiave di licenza,

Immettere la riga di comando:

```
kav4fs-licensemanager -d <key filename>
```

CAPITOLO 6. PARAMETRI SUPPLEMENTARI

Il presente capitolo contiene informazioni sulle impostazioni supplementari di Kaspersky Anti-Virus. Queste configurazioni supplementari consentono di estendere le funzionalità dell'applicazione e personalizzarle in base alle particolari esigenze aziendali.

6.1. Ottimizzazione del funzionamento di Kaspersky Anti-Virus

Kaspersky Anti-Virus offre vari metodi per diminuire il carico del processore e velocizzare l'elaborazione anti-virus sugli oggetti sottoposti ad analisi. Di seguito è illustrata una panoramica dettagliata di queste funzioni.



Utilizzo del database iChecker™ e di cache di secondo livello dei file analizzati.

L'applicazione utilizza vari e tecnologie che rendono superfluo analizzare un file ogni qualvolta vi si accede e, se possibile, consentono di limitare il lavoro al semplice confronto delle informazioni esistenti contenute nello stesso. L'algoritmo di scansione anti-virus degli oggetti (file) include quanto segue:

Dopo l'analisi iniziale di qualsiasi file, le informazioni ad esso relative (nome, checksum) vengono incluse in uno dei seguenti database:

- Il database iChecker™ include informazioni sui file analizzati **non-infected** in formati identificati, fornite da entrambi i componenti *kavmonitor* e *kavscanner*.
- La cache dei file analizzati è un database contenente informazioni su tutti i file controllati dal componente *kavmonitor*. La cache presenta due livelli: il primo livello contiene informazioni sui file **puliti** ad accesso più frequente ed è posizionata nel modulo kernel, che riduce considerevolmente il tempo necessario ad accedervi. Se l'applicazione rileva dati su un determinato file nella cache di primo livello, assegna lo stato **Clean** a quel file e non esegue ulteriori controlli anti-virus. Se la cache di primo livello non contiene le informazioni richieste, l'applicazione

esegue una ricerca nella cache di secondo livello contenente dati su **tutti i file controllati**. Entrambi i database delle cache vengono memorizzati nella RAM e non vengono salvati allo spegnimento dell'applicazione.

Pertanto, se durante una procedura di analisi, le informazioni su un file non vengono aggiunte al database iChecker™ perché il file non è chiaro o ha un formato non supportato, viene inviato alla cache dell'applicazione.

Tutti i successivi accessi da parte dell'utente a un file determinano una ricerca del nome del file nella cache di primo livello; successivamente, se l'oggetto non è stato trovato in tale livello, viene cercato nel database di iChecker™ e nella cache di secondo livello. Se il nome del file non viene trovato in nessun database, la sua condizione corrente verrà confrontata con i dati memorizzati nel database. Il file viene considerato invariato e pertanto non viene sottoposto nuovamente ad analisi se la sua condizione corrente è esattamente identica ai dati memorizzati.

Se per il file in oggetto non vengono trovati dati né nel database iChecker né nella cache, il file viene sottoposto ad analisi anti-virus completa.



Se durante l'uso di Kaspersky Anti-Virus il set di database anti-virus è stato cambiato, occorre eliminare manualmente le informazioni dal database iChecker (il percorso completo al database è definito nel parametro **IcheckerDbFile**, sezione **[path]** del file di configurazione dell'applicazione).

Questo accorgimento è necessario in quanto il database potrebbe contenere oggetti infetti non rilevati durante l'uso del database anti-virus standard, ma rilevati dal set esteso. I file le cui informazioni sono contenute nel database iChecker non saranno sottoposti a nuova scansione e questo potrebbe determinare l'infezione del computer.



Limitazione del carico della CPU.

L'analisi dei file system di un computer può richiedere molto tempo in presenza di un volume considerevole di dati; in questo caso, il carico della CPU potrebbe aumentare significativamente. Poiché il processore deve essere in grado di eseguire le normali attività, è consigliabile sospendere l'analisi anti-virus in caso di superamento di un certo carico limite.

Kaspersky Anti-Virus versione 5.5 presenta un meccanismo di questo tipo. Il parametro **MaxLoadAvg** è stato aggiunto alla sezione **[scanner.options]** del file di configurazione. Se questa opzione è abilitata, *kavscanner* controlla il carico corrente della CPU (**carico medio**) prima di analizzare qualsiasi nuovo file. Se il valore supera la cifra specificata nel file di configurazione, il funzionamento del tool di analisi viene sospeso fino a quando il valore del **carico medio** non diminuisce entro la soglia specificata.

Inoltre, è possibile restringere il numero di oggetti analizzati contemporaneamente in modalità in tempo reale utilizzando l'impostazione **CheckFileLimit** della sezione **[monitor.options]** del file di configurazione dell'applicazione. Questo consente di diminuire il carico del processore e aumenta la velocità di scansione di alcuni oggetti.

6.2. Trasferimento degli oggetti nella cartella Quarantine

È possibile configurare Kaspersky Anti-Virus in modo che sposti tutti gli oggetti infetti rilevati nel file system del computer in una cartella separata.

Tale approccio può essere utilizzato per esempio se durante l'analisi anti-virus non è stato possibile disinfettare un oggetto (per esempio, sono stati rimossi solo due virus su tre che hanno intaccato il file), ma il file stesso contiene informazioni importanti.

Se si intende mantenere la cartella contenente gli oggetti da isolare all'interno del file system del computer, si consiglia di escluderla dall'area di destinazione di tutte le successive analisi, specificandone il percorso nel parametro **ExcludeDir** della sezione **[scanner.options]** nel file di configurazione.

Di seguito è illustrata una panoramica delle operazioni di isolamento degli oggetti infetti durante il processo di scansione a richiesta del file system del computer e la scansione in tempo reale.



Attività: analisi di tutti gli oggetti elencati nel file `/tmp/download.lst` e spostamento degli oggetti infetti nella cartella `/tmp/infected`. Registrazione delle informazioni relative a oggetti infetti, sospetti e danneggiati nel file report.



Soluzione: per eseguire l'attività, procedere come segue:

1. Per specificare le azioni da eseguire sugli oggetti infetti, aggiungere la seguente riga alle sezioni **[scanner.object]** e **[scanner.container]** del file di configurazione:

```
OnInfected=MovePath /tmp/infected
```

2. Se abilitata, disabilitare la modalità di disinfezione (**Cure=no**).
3. Immettere la seguente riga di comando:

```
# kavscanner -@/tmp/download.lst -ePASBME -rq  
-i0 -o /tmp/report.log -j3 -mCn
```

Ora l'operazione si complica imponendo la restrizione dell'accesso ai file nella directory `/tmp/infected` a sola lettura e scrittura; utilizzare gli strumenti standard Unix (il comando **chmod**) apportando le seguenti modifiche alla struttura dell'attività:

Aggiungere la riga sotto riportata come regola per l'elaborazione dei file infetti nelle sezioni **[scanner.object]** e **[scanner.container]** del file di configurazione dell'applicazione:

```
OnInfected=exec mv %FULLPATH%/%FILENAME%
/tmp/infected/%FILENAME%; chmod -x
/tmp/infected/%FILENAME%
```



Operazione: scansione anti-virus di tutti i file a cui è stato tentato l'accesso, disinfezione di tutti gli oggetti infetti. Se la pulizia non riesce, trasferimento degli oggetti infetti con percorsi completi agli stessi nella cartella `/tmp/infected`.



Soluzione: per eseguire questa operazione, procedere come segue:

1. Abilitare la modalità di disinfezione per gli oggetti infetti (**Cure = yes** nella sezione **[monitor.options]** del file di configurazione).
2. Specificare le regole per l'isolamento degli oggetti infetti. A tal fine, configurare le impostazioni nella sezione **[monitor.actions]** del file di configurazione come segue:

```
OnInfected=MovePath /tmp/infected
```

6.3. Modalità di creazione di una copia di backup degli oggetti

Se i file infetti vengono eliminati automaticamente, come specificato nell'azione da compiere sui file infetti, è possibile che dati importanti vadano persi. I dati sono a rischio anche durante la disinfezione. Per non correre questo pericolo, Kaspersky Anti-Virus offre la possibilità di copiare i file infetti in una directory di memorizzazione di backup.

Prima della disinfezione o rimozione di un oggetto, l'applicazione può essere configurata in modo da copiare automaticamente tale oggetto nella directory di memorizzazione di backup, specificata dal parametro **BackupPath** nella sezione **[monitor.path]**. Questo consente di creare una copia di backup (ed eventualmente di ripristinare il file originale), se l'oggetto viene danneggiato durante la disinfezione. Se uno stesso oggetto viene memorizzato due volte nella cartella di backup, la copia precedente verrà sostituita automaticamente con quella più recente.

Si noti che come impostazione predefinita, la modalità backup è disabilitata e il percorso alla directory di memorizzazione di backup non è definito.

Al fine di abilitare la modalità backup, occorre specificare il percorso alla cartella nella quale le copie di backup degli oggetti saranno conservate.



Se un oggetto viene rimosso dal file system, la sua copia di backup viene conservata fino a quando non viene eliminata dall'amministratore.



Le azioni specificate per gli oggetti infetti nel file di configurazione non saranno eseguite sui file memorizzati nella cartella di backup!

6.4. Formato di data e ora

Durante il funzionamento, Kaspersky Anti-Virus compila i report per ciascuno dei suoi componenti oltre alle notifiche per utenti e amministratori, che sono sempre corredati di data e ora.

Come impostazione predefinita, Kaspersky Anti-Virus utilizza formati di data e ora conformi a quelli utilizzati dalla funzione strftime:

%H:%M:%S – formato dell'ora visualizzato.

%d/%m/%y – formato della data visualizzato.

L'amministratore può modificare il formato di data e ora attraverso i parametri nella sezione **[locale]** del file di configurazione. Tra gli esempi di possibili formati rientrano:

%I:%M:%S %P – per la visualizzazione dell'ora nel formato a dodici ore (parametro **TimeFormat**) con indicazione am/pm.

%y/%m/%d e **%m/%d/%y** – per la visualizzazione della data (parametro **DateFormat**) nei formati anno/mese/data o mese/data/anno rispettivamente.

6.5. Impostazioni per la generazione dei report di Kaspersky Anti-Virus

I risultati delle operazioni eseguite da tutti i componenti di Kaspersky Anti-Virus sono riassunti in un report sotto forma di file.



I risultati di un'elaborazione anti-virus dei file system del computer sono visualizzati anche sulla console. Come impostazione predefinita, le informazioni incluse nel report e quelle visualizzate sulla console sono identiche. Affinché le informazioni visualizzate sulla console siano diverse da quelle incluse nel file di registro, sono necessarie configurazioni supplementari. Se si desidera che l'applicazione registri la propria attività nel registro di sistema, impostare il parametro **ReportFileName** nelle sezioni **[monitor.report]**, **[scanner.report]**, e **[updater.report]** su **syslog**.

La quantità di informazioni prodotte può essere modificata cambiando il *livello di dettaglio del report*.

Il **livello di dettaglio** è un numero che stabilisce il livello di prolissità delle informazioni relative al lavoro del componente da includere nel report. Ciascun livello successivo include informazioni sul livello precedente, oltre ad alcuni altri dati supplementari.

La tabella sotto riportata illustra i possibili livelli di dettaglio del report.

Livelli	Nome del livello	Significato
	Critical errors	Solo informazioni relative a errori critici che determinano l'interruzione del programma a causa dell'impossibilità di eseguire un'azione. Per esempio: il componente dell'applicazione è infetto, o si è verificato un errore durante la verifica o il caricamento dei database o delle chiavi di licenza.
1	Errors	Informazioni su altri errori, inclusi quelli che non causano l'interruzione di un componente, per esempio informazioni relative a un errore nell'analisi di un file.
2	Warning	Informazioni su errori che possono causare la chiusura dell'applicazione (per esempio informazioni su spazio insufficiente su disco).
3	Info, Notice	Importanti messaggi informativi, per esempio sul fatto che il componente sia in funzione o meno, sul percorso al file di configurazione, sull'area di analisi, informazioni relative a database anti-virus, chiavi di licenza, e statistiche sui risultati.

Livelli	Nome del livello	Significato
4	Activity	Messaggi relativi all'analisi degli oggetti, in base al livello di dettaglio della scansione.

Le informazioni relative agli errori fatali nel funzionamento del componente vengono prodotte indipendentemente dal livello di dettaglio selezionato. Il livello di dettaglio ottimale è 4, che è quello predefinito.

CAPITOLO 7. DISINSTALLAZIONE E DI KASPERSKY ANTI- VIRUS

La procedura di disinstallazione di Kaspersky Anti-Virus richiede quanto segue:

- Privilegi di superuser (**root**). Se non si dispone di questi privilegi, quando si avvia la procedura di disinstallazione occorre registrarsi nel sistema come utente **root**.
- Installazione del file di registro.
- I nomi e le dimensioni dei file installati come parti di Kaspersky Anti-Virus devono essere esattamente gli stessi di quelli specificati nel file di registro di installazione.
- Prima di avviare il processo di installazione dell'applicazione, occorre arrestare il componente **kavmonitor**.



Se Kaspersky Anti-Virus è stato installato utilizzando il pacchetto .rpm immettere quanto segue nella riga di comando per avviare la procedura di disinstallazione:

```
rpm -e <package_name>
```



Se Kaspersky Anti-Virus è stato installato utilizzando il pacchetto .deb immettere quanto segue nella riga di comando per avviare la procedura di disinstallazione:

```
dpkg -r <package_name>
```




Se Kaspersky Anti-Virus è stato installato utilizzando il pacchetto .pkg immettere quanto segue nella riga di comando per avviare la procedura di disinstallazione::

```
pkg-delete <package_name>
```

Il programma verrà disinstallato automaticamente. Al termine della procedura, un messaggio di notifica verrà visualizzato sulla console.

CAPITOLO 8. VERIFICA DEL FUNZIONAMENTO DI KASPERSKY ANTI-VIRUS

Dopo la procedura di installazione e configurazione di Kaspersky Anti-Virus, si consiglia di testare la correttezza delle impostazioni e del funzionamento dell'applicazione utilizzando una serie di "virus" di prova.

Il virus di prova è stato specificamente progettato dall'organizzazione European Institute for Computer Antivirus Research,  per testare i prodotti anti-virus.

Il "virus" di prova NON È EFFETTIVAMENTE UN VIRUS in quanto non contiene codici che possono realmente danneggiare il computer; tuttavia, la maggior parte dei prodotti anti-virus identificano questo file come un virus.



Non utilizzare mai virus veri per testare il funzionamento di un prodotto anti-virus!

Il "virus" di prova può essere scaricato dal sito web ufficiale dell'organizzazione **EICAR** all'indirizzo: http://www.eicar.org/anti_virus_test_file.htm.

Il file scaricato dal sito web di **EICAR**, o creato come sopra descritto, contiene il corpo di un "virus" di prova standard. L'applicazione lo rileverà, gli assegnerà lo stato **Infected** e applicherà l'azione definita dall'amministratore per la gestione degli oggetti contrassegnati da questo stato.

Per testare la risposta dell'applicazione ad altri tipi di oggetti, modificare il corpo di questo "virus" di prova standard aggiungendo uno dei prefissi (vedere tabella sotto riportata).

Tabella. Modifiche del "virus" di prova

Prefisso	Tipo di oggetto
Nessun prefisso, "virus" di prova standard	Infected . L'oggetto non può essere disinfettato.
CORR-	Corrupted danneggiato

Prefisso	Tipo di oggetto
SUSP-	Suspicious (codice virale sconosciuto).
WARN-	Suspicious (codice modificato di un virus noto).
ERRO-	Not analyzed non analizzato a causa di un errore.
CURE-	Disinfected. L'oggetto è disinfettato; il testo del corpo del "virus" è stato modificato per pulirlo.
DELE-	L'oggetto viene eliminato automaticamente.

La prima colonna della tabella elenca i prefissi da aggiungere all'inizio della stringa del "virus". La seconda colonna della tabella contiene lo stato assegnato dall'applicazione dopo l'aggiunta del prefisso. Le azioni per ogni stato dell'oggetto sono definite dalle impostazioni dell'applicazione anti-virus personalizzate dall'amministratore.

APPENDICE A.

INFORMAZIONI SUPPLEMENTARI SULL'APPLICAZIONE

La presente Appendice contiene la descrizione della struttura ad albero delle cartelle di Kaspersky Anti-Virus dopo l'installazione, del file di configurazione e dei tasti di modifica della linea di comando dei componenti e i relativi codici visualizzati; il file script per la pulizia degli archivi è fornito a titolo esemplificativo.

A.1. File di configurazione di Kaspersky Anti-Virus

Il pacchetto Kaspersky Anti-Virus comprende il file di configurazione **kav4fs.conf** contenente i parametri per il funzionamento dell'applicazione. Nella descrizione delle impostazioni dei file sono indicati i valori predefiniti, a condizione che siano forniti.

La sezione **[path]** include le impostazioni che definiscono i percorsi ai file più importanti, senza i quali l'applicazione non funziona..

BasesPath– percorso completo al database anti-virus.

LicensePath– percorso completo alla cartella contenente le chiavi di licenza.

IcheckerDbFile– percorso completo alla cartella che memorizza il database controllato utilizzando le tecnologie iChecker.

La sezione **[locale]** contiene le impostazioni che determinano i formati di data e ora:

TimeFormat=%H:%M:%S – formato di visualizzazione dell'ora conformemente allo standard strftime.



Il formato di visualizzazione dell'ora può essere modificato nel formato a dodici ore (am, pm): **%I:%M:%S %P**

DateFormat=%d/%m/%y – formato di visualizzazione della data conformemente allo standard strftime.



Il formato di visualizzazione della data può essere modificato per esempio nel formato seguente: `%Y/%m/%d` or `%m/%d/%y`.

La sezione **[monitor.options]** contiene i parametri della scansione anti-virus in tempo reale:

ExcludeDirs=mask1:mask2:...:maskN – maschere delle cartelle che saranno escluse dalla scansione; come impostazione predefinita, tutte le cartelle vengono analizzate.

ExcludeMask=mask1:mask2:...:maskN – maschere dei file che saranno esclusi dalla scansione; come impostazione predefinita, tutti i file vengono analizzati.

IncludeDirs=mask1:mask2:...:maskN –maschere delle cartelle che saranno analizzate.

Packed=yes – modalità di scansione dei file compressi. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

Archives=yes – modalità di scansione degli archivi. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

SelfExtArchives=yes – modalità di scansione degli archivi a decompressione automatica. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione. Se la modalità di scansione archivi è abilitata (**Archives=yes**), gli archivi a decompressione automatica saranno analizzati anche se all'impostazione **SelfExtArchives** non è stato assegnato alcun valore.

MailBases=yes – modalità di scansione del database di posta elettronica. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

MailPlain=yes –scansione dei messaggi di testo in formato testo normale. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

Heuristic=yes – modalità per l'utilizzo dell'analizzatore di codici euristico durante la scansione. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

Cure=no – modalità per la disinfezione degli oggetti infetti. Per abilitare questa modalità, assegnare il valore **yes** a questa impostazione.

Ichecker=yes – modalità per l'uso della tecnologia iChecker durante la scansione anti-virus. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

FileCacheSize– dimensioni del file cache (in MB).

KernelCacheSize – dimensioni della cache memorizzata dal kernel anti-virus (in MB).

CheckFileLimit=20 – numero massimo di oggetti che possono essere analizzati allo stesso tempo.

HashType=md5 – tipo di hash utilizzato.

UseAVbasesSet=standard|extended – set di database anti-virus utilizzato dall'applicazione. Il set **esteso** contiene, oltre ai record presenti nel set **standard**, anche i codici identificativi del riskware, come: adware, programmi di amministrazione remota, ecc.

La sezione **[monitor.path]** include impostazioni che definiscono i percorsi ai file più importanti, senza i quali il modulo kavmonitor non funziona.

BackupPath= path – percorso completo alla cartella che memorizza le copie di backup degli oggetti analizzati.

PidFile=path – percorso completo al file pid file del componente kavmonitor.

La sezione **[monitor.actions]** contiene impostazioni che definiscono le azioni da compiere con oggetti di un determinato tipo durante la protezione anti-virus in tempo reale.

OnInfected=action – azioni da compiere in caso di rilevamento di un file infetto. Se la modalità di disinfezione dei file infetti è attivata, l'azione specificata sarà eseguita sugli oggetti che non è stato possibile pulire.

OnSuspicion=action – azioni da compiere in caso di rilevamento di un codice di file sospetto che assomiglia al codice di un virus sconosciuto a Kaspersky Lab.

OnWarning=action – azioni da compiere in caso di rilevamento di un file il cui codice assomiglia al codice di un virus noto.

OnCured=action – azioni da compiere in caso di rilevamento e disinfezione riuscita di un oggetto infetto.

OnProtected=action – azioni da compiere in caso di rilevamento di un oggetto protetto da password. Questi oggetti non possono essere analizzati.

OnCorrupted=action – azioni da compiere in caso di rilevamento di un file danneggiato.

OnError=actions – azioni da compiere qualora si verifichi un errore di sistema durante la scansione dell'oggetto.

La sezione **[monitor.report]** contiene le impostazioni per la generazione dei report sui risultati di funzionamento del componente kavmonitor.

ReportLevel=4 – livello di dettaglio del report.

ReportFileName – nome del file nel quale saranno registrati i risultati del funzionamento del componente.

Append=yes – modalità per aggiungere nuovi messaggi al file del report. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

ShowOK=yes – modalità per registrare i messaggi sui file puliti nel report. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

La sezione [**scanner.options**] contiene le impostazioni per scansione i file system del server.

Archives=yes – modalità di scansione degli archivi. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

Cure=no – modalità per la disinfezione degli oggetti infetti. Per abilitare questa modalità, assegnare il valore **yes** a questa impostazione.

ExcludeDirs=mask1:mask2:...:maskN – maschere delle cartelle escluse dalla scansione; come impostazione predefinita, tutte le cartelle sono sottoposte ad analisi.

ExcludeMask=mask1:mask2:...:maskN – maschere dei file che saranno esclusi dalla scansione; come impostazione predefinita, tutti i file sono sottoposti ad analisi.

Heuristic=yes – modalità per l'utilizzo dell'analizzatore di codici euristico durante la scansione. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

LocalFS=no – modalità per analizzare unicamente il file system locale. Per abilitare questa modalità, assegnare il valore **yes** a questa impostazione.

MailBases=yes – modalità di scansione del database di posta elettronica. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

MailPlain=yes – scansione dei messaggi di testo in formato testo normale. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

Packed=yes – modalità di scansione dei file compressi. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

Recursion=yes – modalità per l'analisi ricorrente delle cartelle durante la scansione anti-virus. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

SelfExtArchives=yes – modalità di scansione degli archivi a decompressione automatica. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione. Se la modalità di scansione archivi è abilitata (**Archives=yes**), gli archivi a decompressione automatica saranno analizzati anche se al parametro **SelfExtArchives** non è stato assegnato alcun valore.

lchecker=yes – modalità per l'uso della tecnologia iChecker durante la scansione anti-virus. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

UseAVbasesSet=standard|extended – set di database anti-virus utilizzato dall'applicazione. Il set **esteso** contiene, oltre ai record presenti nel set **standard**, anche i codici identificativi del riskware, come: adware, programmi di amministrazione remota, ecc.

FollowSymlinks – questa opzione controlla la gestione dei link simbolici. Se il parametro è impostato su **yes**, l'applicazione seguirà i link che portano alle directory durante la scansione.

MaxLoadAvg – carico massimo del processore.

La sezione **[scanner.report]** contiene le impostazioni per la generazione dei report sui risultati di funzionamento del componente kavscanner.

Append=yes – modalità per aggiungere nuovi messaggi al file del report. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

ReportFileName – nome del file nel quale saranno registrati i risultati del funzionamento del componente.

ReportLevel=4 – livello di dettaglio del report.

ShowOK=yes – modalità per registrare i messaggi sui file puliti nel report. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

ShowContainerResultOnly=no – modalità di visualizzazione dei risultati della scansione degli archivi in formato abbreviato. Per visualizzare il report in formato abbreviato, assegnare il valore **yes** a questa impostazione.

ShowObjectResultOnly=no – modalità di visualizzazione dei risultati di scansione di un oggetto semplice in formato abbreviato. Per visualizzare il formato abbreviato, assegnare il valore **yes** a questa impostazione.

La sezione **[scanner.container]** include impostazioni che determinano le azioni da compiere sugli archivi durante la protezione anti-virus del file system del server.

OnCorrupted=action – azioni da compiere in caso di rilevamento di un contenitore danneggiato.

OnInfected=action – azioni da eseguire in caso di disinfezione di oggetti infetti nel contenitore. Se la modalità di disinfezione dei file infetti è attivata, l'azione specificata sarà eseguita sui contenitori che non è stato possibile disinfettare dopo che tutte le altre azioni sugli oggetti sono state completate.

OnSuspicion=action – azioni da compiere in caso di rilevamento di un oggetto infetto all'interno di un contenitore.

OnWarning=action – azioni da compiere in caso di rilevamento di un file all'interno di un contenitore il cui codice assomiglia al codice di un virus noto.

OnCured =action – azioni da compiere in caso di rilevamento all'interno di un contenitore di un file infetto che era stato disinfettato con esito positivo.

OnProtected=action – azioni da compiere in caso di rilevamento di un oggetto protetto da password. Questi oggetti non possono essere analizzati.

OnError=actions – azioni da compiere qualora si verifichi un errore durante la scansione di un contenitore.

La sintassi dell'impostazione dell'**azione** è composta da due parti: l'azione stessa e un parametro opzionale divisi da uno spazio. Il valore del parametro opzionale è immesso tra virgolette. Per esempio, **OnInfected=move "/tmp/infected"**

L'azione può accettare uno dei seguenti valori:

- *move <folder>* – sposta file in <cartella>.
- *movePath <folder>* – sposta file in <cartella> ricorrente (con percorso assoluto).
- *remove* – elimina il file.
- *exec <parameter>* – esegue sull'oggetto l'azione definite dal valore <parametro>.

Di seguito sono riportate delle macro del parametro opzionale per l'azione da eseguire sui contenitori:

- %LIST% – nome del file o lista dei file infetti, sospetti o danneggiati trovati nel contenitore. Il formato del file è il seguente:
<virus name>\t<filename>.
- %FULLPATH% – percorso completo al contenitore.
- %FILENAME% – nome del file senza percorso.
- %CONTAINERTYPE% – tipo di contenitore in genere.

La sezione **[scanner.actions]** contiene impostazioni che definiscono le azioni da compiere con oggetti semplici di un determinato tipo durante la protezione anti-virus dei file server.

OnCorrupted=action – azioni da compiere in caso di rilevamento di un file danneggiato.

OnInfected=action – azioni da compiere in caso di rilevamento di un file infetto. Se la modalità di disinfezione dei file infetti è attivata, l'azione specificata sarà eseguita sugli oggetti che non è stato possibile pulire.

OnSuspicion=action – azioni da compiere in caso di rilevamento di un codice di file sospetto che assomiglia al codice di un virus sconosciuto a Kaspersky Lab.

OnWarning=action – azioni da compiere in caso di rilevamento di un file il cui codice assomiglia al codice di un virus noto.

OnCured=action – azioni da compiere in caso di rilevamento e disinfezione riuscita di un oggetto infetto.

OnProtected=action – azioni da compiere in caso di rilevamento di un oggetto protetto da password. Questi oggetti non possono essere analizzati.

OnError=actions – azioni da compiere qualora si verifichi un errore durante la scansione di un oggetto.

La sintassi delle azioni eseguite sugli oggetti sopra elencati è simile a quella per i contenitori descritta nella sezione precedente **[scanner.container]**.

La sezione **[scanner.display]** contiene le impostazioni per visualizzare il report sulla console:

ShowContainerResultOnly=no – modalità di visualizzazione dei risultati della scansione degli archivi in formato abbreviato sulla console. Per visualizzare il formato abbreviato, assegnare il valore **no** a questa impostazione.

ShowObjectResultOnly=no – modalità di visualizzazione dei risultati di scansione di un oggetto semplice in formato abbreviato sulla console. Per visualizzare il formato abbreviato, assegnare il valore **no** a questa impostazione.

ShowOK=yes – modalità per visualizzare i messaggi sui file puliti sulla console. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

ShowProgress=yes – modalità di visualizzazione sulla console di informazioni sul funzionamento corrente del componente (processo di download del database anti-virus, informazioni sulla scansione del file

corrente). Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

La sezione **[scanner.path]** contiene parametri che determinano i percorsi ai file senza i quali il modulo kavscanner non funziona:

BackupPath= path – percorso completo alla cartella di backup per le copie di riserva degli oggetti analizzati dal componente.

La sezione **[updater.path]** comprende impostazioni che definiscono i percorsi ai file richiesti per il funzionamento del componente di aggiornamento del database anti-virus:

AVBasesTestPath – percorso completo alla cartella di memorizzazione del database anti-virus.

AVBasesTestPath – percorso completo alla cartella di memorizzazione di backup del database anti-virus.

La sezione **[updater.report]** contiene le impostazioni per la generazione dei report sui risultati di funzionamento del componente keepup2date.

Append=yes – modalità per aggiungere nuovi messaggi al file del report. Per disabilitare questa modalità, assegnare il valore **no** a questa impostazione.

ReportFileName – nome del file nel quale saranno registrati i risultati del funzionamento del componente.

ReportLevel=4 – livello di dettaglio del report.

La sezione **[updater.options]** contiene le impostazioni di funzionamento del componente keepup2date:

KeepSilent=no – modalità per visualizzare sulla console informazioni sul funzionamento del modulo *keepup2date*. Per disabilitare questa modalità, assegnare il valore **yes** a questa impostazione.

ProxyAddress – indirizzo del server proxy utilizzato per il collegamento. Questa impostazione è specificata nel seguente formato: **http://username:password@url:port**; Le impostazioni **username (nome utente)** e/o **password** non sono obbligatorie per l'indirizzo del server proxy. Se l'indirizzo non è specificato, il suo valore sarà importato dalla variabile ambientale **http_proxy**.

UseProxy – modalità per l'utilizzo del server proxy per collegarsi con il server degli aggiornamenti di Kaspersky Lab. Se a questa impostazione è assegnato il valore **no**, il server proxy non viene usato. Se a questa impostazione è assegnato il valore **yes**, viene usato l'indirizzo del server proxy definito dal parametro **ProxyAddress**. Se il valore dell'impostazione **ProxyAddress** non è definito, viene usato il valore

della variabile ambientale **http_proxy**. Se il valore della variabile ambientale non è definito, il server proxy non viene usato.

UseUpdateServerUrl=no modalità per l'utilizzo dell'indirizzo definito dal parametro **UpdateServerUrl** per l'aggiornamento.

UseUpdateServerUrlOnly=no modalità per utilizzare solo l'indirizzo specificato nel parametro **UpdateServerUrl** per l'aggiornamento del database anti-virus. Se a questa impostazione è assegnato il valore **no**, in caso di mancata riuscita dell'aggiornamento del database anti-virus dall'indirizzo **UpdateServerUrl**, sarà usato un altro indirizzo dalla lista dei server di aggiornamento.

UpdateServerUrl=no http://url/ | ftp://url/ | /local_path/ – indirizzo per l'aggiornamento del database anti-virus.

PostUpdateCmd – comando eseguito immediatamente dopo il completamento dell'aggiornamento del database anti-virus con esito positivo. Il valore specificato nel file di configurazione incluso nel pacchetto di installazione dell'applicazione inizia a leggere automaticamente il database anti-virus aggiornato. Si raccomanda di non modificare il valore di questo parametro.

RegionSettings=ru codice del paese dell'utente; questo codice consente di selezionare il server di Kaspersky Lab più idoneo per il download degli aggiornamenti del database anti-virus.

ConnectTimeout=30 timeout di rete per l'aggiornamento del database anti-virus (in secondi). Se, durante il periodo indicato, i dati non sono ricevuti dal server, sarà selezionato un altro server dalla lista dei server di aggiornamento di Kaspersky Lab.

PassiveFtp=no utilizzo della modalità FTP passiva per il collegamento.

A.2 Tasti modificatori della riga di comando per il componente kavscanner

Le impostazioni del file di configurazione possono essere ridefinite dalla riga di comando all'avvio dell'applicazione utilizzando appositi tasti di modifica. Di seguito è illustrata una descrizione dettagliata di questi modificatori.

Opzioni della guida:	
-h	Visualizza le informazioni della guida sul componente kavscanner sulla console;

-v	Visualizza la versione dell'applicazione.
Opzioni di configurazione:	
-c (-C) <path_to_file>	Uso di un file di configurazione alternativo <path_to_file> ;
-g<path_to_file>	Posiziona la lista di tutti i virus noti, i cui record sono contenuti nel database anti-virus, nel file <path_to_file>
-f	Ignora il codice identificativo danneggiato del componente kavscanner e tenta di disinfettare il componente.
Opzioni di scansione:	
-e <option>	Modifica dell'opzione di scansione predefinita. Come <opzione> possono essere usate le seguenti modalità:
P/p	Abilita/disabilita la scansione dei file compressi;
A/a	Abilita/disabilita la scansione degli archivi;
S/s	Abilita/disabilita la scansione degli archivi a decompressione automatica;
B/b	Abilita/disabilita la scansione dei database di posta elettronica;
M/m	Abilita/disabilita la scansione dei messaggi in formato testo normale;
E/e	Abilita/disabilita l'analizzatore di codici euristico.
-R/r	Abilita/disabilita la scansione ricorrente;
-S/s	Abilita/disabilita la modalità di apertura symlinks;
-l	Scansione dei soli file system locali.
Opzioni di generazione dei report:	

-q	Comando che disabilita la visualizzazione dei messaggi sulla console;
-o <name>	Specifica il nome del file nel quale sarà registrato il report sul funzionamento del componente; se il nome del file non è specificato, il report non sarà generato;
-j<number>	Specifica il livello di dettaglio del report in base alla quantità di dati contenuta nello stesso. Come <opzione> può essere utilizzato il seguente livello di dettaglio:
1	Abilita/disabilita la visualizzazione di messaggi su altri errori;
2	Abilita/disabilita la visualizzazione di messaggi informativi;
3	Abilita/disabilita la visualizzazione di messaggi sull'attività di scansione;
-x <opzione>	Specifica il livello di dettaglio per il report di scansione visualizzato sulla console. Come <opzione> può essere utilizzato il seguente livello di dettaglio:
O/o	Formato abbreviato/esteso dei messaggi sulla scansione di un oggetto semplice;
C/c	Formato abbreviato/esteso dei messaggi sulla scansione di un archivio;
N/n	Abilita/disabilita la visualizzazione dei messaggi sui file puliti sulla console.
P/p	Abilita/disabilita la visualizzazione di messaggi sull'operazione corrente del componente sulla console.
-m <opzione>	Specifica il livello di dettaglio per il report di scansione riportato nel file del report. Come <opzione> possono essere usate le seguenti modalità:
O/o	Formato abbreviato/esteso dei messaggi sulla scansione di un oggetto semplice;

C/c	Formato abbreviato/esteso dei messaggi sulla scansione di un archivio;
N/n	Abilita/disabilita l'inclusione di messaggi sui file puliti nel file del report.
Opzioni relative ai file:	
-p<option> <file_name>	Salva l'elenco di oggetti nel file specificato; salva ogni oggetto con il percorso completo in una riga nuova. Come <opzione> possono essere usate le seguenti modalità:
i	Salva l'elenco di oggetti infetti nel file <file_name> ;
s	Salva l'elenco di oggetti sospetti nel file <file_name> ;
c	Salva l'elenco di oggetti danneggiati nel file <file_name> ;
w	Salva l'elenco di oggetti il cui codice assomiglia al codice di un virus noto nel file <file_name> .
-@ <filelist.lst>	Scansiona il percorso degli oggetti specificato nel file <filelist.lst> .
Opzioni di elaborazione file (l'uso di questi modificatori nella riga di comando annulla l'esecuzione delle azioni definite nel file di configurazione):	
-i0	Ricerca dei soli virus;
-i1	Disinfetta gli oggetti infetti; ignora se la disinfezione non è possibile;
-i2	Disinfetta gli oggetti infetti; se la disinfezione non è possibile e se l'oggetto è un oggetto semplice, eliminarlo; non eliminare gli oggetti infetti dal contenitore.
-i3	Disinfetta gli oggetti infetti; se la disinfezione non è possibile e se l'oggetto è un oggetto semplice, eliminarlo; se l'oggetto infetto si trova all'interno di un contenitore, non eliminare il singolo oggetto ma l'intero contenitore.
-i4	Elimina gli oggetti e i contenitori infetti.

A.3 Codici visualizzati per il componente kavscanner

Durante il suo funzionamento il componente kavscanner potrebbe produrre i seguenti codici:

0	Non è stato rilevato alcun virus;
5	Tutti gli oggetti infetti sono stati puliti;
10	Sono stati rilevati archivi protetti da password;
15	Sono stati rilevati file danneggiati;
20	Sono stati rilevati file sospetti;
21	Sono stati rilevati file contenenti un codice che assomiglia a quello di un virus noto;
25	Sono stati rilevati file infetti;
30	Si è verificato un errore di system durante la scansione del file;
50	Impossibile caricare il database anti-virus (il percorso specificato nel file di configurazione non è stato trovato);
55	Il database anti-virus è stato danneggiato;
60	La data indicata sul database anti-virus è successiva al periodo di validità della chiave di licenza;
64	Mancano dati relativi alla licenza oppure non è stata trovata la chiave di licenza nel percorso specificato nel file di configurazione;
66	Opzione non valida per il file di configurazione
65	Impossibile caricare il file di configurazione;
70	Il componente kavscanner è stato danneggiato;

75	Il componente kavscanner è stato danneggiato in modo irreparabile.
-----------	--

A.4 Tasti modificatori della riga di comando del componente kavmonitor

Opzioni della guida:	
-h	Visualizza le informazioni della guida sul componente sulla console;
-v	Visualizza la versione dell'applicazione.
Opzioni di configurazione:	
-c<path_to_file>	Uso di un file di configurazione alternativo <path_to_file> ;

A.5 Tasti modificatori della riga di comando per il componente licensemanager

Opzioni della guida:	
-h	Visualizza le informazioni della guida sul componente <i>licensemanager</i> sulla console;
-v	Visualizza la versione dell'applicazione.
Opzioni relative alla gestione delle chiavi di licenza:	
-s	Visualizza sulla console informazioni relative a tutte le chiavi di licenza installate;
-c (-C) <path_to_file>	Uso di un file di configurazione alternativo <path_to_key_file> ;

-k <path_to_file>	Visualizza sulla console informazioni relative alla chiave <path_to_key_file>;
-a <path_to_file>	Installa la chiave di licenza <path_to_key_file>;
-d <path_to_file>	Rimuove la chiave di licenza.

A.6 Codici visualizzati per il componente licensemanager

Durante il suo funzionamento, il componente licensemanager potrebbe produrre i seguenti codici:

0	Il componente ha caricato con successo le informazioni sulla chiave di licenza ed ha completato le operazioni con esito positivo.
30	Si è verificato un errore di sistema durante il funzionamento del componente;
64	Mancano dati relativi alla licenza oppure non è stata trovata la chiave di licenza nel percorso specificato nel file di configurazione;
65	Impossibile caricare il file di configurazione;
66	Opzione non valida per il file di configurazione

A.7 Tasti modificatori della riga di comando del componente keepup2date

Opzioni della guida:	
-v	-v
-h	-h

-s	-s
Opzioni di funzionamento:	
-r	-r
-k	-k
-q	-q
-e	-e
-x<path_to_file>	-x<path_to_file>
-g <URL>	-g <URL>
-d<path_to_file>	-d<path_to_file>
Opzioni di generazione dei report:	
-l<path_to_file>	-l<path_to_file>

A.8 Codici visualizzati per il componente keepup2date

Durante questa operazione il componente *keepup2date* potrebbe produrre i seguenti codici:

0	Il database anti-virus non richiede di essere aggiornato;
1	L'aggiornamento del database anti-virus è stato completato;
10	Si è verificato un errore critico; il processo di aggiornamento sarà interrotto;
12	Si è verificato un errore durante il rollback all'ultimo aggiornamento del database anti-virus;

30	Impossibile eseguire il comando PostUpdateCmd in seguito all'aggiornamento del database anti-virus;
60	Mancano dati relativi alla licenza oppure non è stata trovata la chiave di licenza nel percorso specificato nel file di configurazione;
75	Impossibile caricare il file di configurazione o impostazioni errate.

APPENDICE B. DOMANDE FREQUENTI

Il presente capitolo illustra le domande più frequenti degli utenti relativamente a installazione, impostazione e funzionamento di Kaspersky Anti-Virus; la presente sezione cerca di fornire risposte dettagliate.



Domanda: *È possibile utilizzare Kaspersky Anti-Virus con prodotti anti-virus di altri fabbricanti?*

Si raccomanda di disinstallare i prodotti anti-virus di altri fabbricanti prima di installare Kaspersky Anti-Virus per evitare conflitti tra i programmi.



Domanda: *Kaspersky Anti-Virus non rianalizza un file. Perché?*



Domanda: *Kaspersky Anti-Virus non ripete la scansione dei file. Perché?*

In effetti, Kaspersky Anti-Virus non rianalizza i file che non sono stati modificati dall'ultima scansione.

Questo è stato possibile grazie alla nuova tecnologia iChecker. L'applicazione implementa la tecnologia utilizzando un database dei checksum degli oggetti.



Domanda: *Perché Kaspersky Anti-Virus causa un rallentamento delle prestazioni del computer, in particolare sovraccaricando il processore?*

Il rilevamento dei virus è un problema di calcolo matematico che richiede molte risorse, analisi strutturale, calcolo dei checksum e conversione di dati matematici. Il tempo del processore è pertanto la risorsa principalmente consumata dall'Anti-Virus, e ogni nuovo virus aggiunto al database anti-virus database aumenta il tempo complessivo di analisi.

Altri prodotti anti-virus accelerano i tempi di analisi escludendo dai propri database sia i prodotti meno facilmente rilevabili o meno frequenti (per esempio in una data posizione geografica), che i formati di file che richiedono analisi complicate (per esempio i PDF). Kaspersky Lab

ritiene che lo scopo di una protezione anti-virus sia quello di fornire una sicurezza anti-virus reale e completa per i propri utenti.

Gli utenti esperti possono ovviamente accelerare l'analisi anti-virus disabilitando l'analisi di determinati tipi di file. Si ricorda, tuttavia, che così facendo, si diminuisce il livello di sicurezza complessivo.

Kaspersky Anti-Virus riconosce oltre 700 formati di file archivi e compressi. Questo è fondamentale per la sicurezza anti-virus in quanto un codice nocivo eseguibile potrebbe nascondersi all'interno dei file di qualsiasi formato riconosciuto. Tuttavia, nonostante la crescita giornaliera del numero di virus rilevati da Kaspersky Anti-Virus (ogni giorno compaiono circa 30 nuovi virus) oltre al sempre crescente numero di formati di file riconosciuti, ogni nuova versione dell'applicazione funziona più velocemente di quella precedente. Questo risultato è stato ottenuto attraverso l'uso di nuove tecnologie esclusive, come iChecker™ sviluppate da Kaspersky Lab.



Domanda: Perché occorre disporre della chiave di licenza? La copia dell'Anti-Virus funziona anche senza?

No, Kaspersky Anti-Virus non funziona senza una chiave di licenza.

Se si è ancora indecisi se acquistare o meno Kaspersky Anti-Virus, possiamo fornire un file contenente una chiave di licenza temporanea (chiave di prova) che funzionerà solo per due settimane o per un mese. Allo scadere di questo periodo, la chiave risulta bloccata.



Domanda: Cosa succede quando la licenza scade?

Dopo la scadenza della licenza, Kaspersky Anti-Virus continua a funzionare ma la funzione di aggiornamento dei database anti-virus sarà disabilitata. L'applicazione anti-virus continua a pulire gli oggetti infetti utilizzando i vecchi database anti-virus.

Se si verifica una situazione del genere, contattare l'amministratore di sistema, il rivenditore presso il quale è stato acquistato Kaspersky Anti-Virus o Kaspersky Lab direttamente.



Domanda: la chiave di licenza per Kaspersky Anti-Virus è su dischetto. Cosa fare se il computer non è dotato di unità dischetto?

Il problema può essere risolto in molti modi.

È possibile scrivere una e-mail con la descrizione del problema all'ufficio vendite di Kaspersky Lab (sales@kaspersky.com). Assicurarsi di indicare la data e il luogo in cui è stato acquistato Kaspersky Anti-Virus e il numero completo di registrazione. Il personale dell'ufficio vendite invierà il file contenente la chiave di licenza all'indirizzo e-mail specificato.

È inoltre possibile leggere il contenuto del dischetto su un altro computer dotato di unità dischetto e registrare i dati su un altro supporto leggibile dal computer di cui si dispone. Durante l'installazione di Kaspersky Anti-Virus, specificare quel supporto come sorgente della chiave di licenza.

In alternativa, il contenuto del dischetto può essere letto su un altro computer con un'unità corrispondente e inviare via e-mail il file contenente la chiave di licenza al proprio indirizzo. Una volta ricevuto il file, salvarne i dati in allegato in qualsiasi cartella sul disco fisso e specificare la cartella come sorgente della chiave di licenza durante l'installazione di Kaspersky Anti-Virus.



Domanda: *L'Anti-Virus non funziona.*

Che fare?

Innanzitutto, controllare se la documentazione specifica una soluzione al problema, in particolare nella presente sezione o sul nostro sito web.

Inoltre, si raccomanda di richiedere assistenza al distributore presso il quale è stato acquistato Kaspersky Anti-Virus, o consultare la sezione di Supporto Tecnico di Kaspersky Lab (<http://www.kaspersky.ru/faq>).



Domanda: *A cosa servono gli aggiornamenti quotidiani?*

Qualche anno fa i virus venivano trasmessi dai dischetti e il computer poteva essere protetto adeguatamente attraverso l'installazione di un programma anti-virus seguito da saltuari aggiornamenti dei database. Tuttavia, per far fronte alle recenti epidemie virali che si diffondono nel mondo in poche ore, la protezione anti-virus scaricata da database non aggiornati potrebbe essere inefficace contro nuove minacce. Per essere protetti contro nuovi virus, si consiglia di aggiornare i database anti-virus ogni giorno.

Ogni anno Kaspersky Lab aumenta la frequenza degli aggiornamenti pubblicati per i database anti-virus, i cui server sono attualmente aggiornati ogni tre ore.

L'aggiornamento dei moduli dell'applicazione è una funzione supplementare che consente sia la correzione delle vulnerabilità scoperte che l'aggiunta di nuove funzioni.



***Domanda:** Quali modifiche sono state apportate al servizio di aggiornamento, a partire dalla versione 5.0?*

La nuova gamma di prodotti Kaspersky Lab, a partire dalla versione 5.0, presenta un nuovo servizio di aggiornamento che è stato sviluppato in base alle richieste degli utenti e alle esigenze di commercializzazione. Inoltre, gli sviluppatori hanno aumentato il livello di automazione dell'intera procedura di aggiornamento, dalla preparazione degli aggiornamenti presso Kaspersky Lab fino al momento dell'aggiornamento dei file pertinenti sui computer degli utenti.

I vantaggi del nuovo servizio di aggiornamento includono:

- Capacità di ripristinare l'aggiornamento dei file in seguito a una caduta del collegamento. Al momento del ripristino del collegamento, vengono recuperati solo i file che non sono stati ancora scaricati.
- Gli aggiornamenti cumulativi sono di dimensioni dimezzate. Un aggiornamento cumulativo contiene l'intero database anti-virus; pertanto, la sua dimensione supera considerevolmente quella degli aggiornamenti tipici. Il nuovo servizio si avvale di una tecnologia speciale che consente di utilizzare un database anti-virus esistente per un aggiornamento cumulativo.
- Scaricamento accelerato da Internet. Kaspersky Anti-Virus preleva i file da un server di aggiornamento Kaspersky Lab situato nel paese dell'utente. Inoltre, i server sono assegnati in base alle loro prestazioni, pertanto l'utente non verrà convogliato su un server sovraccarico se vi è un altro server libero disponibile.
- Uso di black list delle chiavi. Gli utenti sprovvisti di licenza o illegali ora non possono utilizzare il servizio di aggiornamento. Gli utenti titolari di licenza quindi non risentiranno del sovraccarico del server.
- Le aziende ora possono creare un server di aggiornamento in locale. Questa funzione è concepita per le organizzazioni in cui una singola LAN collega i computer protetti dai prodotti Kaspersky Lab. Qualsiasi computer sulla LAN può essere commutato su un server di aggiornamento che recupera gli aggiornamenti da Internet, li mette su una cartella locale e li condivide con tutti gli altri computer collegati in rete.



Domanda: Un utente non autorizzato può sostituire il database anti-virus?

Ciascun database anti-virus è identificato da una firma inequivocabile controllata da Kaspersky Anti-Virus ogni qualvolta si accede al database. Se la firma è errata o la data del database è successiva a quella della scadenza della licenza, Kaspersky Anti-Virus non la utilizza.



Domanda: Con quali versioni del sistema operativo Linux funziona Kaspersky Anti-Virus?

La versione 5.5 di Kaspersky Anti-Virus è stata testata con le distribuzioni RedHat, Debian e SuSE e Mandria Linux OS e i pacchetti Kaspersky Anti-Virus sono stati compilati specificamente per queste versioni di Linux.

L'applicazione potrebbe funzionare in modo scorretto se utilizzata con versioni non incluse nell'elenco supportato da Kaspersky Lab. Questo è dovuto innanzitutto a caratteristiche specifiche del sistema operativo. Per esempio, il sistema operativo può utilizzare una differente versione di una libreria o gli script di inizializzazione del sistema possono avere un'ubicazione non standard. In questi casi, il Supporto Tecnico di Kaspersky Lab non sarà di aiuto.



Domanda: perché kavmonitor avvia più processi contemporaneamente?

Il numero di processi avviati da *kavmonitor* è determinato dal parametro **CheckFileLimit** nel file di configurazione dell'applicazione; specifica il numero di file elaborati contemporaneamente. Pertanto, il numero di processi di controllo è sempre superiore a 1 (come impostazione predefinita sono avviati 20 processi). Se non vi sono file da analizzare, i processi non consumano risorse di sistema.



Domanda: È possibile controllare Kaspersky Anti-Virus utilizzando Network Control Centre per Windows?

Il Network Control Centre per Windows non può essere utilizzato per operazioni con Kaspersky Anti-Virus per workstation e file server Linux e FreeBSD. In questa versione del prodotto, abbiamo fornito l'opportunità di configurare l'applicazione a distanza attraverso uno speciale modulo Webmin.



Domanda: Come procedere per salvare su un file il contenuto di ciò che l'applicazione visualizza sulla console?

Per salvare le informazioni prodotte da Kaspersky Anti-Virus sulla console durante l'attività dell'applicazione, occorre configurare il parametro corrispondente oppure immettere quanto segue nella riga di comando:

```
$ some_app > ./text_file 2>&1
```

dove:

`some_app` – indica il software, la visualizzazione standard e i messaggi di errore che si desidera salvare in formato file;

`text_file` – indica il percorso completo al file in cui saranno registrate le informazioni.

Per esempio:

```
$keepup2date > ./updater.log 2>&1
```

In quel caso, i messaggi standard e i messaggi di errore emessi dal componente *keepup2date* saranno memorizzati nel file *updater.log*.

APPENDICE C. KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab è diventata un leader indiscusso nel settore delle tecnologie per la sicurezza informatica. Produce una vasta gamma di applicazioni per la sicurezza dei dati e offre soluzioni complete di alto livello per garantire la sicurezza di computer e reti contro ogni tipo di programma dannoso, messaggi di posta elettronica non sollecitati e indesiderati e attacchi di pirateria informatica.

Kaspersky Lab è un'azienda internazionale con sede nella Federazione Russia e filiali nel Regno Unito, Francia, Germania, Giappone, USA (CA), Benelux, Cina e Polonia. Recentemente è stato inaugurato un nuovo reparto, l'European Anti-Virus Research Centre, in Francia. Kaspersky Lab conta su una rete di partner costituita da oltre 500 aziende in tutto il mondo.

Oggi Kaspersky Lab si avvale di oltre 450 esperti, tutti specializzati in tecnologie antivirus, 10 dei quali in possesso di laurea in amministrazione aziendale, 16 di specializzazione postlaurea, e due appartenenti alla Computer Anti-Virus Researcher's Organization (CARO).

Kaspersky Lab offre soluzioni di sicurezza di alto livello, elaborate grazie a un'esperienza esclusiva accumulata in più di 14 anni di attività nel settore dei virus informatici. La scrupolosa analisi delle attività dei virus consente all'azienda di offrire una protezione completa contro minacce presenti e perfino future. La resistenza agli attacchi futuri è la strategia di base implementata in tutti i prodotti Kaspersky Lab. L'azienda si trova costantemente all'avanguardia rispetto a numerosi altri produttori offrendo una protezione antivirus completa per utenti domestici e aziendali.

Anni di duro lavoro ne hanno fatto un'azienda leader tra i principali produttori di software per la sicurezza informatica. Kaspersky Lab è stata una delle prime aziende di questo tipo a sviluppare i più severi standard della protezione antivirus. Il prodotto di punta dell'azienda, Kaspersky Anti-Virus[®], offre una protezione completa a tutti i livelli di una rete, inclusi workstation, server di file, gateway di posta elettronica, firewall e portatili. I suoi strumenti di gestione, pratici e di facile utilizzo, garantiscono l'automazione avanzata per una sollecita protezione antivirus ad ogni livello dell'impresa. Numerose imprese di grande notorietà si affidano a Kaspersky Anti-Virus[®], per esempio Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India) e BorderWare (Canada).

I clienti di Kaspersky Lab beneficiano di un'ampia gamma di servizi supplementary che garantiscono sia il funzionamento stabile dei nostri prodotti, che la conformità con specifici requisiti aziendali. Il database anti-virus di Kaspersky Lab viene aggiornato a cadenza oraria. La società fornisce ai propri clienti un servizio di supporto tecnico attivo 24 ore al giorno, disponibile in varie lingue per soddisfare una clientela internazionale.

C.1. Altri prodotti Kaspersky Lab

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus Personal è stato concepito per fornire una protezione anti-virus ai personal computer che operano su sistema operativo Microsoft Windows 98/ME o Microsoft Windows 2000/NT/XP contro tutti i virus noti, incluso il software potenzialmente pericoloso. Kaspersky Anti-Virus Personal fornisce il monitoraggio in tempo reale di tutte le fonti di intrusione dei virus: e-mail, Internet, dischetti, CD, ecc. L'esclusivo sistema euristico di analisi dei dati consente l'efficace neutralizzazione di virus ancora sconosciuti. Questa applicazione può operare nelle seguenti modalità (che possono essere impiegate separatamente o congiuntamente):

- **Protezione in tempo reale** - scansione anti-virus di tutti gli oggetti eseguiti, aperti o salvati sul computer dell'utente.
- **Scansione a richiesta**-scansione e pulizia dell'intero computer o dei singoli dischi, cartelle o file. La scansione può essere avviata manualmente o è possibile configurare una scansione automatica a cadenze programmate.

Kaspersky Anti-Virus® Personal non sottopone nuovamente a scansione gli oggetti già analizzati durante una scansione precedente e che da allora non sono stati modificati e questo sia durante la scansione in tempo reale che durante quella programmata. Questa funzione **augmenta notevolmente la velocità di funzionamento del programma.**

L'applicazione crea un'affidabile barriera contro i virus quando tentano di introdursi nel computer attraverso la posta elettronica. Kaspersky Anti-Virus® Personal esegue la scansione e la pulizia automatica di tutta la posta in entrata e in uscita inviata o ricevuta utilizzando i protocolli POP3 e STMP e fornisce un rilevamento altamente efficiente dei virus nei database di posta.

L'applicazione supporta oltre 700 formati di file archivi e compressi e fornisce la scansione automatica del contenuto oltre alla rimozione del codice nocivo dalle estensioni **ZIP, CAB, RAR, ARJ, LHA e ICE.**

La configurazione dell'applicazione risulta semplice ed intuitiva grazie alla possibilità di selezionare uno dei tre livelli di protezione preimpostati: **Protezione massima, Raccomandato o Alta velocità.**

Il database anti-virus è aggiornato ogni ora e il download sul computer è garantito anche quando il computer viene temporaneamente disconnesso da Internet o occorre modificare la connessione.

Kaspersky Anti-Virus ® Personal Pro

Pacchetto progettato per offrire una protezione antivirus completa ai computer domestici con sistema operativo Windows 98/ME, Windows 2000/NT e Windows XP oltre alle applicazioni di MS Office 2000/NT, Microsoft Windows XP e le applicazioni Microsoft Office. Kaspersky Anti-Virus Personal Pro include un'applicazione di facile utilizzo per il prelievo quotidiano automatico degli aggiornamenti del database antivirus e dei moduli del programma. L'esclusivo sistema di analisi euristica di seconda generazione rileva con efficacia perfino i virus ignoti. Kaspersky Anti-Virus Pro presenta un'interfaccia migliorata sotto molti aspetti, agevolando più che mai l'uso del programma.

Kaspersky Anti-Virus ® Personal Pro presenta le seguenti funzioni:

- **scansione manuale** di dischi locali;
- **protezione in tempo reale** di tutti i file dai virus;
- **un filtro di posta** che scansiona e disinfetta tutti i messaggi in entrata e in uscita per qualsiasi clienti di posta e utilizza i protocolli PO3 e SMTP e rileva in modo efficiente i virus nei database di posta elettronica;
- **behavior blocker** che garantisce la protezione massima delle applicazioni MS Office dai virus.
- **Analisi degli archivi** - Kaspersky Anti-Virus riconosce oltre 900 formati di file archivi e compressi e garantisce l'analisi anti-virus automatica del contenuto e la rimozione dei codici nocivi dai file all'interno di archivi con estensione **ZIP, CAB, RAR, ARJ, LHA e ICE**.

Kaspersky ® Anti-Hacker

Kaspersky ® Anti-Hacker è una firewall personale, progettata cioè per garantire la protezione di computer con sistema operativo Windows da qualsiasi accesso non autorizzato ai dati e dagli attacchi esterni da Internet o reti locali.

Kaspersky ® Anti-Hacker controlla l'attività di rete TCP/IP di tutte le applicazioni eseguite sul computer. In caso di rilevazione di azioni sospette, il programma blocca l'accesso alla rete da parte di tali applicazioni. Questa misura consente all'utente di conservare con sicurezza dati confidenziali sul proprio computer.

Grazie alla tecnologia SmartStealth™ la rilevazione del computer dall'esterno è oggi più difficoltosa. In questa modalità trasparente, l'applicazione opera in modo continuo per tutelare il computer mentre è presente in rete. Fornisce trasparenza e accessibilità ai dati.

- Kaspersky ® Anti-Hacker blocca i più comuni attacchi di pirateria informatica ed effettua un monitoraggio costante dei tentativi di scansione delle porte del computer.

- La configurazione dell'applicazione implica unicamente la scelta di uno dei cinque livelli di sicurezza. Per impostazione predefinita, il programma si apre sulla modalità di autoapprendimento che configura automaticamente il sistema di sicurezza in base alle risposte dell'utente a eventi di vario tipo. Questa caratteristica consente di personalizzare il programma in base alle preferenze ed esigenze specifiche dell'utente.

Kaspersky® Personal Security Suite

Kaspersky Personal Security Suite è un software concepito per organizzare la protezione globale di personal computer con sistemi operativi Microsoft Windows. La suite impedisce che programmi nocivi e potenzialmente pericolosi penetrino attraverso qualsiasi possibile sorgente di dati e protegge l'utente da tentativi non autorizzati di accedere ai dati del computer, oltre a bloccare lo spam.

Kaspersky Personal Security Suite presenta le seguenti funzioni:

- protezione anti-virus per i dati salvati sul computer;
- protezione anti-spam per gli utenti di Microsoft Office Outlook e Microsoft Outlook Express;
- protezione del computer da accesso non autorizzato e anche dagli attacchi degli hacker attraverso la LAN o Internet.

Kaspersky Lab News Agent

News Agent consente la consegna tempestiva dei bollettini pubblicati da Kaspersky Lab, per le notifiche sullo stato corrente dell'attività virale e sulle ultime notizie. Il programma legge la lista dei canali di news disponibili e il relativo contenuto dal server corrispondente di Kaspersky Lab alla frequenza specificata.

Il prodotto esegue le seguenti funzioni:

- Visualizza nella barra di sistema lo stato corrente dell'attività virale.
- Il prodotto consente agli utenti di abbonarsi e disdire l'abbonamento per ricevere le news.
- Recupera le news da ogni canale sottoscritto alla frequenza specificata e comunica le ultime notizie.
- Consente di controllare le news sui canali sottoscritti.
- Consente di controllare la lista dei canali e il relativo stato.
- Consente di aprire le pagine contenenti informazioni dettagliate sulle news sul proprio browser.

News Agent è un'applicazione Windows stand-alone, che può essere usata indipendentemente o può essere fornita integrata a varie soluzioni offerte da Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

Questo programma è un servizio gratuito offerto ai visitatori del sito aziendale di Kaspersky Lab. Il servizio consente un efficiente controllo anti-virus online del computer. Kaspersky OnLine Scanner si esegue direttamente dal browser. Pertanto, l'utente può rapidamente testare i propri computer in caso del minimo sospetto di infezione. Questo servizio consente ai visitatori di:

- Escludere gli archivi e i database di posta dalla scansione.
- Selezionare i database anti-virus standard/estesi per la scansione.
- Salvare un report sui risultati di scansione in formato txt o html.

Kaspersky® OnLine Scanner Pro

Questo programma è un servizio riservato agli utenti iscritti del sito aziendale di Kaspersky Lab. Il servizio consente un efficiente controllo anti-virus online del computer e la disinfezione di file pericolosi. Kaspersky OnLine Scanner Pro si esegue direttamente dal browser. Questo servizio consente ai visitatori di:

- Escludere gli archivi e i database di posta dalla scansione.
- Selezionare i database anti-virus standard/estesi per la scansione.
- Salvare un report sui risultati di scansione in formato txt o html.

Kaspersky Anti-Virus® 6.0

Kaspersky Anti-Virus 6.0 è concepito per proteggere i personal computer da software nocivo attraverso una combinazione ottimale di metodi convenzionali di protezione anti-virus e nuove tecnologie proattive.

Il programma fornisce complessi controlli anti-virus comprendenti:

- Scansione anti-virus del traffico di posta a livello del protocollo di trasmissione dati (POP3, IMAP e NNTP per la posta in entrata e SMTP per la posta in uscita) indipendentemente dal client di posta utilizzato, oltre alla pulizia dei database di posta.
- Scansione anti-virus in tempo reale del traffico Internet trasferito via HTTP.
- Scansione anti-virus di singoli file, directory e unità. Inoltre, è possibile utilizzare un'operazione di scansione preimpostata per lanciare l'analisi anti-virus esclusivamente per le aree critiche del sistema operativo e per gli oggetti ad esecuzione automatica di Microsoft Windows.

La protezione proattiva fornisce le seguenti funzioni:

- **Controllo delle modifiche all'interno del file system.** Il programma consente all'utente di creare una lista di applicazioni che saranno controllate in base al componente. Questo contribuisce a tutelare l'integrità delle applicazioni dalle influenze del software nocivo.
- **Monitoraggio dei processi nella memoria ad accesso casuale.** Kaspersky Anti-Virus 6.0 notifica tempestivamente l'utente ogni qualvolta rileva processi pericolosi, sospetti o nascosti o in caso di rilevamento di modifiche non autorizzate nei processi standard.
- **Monitoraggio delle modifiche di registro del sistema operativo** grazie al controllo di registro interno del sistema.
- **Blocco delle macro VBA pericolose** nei documenti di Microsoft Office.
- **Ripristino del sistema** in seguito all'influenza di spyware nocivo grazie alla registrazione di tutte le modifiche nel registro e nel file system del computer e alla possibilità di eseguire il rollback a discrezione dell'utente.

Kaspersky® Internet Security 6.0

Kaspersky® Internet Security 6.0 è una soluzione integrata per la protezione dei personal computer dalle più diffuse minacce informatiche, come virus, attacchi degli hacker, spam e spyware. Un'interfaccia utente comune consente la configurazione e la gestione di tutti i componenti della soluzione.

La funzione di protezione anti-virus comprende:

- **Scansione anti-virus del traffico di posta** a livello del protocollo di trasmissione dati (POP3, IMAP e NNTP per la posta in entrata e SMTP per la posta in uscita) indipendentemente dal client di posta utilizzato. Il programma include plug-in per diffusi client di posta elettronica (Microsoft Office Outlook, Microsoft Outlook Express e The Bat!) e supporta la pulizia dei loro database.
- **Scansione anti-virus in tempo reale del traffico Internet** trasferito via HTTP.
- **Protezione del file system:** scansione anti-virus di singoli file, directory e unità. Inoltre, l'applicazione può eseguire un'analisi anti-virus esclusivamente per le aree critiche del sistema operativo e per gli oggetti ad esecuzione automatica di Microsoft Windows.
- **Protezione proattiva:** il programma esegue il monitoraggio costante dell'attività dell'applicazione e dei processi nella memoria RAM impedendo modifiche pericolose al file system e al registro e ripristina il sistema dopo influenze di software nocivo.

Protezione dalle truffe via Internet garantita grazie alla capacità di riconoscere gli attacchi di phishing; questo impedisce la diffusione di dati confidenziali (innanzitutto, password, numeri di conti bancari e di carte di credito), e blocca l'esecuzione di script pericolosi sulle pagine web, pop-up e banner pubblicitari. La funzione di **blocco dell'addebito chiamate** agevola l'identificazione del software che tenta di utilizzare il modem dell'utente per collegarsi furtivamente a servizi telefonici a pagamento e impedisce questo tipo di attività.

Kaspersky® Internet Security 6.0 **registra i tentativi di scansione delle porte del computer**, che spesso precedono gli attacchi di rete, e difende efficacemente dai tipici attacchi di pirateria. Il programma utilizza **regole definite come base** per controllare tutte le transazioni effettuate in rete tenendo traccia di **tutti i pacchetti di dati in entrata e in uscita. La modalità Stealth** (derivata dalla tecnologia SmartStealth™) **impedisce che il computer sia rilevato dall'esterno**. Commutandosi su quella modalità, il sistema blocca tutta l'attività di rete tranne qualche transazione consentita nelle regole definite dall'utente.

Il programma si avvale di un approccio complesso al filtro anti-spam dei messaggi di posta in entrata:

- Verifica comparata con la rubrica/lista nera dei destinatari (inclusi gli indirizzi dei siti di phishing).
- Ispezione di frasi nel corpo del messaggio.
- Analisi del testo dei messaggi utilizzando un algoritmo di autoapprendimento.

Riconoscimento dello spam inviato nei file immagine.

Kaspersky® Security per PDA

Kaspersky® offre un'affidabile protezione antivirus dei dati memorizzati su PDA con Palm OS o Windows CE, e di qualsiasi informazione trasferita da un PC o scheda di estensione, file ROM e database. Il software contiene una combinazione di strumenti antivirus mirati:

- uno **scanner antivirus**, usato per la scansione manuale di tutti i dati memorizzati (sia sul PDA stesso che su qualsiasi scheda di estensione) e
- un **monitor antivirus** che intercetta i virus durante il trasferimento di dati con l'utility HotSync™ o prelevati da dispositivi portatili.

Esso offre l'accesso criptato al dispositivo e codifica tutti i dati memorizzati nel dispositivo e nelle schede di memoria.

Kaspersky Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile fornisce la protezione anti-virus per dispositivi mobili con sistema operativo Symbian e Microsoft Windows Mobile. Il programma fornisce una scansione anti-virus completa, inclusi:

- **Scansione su richiesta** della memoria integrata del dispositivo portatile, schede di memoria, singola cartella o file specifico. In caso di rilevamento di un oggetto infetto, questo viene trasferito nella cartella Quarantine o eliminato.
- **Scansione in tempo reale** – tutti i file in entrata e in uscita vengono analizzati automaticamente, così come quelli a cui è stato tentato l'accesso
- **Scansione programmata** dei dati memorizzati nella memoria del dispositivo portatile
- **Protezione dallo spam nei messaggi di testo**

Kaspersky Anti-Virus® Business Optimal

Il pacchetto è stato sviluppato per garantire una soluzione di sicurezza configurabile specifica per reti aziendali di piccole e medie dimensioni.

Kaspersky Anti-Virus® Business Optimal include la protezione antivirus completa 1 per:

- *workstation* con Windows 98/ME, Windows NT/2000/XP Workstation e Linux;
- *File server* con sistema operativo Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD e Linux; dispositivo di archiviazione file *Samba*
- *Sistemi di posta elettronica* inclusi Microsoft Exchange 2000/2003, Lotus Notes/Domino, postfix, exim, sendmail, e gmail

Internet gateway: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition, Microsoft ISA Server 2004 Standard Edition

Il kit retail di Kaspersky Anti-Virus® Business Optimal comprende Kaspersky® Administration Kit, uno strumento esclusivo per la gestione e l'amministrazione automatizzate.

La vasta gamma di programmi antivirus disponibili offre la massima libertà di scelta in base al sistema operativo e alle applicazioni in uso.

Kaspersky® Corporate Suite

Questo pacchetto è stato sviluppato al fine di offrire una protezione totale dei dati di reti aziendali di qualsiasi dimensione e complessità. I componenti del pacchetto garantiscono la protezione di tutti i nodi di una rete aziendale, anche in

¹ In base al tipo di kit retail.

ambienti informatici misti. Kaspersky® Corporate Suite supporta la maggior parte dei sistemi operativi e delle applicazioni in uso nelle aziende. Tutti i componenti del pacchetto sono gestiti da una console mediante un'unica interfaccia utente. Kaspersky® Corporate Suite è un affidabile sistema di protezione di alto livello totalmente compatibile con le esigenze specifiche di ogni configurazione di rete.

Kaspersky® Corporate Suite include la protezione antivirus completa per:

- *Workstation* con Windows 98/ME, Windows NT/2000/XP e Linux;
- *file server e application server* con Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell NetWare, FreeBSD, OpenBSD, Linux; Sistema di archiviazione file Samba.
- *Sistemi di posta*, inclusi Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim e Qmail;
- *Gateway di Internet*. CheckPoint Firewall –1; MS ISA Server 2000 Enterprise Edition, Microsoft ISA Server 2004 Enterprise Edition
- *Computer portatili* (PDA) con sistema operativo Symbian OS, Microsoft Windows CE e Palm OS, oltre a smartphone con Microsoft Windows Mobile 2003 for Smartphone e Microsoft Smartphone 2002.

Il kit retail di Kaspersky® Corporate Suite comprende Kaspersky® Administration Kit, uno *strumento esclusivo per la gestione e l'amministrazione automatizzate*.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam è un'innovativa suite di software progettata per assistere le aziende con reti di piccole e medie dimensioni nella difesa contro i sempre più numerosi messaggi di posta elettronica non desiderati (spam). Il prodotto combina una tecnologia all'avanguardia in cui il programma analizza dal punto di vista linguistico il testo dei messaggi, tutti i moderni metodi di filtraggio della posta elettronica (inclusi gli elenchi RBL e le caratteristiche della posta formale) e una raccolta esclusiva di servizi che consentono agli utenti di individuare ed eliminare fino al 95% del traffico indesiderato.

Installato all'ingresso di una rete, dove monitora il traffico di posta in entrata alla ricerca di spam, Kaspersky® Anti-Spam funge da barriera alla posta indesiderata. Il software è compatibile con qualsiasi sistema di posta già in uso presso il cliente, e può essere installato sia su server mail esistenti sia su server dedicati.

L'elevato grado di efficacia di Kaspersky® Anti-Spam è consentito dall'aggiornamento quotidiano del database di filtraggio dei contenuti con i campioni forniti dagli specialisti del laboratorio linguistico. I database sono aggiornati ogni 20 minuti.

Kaspersky Security® per Microsoft Exchange 2003

Kaspersky Security per Microsoft Exchange esegue l'elaborazione anti-virus della posta in entrata e in uscita oltre che dei messaggi memorizzati sul server, incluse le lettere nelle cartelle pubbliche, e filtra la corrispondenza indesiderata utilizzando tecniche intelligenti di riconoscimento dello spam in combinazione a tecnologie Microsoft. L'applicazione scansiona tutti i messaggi in arrivo sul server Exchange Server attraverso il protocollo SMTP analizzandoli per individuare l'eventuale presenza di virus utilizzando le tecnologie anti-virus di Kaspersky Lab e verificando la presenza di attributi SPAM. Filtra lo spam sulla base di attributi formali (indirizzo di posta, indirizzo IP, dimensioni delle lettere, intestazione) e analizza il contenuto dei messaggi e dei relativi allegati utilizzando tecnologie intelligenti, incluse firme grafiche inequivocabili per identificare lo SPAM grafico. L'applicazione scansiona sia il corpo del messaggio che i file in allegato.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway è una soluzione completa che fornisce la protezione totale per gli utenti dei sistemi di posta. Questa applicazione installata tra la rete aziendale e Internet scansiona tutti i componenti dei messaggi di posta per verificare la presenza di virus e altro software nocivo (Spyware, Adware, ecc.) ed esegue un filtro anti-spam centralizzato del flusso di posta. L'applicazione contiene numerosi strumenti supplementari per filtrare il traffico di posta in base al nome e al tipo MIME degli allegati, oltre a numerosi tool per ridurre il carico sul sistema di posta e prevenire gli attacchi degli hacker.

Kaspersky Anti-Virus® per Proxy Server

Kaspersky Anti-Virus® per Proxy Server è una soluzione anti-virus per proteggere il traffico di rete trasferito attraverso con protocollo HTTP attraverso un server proxy. L'applicazione scansiona il traffico Internet in tempo reale, protegge da software nocivo che penetra nel sistema durante la navigazione in rete, e analizza i file scaricati da Internet.

Kaspersky Anti-Virus® per MIMESweeper per SMTP

Kaspersky Anti-Virus® per MIMESweeper per SMTP esegue scansioni anti-virus ad alta velocità del traffico SMTP su server con Clearswift MIMESweeper.

Il programma è sotto forma di plug-in per Clearswift MIMESweeper per SMTP, esegue la scansione anti-virus ed elabora la posta in entrata e in uscita in tempo reale.

C.2. Recapiti

Per qualsiasi domanda, commento o suggerimento, l'utente può rivolgersi ai distributori o direttamente a Kaspersky Lab. Saremo lieti di assistere i nostri

clienti relativamente ai nostri prodotti via telefono o via posta elettronica. Tutte le raccomandazioni e i suggerimenti ricevuti saranno attentamente presi in considerazione.

Supporto tecnico	Per qualsiasi informazione relativa al supporto tecnico, visitare la pagina http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html
Informazioni di carattere generale	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: sales@kaspersky.com

APPENDICE D. CONTRATTO DI LICENZA

Contratto di licenza standard con l'utente finale

AVVERTENZA PER TUTTI GLI UTENTI: LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO LEGALMENTE VINCOLANTE ("CONTRATTO") RELATIVO AL SOFTWARE SPECIFICATO ("SOFTWARE") PRODOTTO DA KASPERSKY LAB ("KASPERSKY LAB").

QUANDO ACQUISTA IL PRESENTE SOFTWARE VIA INTERNET, FACENDO CLIC SUL PULSANTE DI ACCETTAZIONE, L'UTENTE ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO. PER NON ACCETTARE TUTTE LE CONDIZIONI DEL PRESENTE CONTRATTO, FARE CLIC SUL PULSANTE CHE INDICA LA MANCATA ACCETTAZIONE DEI TERMINI E DELLE CONDIZIONI DEL PRESENTE E NON INSTALLARE IL SOFTWARE.

SE IL SOFTWARE È STATO ACQUISTATO FISICAMENTE, LA ROTTURA DEL SIGILLO DELLA BUSTA DEL CD, SCARICARE, INSTALLARE O UTILIZZARE QUESTO SOFTWARE. SE IL SIGILLO DELLA BUSTA DEL CD È ROTTO O LA SCATOLA È STATA APERTA, IL DIRITTO DELL'UTENTE ALLA RESTITUZIONE E AL RIMBORSO DECADE. IL SOFTWARE PER USO PRIVATO (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY PER PDA) ACQUISTATO SCARICANDO IL FILE DA INTERNET PUÒ ESSERE RESTITUITO PER IL RIMBORSO COMPLETO ENTRO 14 GIORNI DALLA DATA DELL'ACQUISTO PRESSO KASPERSKY LAB O IL SUO DISTRIBUTORE O RIVENDITORE AUTORIZZATO. ALTRI PRODOTTI NON SONO RIMBORSABILI. IL DIRITTO ALLA RESTITUZIONE E AL RIMBORSO SI RIFERISCE SOLO ALL'ACQUIRENTE ORIGINARIO.

Tutti i riferimenti al termine "Software" contenuti nel presente includeranno la chiave di attivazione software ("File di identificazione chiave") che sarà fornita all'utente da Kaspersky Lab come parte integrante del Software.

1. Concessione della licenza. Previo pagamento delle tasse di licenza applicabili e nel rispetto dei termini e delle condizioni del presente Contratto, con il presente Kaspersky Lab concede all'utente il diritto non esclusivo e non trasferibile di utilizzare una copia della versione specificata del Software e la documentazione in accompagnamento (la "Documentazione") per la durata del presente Contratto

e unicamente a uso aziendale interno. La copia del software può essere installata su computer, workstation, palmare o altro dispositivo elettronico per cui è stato progettato il Software (ciascuno dei quali denominato "Dispositivo client"). Se il Software è concesso su licenza come suite o pacchetto contenente più di un prodotto Software specificato, tale licenza si applica a tutti i prodotti software specificati, ed è soggetta alle restrizioni o alle condizioni d'uso specificate sul listino prezzi applicabile o sull'imballo di ciascun singolo prodotto Software.

1.1 Uso. Il Software è concesso in licenza in qualità di singolo prodotto; non può essere utilizzato su più di un Dispositivo client o da più di un utente per volta, salvo diversamente specificato nella presente Sezione.

1.1.1 Il Software è "in uso" su un Dispositivo client quando è caricato nella memoria temporanea (vale a dire nella memoria ad accesso casuale o RAM) o è installato nella memoria permanente (per esempio disco fisso, CD-ROM, o altro dispositivo di memoria) di quel dispositivo client. La presente licenza autorizza l'utente a creare il numero di copie di backup del Software necessarie per il suo utilizzo legale e unicamente a scopi di archivio, a condizione che tutte le copie contengano le informazioni di proprietà del software. L'utente è tenuto a mantenere traccia del numero e dell'ubicazione di tutte le copie del Software e della Documentazione e a prendere tutte le ragionevoli precauzioni per proteggere il Software da copia o utilizzo non autorizzati.

1.1.2 Qualora l'utente venda il Dispositivo client su cui è installato il Software, dovrà assicurarsi che tutte le copie del Software siano state cancellate.

1.1.3 All'utente è fatto divieto di decompilare, reverse engineer, disassemblare o altrimenti ridurre qualsiasi parte del presente Software a una forma leggibile dall'uomo e di permettere a terzi di compiere tali azioni. Le informazioni di interfaccia necessarie per ottenere l'interoperabilità del Software con programmi informatici creati autonomamente saranno fornite da Kaspersky Lab su richiesta, previo pagamento dei costi e delle spese ragionevolmente sostenuti per ottenere e fornire tali informazioni. Nel caso in cui Kaspersky Lab informi l'utente di non avere intenzione di mettere a disposizione tali informazioni per qualsiasi ragione, inclusi (senza limitazione) i costi, l'utente sarà autorizzato ad adottare le misure necessarie per ottenere l'interoperabilità, a condizione di poter soltanto decodificare o decompilare nella misura concessa per legge.

1.1.4 L'utente non deve, né deve permettere ad altri (in modo diverso da quanto espressamente permesso nel presente) di effettuare la correzione di errori o altrimenti modificare, adattare o tradurre il Software né creare opere derivate dal Software.

1.1.5 All'utente è fatto divieto di affittare, noleggiare o prestare il Software a terzi oltre che di trasferire o di fornire a terzi la licenza in concessione.

1.1.6 All'utente è fatto divieto di utilizzare il Software con strumenti automatici, semi-automatici o manuali progettati per creare firme virus, routine di rilevazione virus, qualsiasi altro dato o codice per la rilevazione di codici o dati nocivi.

1.2 Utilizzo in modalità Server. L'utente può utilizzare il Software su un Dispositivo Client o su un server o un dispositivo che operi come tale ("Server") nell'ambito di un ambiente multiutente o collegato in rete ("Modalità Server") solo se tale uso è consentito dal listino prezzi applicabile o sull'imballo del Software. È richiesta una licenza separata per ogni Dispositivo Client o postazione dalla quale ci si connette al Server, indipendentemente dal fatto che tali dispositivi Client o postazioni concesse in licenza si connettano contemporaneamente o stiano effettivamente accedendo al Software o utilizzando lo stesso. L'utilizzo di software o hardware che riduce il numero di Dispositivi Client o postazioni con utilizzo o accesso diretto al Software (per esempio software o hardware di "multiplexing" o "pooling") non riduce il numero di licenze richieste (in quanto il numero richiesto di licenze sarebbe pari al numero di ingressi distinti al software o hardware di multiplexing o pooling "front end"). Se il numero di Dispositivi Client o di postazioni che possono connettersi al Software è maggiore del numero di licenze ottenute, l'utente deve disporre di un meccanismo ragionevole che garantisca che l'uso del Software non supera i limiti di utilizzo specificati per la licenza ottenuta. La presente licenza autorizza l'utente a effettuare o scaricare il numero di copie della Documentazione per ogni Dispositivo Client o postazione concessi in licenza necessario per il suo utilizzo ai termini di legge, a condizione che ogni copia contenga tutte le informazioni sui diritti di proprietà della Documentazione.

1.3 Licenze per volume. Se il Software è concesso dietro una licenza per volume le cui condizioni sono specificate nella fattura applicabile del prodotto o sull'imballo del Software, l'utente può effettuare, utilizzare o installare tante copie supplementari del software sul numero di Dispositivi Client quante sono specificate nelle condizioni della licenza per volume. L'utente deve applicare meccanismi ragionevoli per garantire che il numero di Dispositivi Client su cui è stato installato il Software non superi il numero di licenze ottenute. La presente licenza autorizza l'utente a effettuare o scaricare una copia della Documentazione per ogni copia supplementare autorizzata dalla licenza per volume, a condizione che ogni copia contenga tutte le informazioni sui diritti di proprietà della Documentazione.

2. Periodo di validità. Il presente Contratto è valido per un (1) anno, salvo e fino a rescissione anticipata come stabilito nel presente. Il presente Contratto terminerà automaticamente in caso di mancata osservanza da parte dell'utente di una delle condizioni, limitazioni o altri requisiti descritti nel presente. Al momento della rescissione o alla scadenza del presente Contratto, l'utente è tenuto a distruggere immediatamente tutte le copie del Software e della Documentazione. È possibile rescindere dal presente Contratto in qualsiasi momento distruggendo tutte le copie del Software e della Documentazione.

3. Assistenza.

(i) Kaspersky Lab fornirà al cliente i servizi di assistenza ("Servizi di assistenza") di seguito definiti per un periodo di un anno dietro:

- (a) pagamento della tariffa di assistenza corrente;
- (b) soddisfacente compilazione del Modulo di sottoscrizione ai servizi di assistenza fornito all'utente unitamente al presente Contratto o disponibile sul sito web di Kaspersky Lab, che richiede all'utente di produrre il File di identificazione chiave fornito all'utente da Kaspersky Lab con il presente Contratto. Kaspersky Lab ha il diritto di stabilire, a propria discrezione, se l'utente abbia soddisfatto o meno questa condizione per la fornitura dei Servizi di Assistenza.
- (ii) I Servizi di Assistenza termineranno alla scadenza, salvo rinnovo annuo dietro il pagamento della tariffa annuale corrente e dietro soddisfacente nuova compilazione del Modulo di sottoscrizione ai servizi di assistenza.
- (iii) Con la compilazione del Modulo di richiesta dei Servizi di assistenza, l'utente accetta le condizioni esposte nell'Informativa sulla tutela della privacy applicata da Kaspersky Lab e allegata al presente Contratto, e acconsente esplicitamente al trasferimento dei propri dati all'esterno dei propri confini nazionali, come specificato nell'Informativa sulla tutela della privacy.
- (iv) Per "Servizi di assistenza" si intende
 - (a) Aggiornamenti gratuiti del software, inclusi gli aggiornamenti della versione;
 - (b) Aggiornamenti gratuiti del software, inclusi gli aggiornamenti della versione;
 - (c) Assistenza tecnica estesa tramite posta elettronica o linea telefonica dedicata forniti dal distributore o dal rivenditore;
 - (d) Rilevamento virus e aggiornamenti per l'eliminazione entro 24 ore.

4. Diritti di proprietà. Il Software è protetto dalle leggi sul copyright. Tutti i diritti, titoli e interessi in e sul Software, compresi tutti i diritti d'autore, brevetti, marchi e altri diritti sulla proprietà intellettuale sono proprietà e possesso di Kaspersky Lab e dei suoi fornitori. Il possesso, l'installazione o l'utilizzo del Software non trasferiscono all'utente alcun diritto relativo alla proprietà intellettuale del Software e non determinano l'acquisizione di diritti sul Software salvo quelli espressamente indicati nel presente Contratto.

5. Riservatezza. L'utente riconosce che il Software e la Documentazione, inclusa la specifica configurazione e la struttura dei singoli programmi e il File di identificazione chiave costituiscono informazioni proprietarie riservate di Kaspersky Lab. L'utente non dovrà divulgare, fornire o altrimenti rendere disponibili tali informazioni riservate in qualsivoglia forma a terzi senza previo consenso scritto di Kaspersky Lab. Dovrà inoltre applicare ragionevoli misure di sicurezza volte a proteggere tali informazioni riservate ma, senza tuttavia limitarsi a quanto sopra espresso dovrà fare quanto in suo potere per tutelare la sicurezza del File di identificazione chiave.

6. Garanzia limitata

(i) Kaspersky Lab garantisce che per un periodo di 90 giorni a decorrere dal primo caricamento o installazione il Software opererà sostanzialmente in conformità alle funzioni descritte nella Documentazione, a condizione che sia utilizzato in modo corretto e nella maniera specificata nella Documentazione.

(ii) L'utente si assume ogni responsabilità in merito alla scelta del presente Software per le proprie esigenze. Kaspersky Lab non garantisce che il Software e/o la relativa Documentazione saranno idonei a soddisfare tali esigenze, né che l'uso sarà privo di interruzioni e di errori;

(iii) Kaspersky Lab non garantisce che il Software identifichi tutti i virus noti né esclude che possa occasionalmente eseguire il report erroneo di un virus in un titolo non infettato da quel virus.

(iv) L'unico rimedio per l'utente e l'unica responsabilità a carico di Kaspersky Lab in caso di violazione della garanzia come da paragrafo (i) consiste, a discrezione di Kaspersky Lab, nella riparazione, sostituzione o rimborso del Software qualora tale violazione venga riferita a Kaspersky Lab o a chi in sua vece durante il periodo di validità della garanzia. L'utente dovrà fornire tutte le informazioni ragionevolmente necessarie per agevolare il Fornitore nel ripristino dell'articolo difettoso.

(v) La garanzia di cui al punto (i) non è applicabile qualora l'utente (a) apporti modifiche al presente Software o determini la necessità di modificarlo senza il consenso di Kaspersky Lab, (b) utilizzi il Software in modo difforme dall'uso previsto o (c) impieghi il Software per usi diversi da quelli permessi ai sensi del presente Contratto.

(vi) Le garanzie e le condizioni stabilite dal presente Contratto sostituiscono eventuali altre condizioni, garanzie o termini relativi alla fornitura o fornitura presunta dello stesso; la mancata fornitura o eventuali ritardi nella fornitura del Software o della Documentazione che, salvo per il presente paragrafo (v) potrebbero avere effetto tra Kaspersky Lab e l'utente o potrebbero essere diversamente impliciti o integrati nel presente Contratto o in un eventuale accordo collaterale mediante statuto, diritto consuetudinario o altrimenti, sono esclusi mediante il presente (inclusi, senza tuttavia ad essi limitarsi, le condizioni implicite, le garanzie o altri termini relativi a qualità soddisfacente, idoneità per l'uso previsto o esercizio di ragionevoli competenze e cautele).

7. Responsabilità limitata

(i) Nessun elemento nel presente Contratto deve escludere o limitare la responsabilità di Kaspersky Lab relativamente a (i) responsabilità civile per frode, (ii) decesso o lesioni personali causate da un suo mancato esercizio di cautela ai sensi del diritto consuetudinario o dalla violazione negligente di una delle condizioni del presente Contratto, (iii) eventuali violazioni degli obblighi stabiliti dalla sezione 12 del Sale of Goods Act del 1979 o della sezione 2 del Supply of Goods and Services Act del 1982 o (iv) eventuali responsabilità che non possono essere escluse ai termini di legge.

(ii) Ai sensi del paragrafo (i), il Fornitore non deve essere ritenuto responsabile (relativamente al contratto, per responsabilità civile, restituzione o altro) per i seguenti danni o perdite (siano questi danni o perdite previsti, prevedibili, noti o altro):

(a) perdita di reddito;

(b) perdita di utili effettivi o presunti (inclusa la perdita di utili sui contratti);

(c) perdita di liquidità;

(d) perdita di risparmi presunti;

(e) perdita di affari;

(f) perdita di opportunità;

(g) perdita di avviamento;

(h) danni alla reputazione;

(i) perdita, danni o corruzione di dati;

(j) eventuali perdite indirette o conseguenti o danni arrecati in qualsiasi modo (inclusi, a scanso di dubbi, i danni o le perdite del tipo specificato nel paragrafo (ii), da (a) a (ii), (i).

(iii) Ai sensi del paragrafo (i), la responsabilità di Kaspersky Lab (né a fini del contratto, frode, restituzione o in nessun'altra maniera) derivante da o in relazione alla fornitura del Software non supererà in nessun caso l'importo corrispondente all'onere ugualmente sostenuto dall'utente per il Software.

8. La costituzione e l'interpretazione del presente Contratto devono essere effettuate in conformità alle leggi dell'Inghilterra e del Galles. Le parti si sottopongono alla giurisdizione delle corti di Inghilterra e Galles, salvo il diritto di Kaspersky Lab in qualità di parte ricorrente, di avviare il ricorso in qualsiasi corte della giurisdizione competente.

9. (i) Il presente Contratto contiene per intero tutti gli intendimenti delle parti relativamente all'oggetto del presente e sostituisce tutti gli eventuali accordi, impegni e promesse precedenti tra l'utente e Kaspersky Lab, sia orali che per iscritto, che possano scaturire o essere impliciti da qualsiasi cosa scritta o pronunciata oralmente in fase di negoziazione tra Kaspersky Lab o suoi rappresentanti e l'utente precedentemente al presente Contratto; tutti gli accordi precedenti tra le parti relativamente all'oggetto di cui sopra decadranno a partire dalla Data di entrata in vigore del presente Contratto. Fatto salvo quanto stabilito ai paragrafi (ii) - (iii), l'utente non sarà in alcun modo risarcito per eventuali false dichiarazioni ricevute sulle quali aveva fatto affidamento nella stipula del presente Contratto ("Falsa dichiarazione") e Kaspersky Lab non sarà vincolata da altre responsabilità oltre a quelle relative alle espresse condizioni del presente Contratto.

(ii) Nessun elemento nel presente Contratto esclude o limita la responsabilità di Kaspersky Lab per eventuali false dichiarazioni rilasciate intenzionalmente.

(iii) La responsabilità di Kaspersky Lab per Dichiarazioni erronee in merito a questioni fondamentali, incluse le questioni fondamentali ai fini della capacità del produttore di adempiere agli obblighi previsti dal presente Contratto, sarà soggetta alle limitazioni di responsabilità esposte nel paragrafo 7 (iii).